anno I, n. 1, 2011

Osservatorio degli operatori della sicurezza

LA VIDEOSORVEGLIANZA
PROFILI APPLICATIVI*

Claudio CAPPELLIERI**

Angela CATAPANO**

Italo CERINI**

Fabrizio MANCINI**

Giovanni MANDATO**

*Il presente lavoro è stato presentato dagli autori, in una prima versione, nell'ambito del **26° Corso di formazione dirigenziale**, organizzato dalla **Scuola Superiore di Polizia.**

**Primo dirigente della Polizia di Stato.

INDICE

Presentazione

Il presente lavoro ha avuto come obiettivo l'analisi di aspetti normativi, operativi e sperimentali, concernenti l'applicazione della videosorveglianza nell'ambito dell'attività di polizia. Esso ha costituito un'occasione interessante per sperimentare il modello di lavoro di gruppo, verificandone le dinamiche interne e l'evoluzione delle relazioni interpersonali attraverso un percorso orientato a coniugare conoscenze giuridiche ed esperienze professionali acquisite.

Il punto di partenza del progetto ha riguardato lo studio evolutivo delle normative interne ed internazionali, con particolare riferimento al concetto di *privacy* e videosorveglianza.

Nella seconda fase, l'attenzione è stata focalizzata su aspetti processuali ed investigativi delle videoriprese, con particolare riferimento ai limiti di ammissibilità probatoria nei luoghi pubblici e di privata dimora. In particolare, ne sono stati esaminati i vari ambiti applicativi offrendo spunti di riflessione, in una prospettiva *de iure condendo,* con riferimento ai comportamenti non comunicativi e alla comunicazione con se stessi.

Nell'ultima parte dello studio, l'obiettivo è stato invece quello di offrire uno spaccato di dettaglio dei c.d. processi biometrici, consequenziali all'utilizzo di strumenti di videosorveglianza, considerando anche le criticità delle tecniche sino a oggi sperimentate. In particolare, traendo spunto dal sistema realizzato presso l'aeroporto di Fiumicino, sono state descritte le fasi di progettazione di un impianto di videosorveglianza da utilizzare quale supporto operativo nell'attività di controllo e di prevenzione rispetto a un obiettivo sensibile come, appunto, un

aeroporto internazionale, rilevando, tuttavia, i limiti applicativi connessi allo sviluppo tecnologico attuale.

CAPITOLO I
L'inquadramento generale della materia

di Italo Cerini

1. Videosorveglianza e *privacy*

La tematica della *privacy*, della sua estensione e della sua tutela, nasce alla fine del 1700 in Inghilterra per poi affermarsi negli Stati Uniti d'America. Inteso dapprima come semplice capacità della persona di opporsi alla forza della Corona e derivandone dunque la necessità di determinare precisi limiti all'azione dello Stato nei confronti dell'individuo, il concetto viene meglio rielaborato a fine '800. Nel 1890, infatti, il saggio "*The right to privacy*", di Samuel Warren e Louis Brandeis, concettualizza la *privacy* come *the right to be let alone* ossia la naturale aspirazione dell'individuo a che la propria sfera privata venga tutelata da interferenze pubbliche o private altrui.

Per i suddetti Autori, ogni individuo ha dunque il diritto di essere "lasciato solo" e di proteggere questa sua solitudine allo stesso modo in cui ha diritto di proteggere la proprietà privata.

Il diritto alla *privacy* era costruito, pertanto, come diritto soggettivo al pari di quello di proprietà sul quale viene, in principio, modellato.

Oggi però non sfugge come questa originaria accezione assolutamente individualistica della *privacy*, colga solo un parziale aspetto della problematica. Nell'odierna società, infatti, l'attenzione va spostata sull'interesse del soggetto a un controllo sul complesso delle informazioni che lo riguardano e sull'uso che ne può venir fatto da chi le detiene e le tratta.

L'odierna informatizzazione della stragrande maggioranza delle attività e dei servizi costringe, infatti, ciascuno di noi a lasciare inevitabilmente una traccia delle proprie azioni, abitudini, preferenze, caratteristiche e inclinazioni. Tutti dati che, sebbene singolarmente possano apparire neutri, una volta subìto un qualche trattamento possono acquistare un diverso significato, essere utilizzati per vari fini e uscire comunque dal controllo del soggetto titolare degli stessi.

Questo cambiamento di scenario storico-sociale ci porta dunque a riconsiderare la *privacy* e la sua tutela in termini diversi dagli originari, per orientarli e centrarli sul potere di controllo della circolazione delle informazioni personali: la *privacy* cioè come sinonimo di protezione dei dati personali.

Isolato il concetto di *privacy* rilevante ai fini del nostro studio, passiamo ora brevemente all'analisi del concetto di sorveglianza e, da questo, al concetto di videosorveglianza.

In un'ottica storica e sociologica può infatti dirsi che, dalla nascita dei feudi sino a quella dei primi Comuni, l'esercizio del potere di governo è sempre coinciso con il potere di sorveglianza sulle masse.

Il *Domesday Book*, primo censimento di tutte le proprietà fondiarie inglesi pubblicato nell'anno 1086, costituisce il primo esempio di controllo amministrativo globale effettuato dal re e diretto a rafforzare il suo potere attraverso la conoscenza completa del suo territorio.

Con la nascita dello stato moderno, poi, la raccolta dei dati necessari alla creazione di strutture organizzative centralizzate, rese più solide attraverso la sorveglianza, è divenuta sempre più amplia e più complessa contemplando informazioni sempre più dettagliate e complete.

Da questo momento il binomio controllo/potere diventa oggetto di importanti studi sociologici.
Hanno analizzato a fondo il tema della sorveglianza come strumento di potere che consente all'amministrazione statale di "tener d'occhio" la popolazione, Karl Marx, Max Weber e poi Foucault. Il punto di partenza di quest'ultimo è stato lo studio del progetto dell'architetto Jeremy Bentham per il penitenziario *Panopticon*, pubblicato nel 1791. Esso riguardava un edificio a struttura semicircolare con un reparto di ispezione posto al centro e le celle individuali tutte intorno al perimetro. I detenuti, cosi sistemati, erano dunque esposti allo sguardo delle guardie senza avere la reciproca possibilità di vedersi dal momento che, un mirato sistema di illuminazione e l'uso di apposite persiane di legno, consentivano agli agenti di essere invisibili ai detenuti.
Il controllo, dunque, era garantito dalla sensazione costante di essere osservati da occhi invisibili e da qui il termine, tratto dal greco, *panopticon* ossia il luogo dove tutto è visto.
Il merito di Foucault sta nell'aver messo in luce come l'innovazione di Bentham non servisse solo a sorvegliare ma a utilizzare l'incertezza come metodo di subordinazione perché, se il vedere è causa di conoscenza, il non vedere è causa di subordinazione. La sorveglianza, in conclusione, rafforza il potere di chi guarda indebolendo quello di chi è osservato.
Il contributo di Foucault è stato poi ripreso da uno dei più grandi sociologi contemporanei, Anthony Giddens, il quale, partendo dal pensiero che nell'era moderna il potere disciplinare è caratterizzato da nuove modalità per le quali l'osservazione è cruciale, afferma che oggi la sorveglianza elettronica evidenzia tratti panottici: l'invisibilità dell'ispezione,

il suo automatismo, il coinvolgimento dei soggetti nella propria sorveglianza.

Più di recente, la tematica del controllo sociale attraverso sistemi di sorveglianza è stata al centro di approfonditi dibattiti anche da parte di alcuni dei più moderni sociologi americani, componenti della c.d. scuola di Chicago, i quali per primi hanno ipotizzato la possibilità di prevenire la criminalità urbana attraverso lo strumento della sorveglianza.

Nel tralasciare, per intuibili ragioni di tempo, altri pur rilevanti contributi al tema, come quello di Ronald Clarke e del suo modello di prevenzione situazionale, arriviamo alla attuale costruzione della cosiddetta nozione di "nuova sorveglianza", elaborata dallo studioso americano Gary T. Marx nel 1985. Secondo questo autore, nel passaggio dall'era moderna alla postmoderna, la nuova sorveglianza è caratterizzata da una serie di peculiarità proprie delle tecnologie elettroniche quali l'invisibilità, l'involontarietà, l'intensività e l'estensività.

La sua logica sta nella possibilità di modificare l'ambiente attraverso dispositivi elettronici al fine di prevenire o ridurre la criminalità; suo obiettivo principale è quello di ottenere il controllo sociale agendo sulle situazioni piuttosto che sulle predisposizioni criminali del singolo.

I sistemi di videosorveglianza, oggi, sono quindi da ritenersi componente fondamentale dei sistemi di sicurezza perché per il loro tramite si ha, infatti, la possibilità di visualizzare immagini in tempo reale o, a seguito della loro registrazione, quella di controllare ambienti o più vaste aeree, individuare pericoli, organizzare l'intervento necessario.

Precisati come sopra i concetti di *privacy* e di videosorveglianza, è di tutta evidenza come quest'ultima abbia un impatto forte sulla vita dei singoli e sul loro diritto alla riservatezza perché

permette a chiunque (pubblico o privato) di visualizzare, raccogliere, memorizzare, archiviare dati personali consentendogli, oltretutto, di procedere alla localizzazione delle persone fisiche nel tempo e nello spazio. Da ciò emerge la naturale necessità di garantire la tutela dei dati personali dei soggetti interessati, raccolti con l'uso di tale tecnologia; tutela e disciplina che passiamo quindi ad illustrare.

2. La normativa internazionale

Un primo passo nel riconoscimento della tutela dell'individuo contro le interferenze illecite nella sua sfera privata è possibile rinvenirlo nella Dichiarazione universale dei diritti dell'uomo, approvata nel 1948 dall'Assemblea Generale delle Nazioni Unite.

Lo stesso dicasi per la Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata nel 1950 e ratificata dall'Italia nel 1955.

Si passa poi alla Convenzione di Strasburgo n. 108 del 1981, relativa alla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, per approdare alla più recente Carta dei diritti fondamentali dell'Unione Europea (cosiddetta Carta di Nizza) del dicembre 2000, in seguito trasfusa nel Trattato firmato a Roma nell'ottobre 2004, che all'art. 8 riconosce il diritto alla protezione dei dati personali.

Fondamentale in materia è anche la Direttiva Europea n.95/46/CE (alla quale hanno fatto seguito altre direttive come, ad esempio, la n. 2002/58/CE e la n. 2006/24/CE) dalla cui attuazione traggono origine le varie normative adottate nei singoli Stati membri dell'Unione Europea in materia di protezione dei dati personali.

3. La normativa nazionale.

A livello nazionale la nostra attenzione va riposta, principalmente, nelle norme costituzionali (in particolare negli articoli 2, 3, 13, 14, 15, 21), nella legge n. 300/1970 (c.d. Statuto dei lavoratori), nella n. 98/1974, nel d.lgs. n. 196/2003 (c.d. Codice della *privacy*) e nel provvedimento generale in materia di videosorveglianza, adottato dal Garante per la protezione dei dati personali l'8 aprile 2010.

Le prime rilevano perché è da esse (e dai principi che esse esprimono) che la giurisprudenza è partita per individuare il concetto giuridico della *privacy* e riconoscerlo come diritto costituzionalmente tutelato, seppure implicitamente, connaturato alla natura stessa dell'uomo, sia come singolo sia come componente delle formazioni sociali entro le quali si sviluppa la sua personalità (per tutte Corte Cass. sent. n. 2129/1975).

La legge n. 300/1970 rileva invece perché, sancendo il divieto per il datore di lavoro di effettuare indagini ai fini dell'assunzione e nel corso del rapporto di lavoro, sulle opinioni politiche, religiose o sindacali dei lavoratori, ma anche il divieto di controllo a distanza dei lavoratori, fornisce un primo riconoscimento legislativo alla *privacy*.

La legge n. 98/1974 va invece ricordata perché, per la prima volta, introduce nel nostro sistema ordinamentale il concetto di riservatezza come bene giuridico individuale meritevole di tutela.

È stato però il decreto legislativo n. 196/2003 (preceduto dalla ormai abrogata legge n. 675/1996) che ha elevato la protezione dei dati personali a posizione giuridica autonoma, riconoscendola in capo a chiunque. Questa assurge, dunque, a diritto fondamentale della persona affiancandosi a quella della più tradizionale riservatezza e del diritto all'identità personale.
La questione dei potenziali rischi per la *privacy* dell'individuo, rappresentati dai dispositivi di videosorveglianza, è stata nel tempo oggetto di molteplici attenzioni e interventi da parte dell'Autorità del Garante per la protezione dei dati personali, a partire dal 1999. È in quell'anno, infatti, che alcuni Enti Locali avanzano le prime richieste per controllare, tramite questo sistema, il territorio di competenza e il traffico veicolare cittadino. Il Garante, in risposta, evidenzia la necessità per questi Comuni di adottare per le riprese alcune cautele minime a garanzia della *privacy* dei cittadini, idonee a limitare l'ingrandimento delle immagini e lo stesso livello di dettaglio (ad esempio sui tratti somatici). Ancora il Garante sottolinea l'irrinunciabilità di fornire un'informativa, mediante appositi avvisi, nonché la necessità di rispettare il principio di non eccedenza dei dati rispetto agli scopi e finalità perseguiti.
Nel corso del successivo anno 2000 l'Autorità Garante, nello svolgere una prima indagine ricognitiva sulle attività di videosorveglianza espletate dai Comuni di Milano, Verona, Roma e Napoli, concludeva sottolineando l'urgenza di una specifica normativa in materia e dettava, in pari tempo, una prima serie di dieci punti, il c.d. decalogo, che dovevano comunque essere rispettati in caso di utilizzo di sistemi di videosorveglianza che permettessero la registrazione di immagini. Tra questi il diritto ad essere informati della presenza della videosorveglianza in atto, l'obbligo di registrare

solo quando veramente necessario, quello di evitare immagini troppo dettagliate o ingrandite, il limite temporale di conservazione delle immagini, e altri principi che troveranno, poi, più completa disciplina in un successivo provvedimento generale del 2004.

L'approvazione, nel 2003, del Codice della *privacy* che, all'art. 134 tratta esplicitamente della videosorveglianza, porta il Garante, nel corso del successivo anno 2004, ad emanare un primo provvedimento generale in materia, oggi integralmente sostituito da quello del 2010.

Preliminare all'analisi più dettagliata delle richiamate fonti di disciplina della videosorveglianza è però la definizione di alcuni concetti base in materia di protezione della *privacy* (qui intesa come protezione dei dati personali) diffusamente elencati all'art. 4 del citato Codice e di seguito specificati.

a) Dato personale (art. 4, comma 1, lett. b): è, in buona sostanza, qualunque informazione (come ad esempio l'immagine) riconducibile a un determinato soggetto e, per il Codice, «relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale».

b) Trattamento (art. 4, comma 1, lett. a): è qualunque operazione (come ad esempio la ripresa visiva o la rilevazione audio) effettuata su dati personali, anche senza l'ausilio di strumenti elettronici, concernente «la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati».

c) Titolare del trattamento (art. 4, comma 1, lett. f): è «la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza».
d) Interessato (art. 4, comma 1, lett. i): è colui al quale si riferiscono i dati personali, sia esso persona fisica, giuridica, ente o associazione.
Introdotto il concetto di trattamento, la formulazione esistente non consentiva di disporre di una definizione legislativa della videosorveglianza che poteva essere, tuttavia, ricostruita in via interpretativo-sistematica. L'art. 134 del Codice, infatti, pur essendo l'unico del capo III intitolato "videosorveglianza", non ne dà una definizione univoca; un aiuto in tal senso è stato fornito dalla dottrina, che la definisce come «attività di rilevamento di immagini con strumenti elettronici per finalità di controllo e in modo non occasionale, eventualmente in associazione con l'acquisizione di dati sonori e/o biometrici (ad es. le impronte digitali)» (V. Gagliardi). Conseguentemente, chiunque voglia svolgere un'attività di videosorveglianza che, come detto, costituisce un trattamento di dati personali, dovrà attenersi a specifici principi, stabiliti dal Codice e richiamati nel provvedimento generale del 2010, che assicurano un necessario contemperamento fra le esigenze di sicurezza, generalmente perseguite con la videosorveglianza, e il diritto fondamentale alla protezione dei dati personali.
Si tratta, in particolare, dei seguenti principi[1].

[1] Per un approfondimento si rinvia a A. FROSINI, *La disciplina generale della*

1) Principio di liceità. Enunciato all'art. 11, comma 1, lett. *a)* del Codice, stabilisce che i dati personali devono essere trattati «n modo lecito e secondo correttezza» ovvero il loro trattamento deve essere conforme alla legge o a qualsiasi norma di volta in volta applicabile. Meglio ancora, il trattamento dati attraverso sistemi di videosorveglianza è possibile solo se è fondato su uno dei presupposti di liceità che il Codice prevede espressamente per gli organi pubblici o per i soggetti privati ed enti pubblici economici. In questo secondo caso si deve però distinguere:

- se il sistema di videosorveglianza viene usato da una persona fisica esclusivamente per fini personali, domestici o di sicurezza individuale, il relativo trattamento dei dati non è soggetto alle disposizioni del Codice a meno che le immagini così raccolte non siano destinate ad una comunicazione sistematica o alla diffusione (art. 5, co. 3). Devono applicarsi comunque, anche in questo caso, le disposizioni in tema di sicurezza dei dati e di responsabilità di cui agli artt. 31 e 15 del Codice nonché la norma di cui all'art. 615 c. p. in relazione al reato di interferenza illecita nella vita privata;
- se il sistema di videosorveglianza viene usato da persone giuridiche il trattamento dei dati deve essere fondato su uno dei presupposti di cui agli artt. 23 e 24 del Codice (consenso espresso dell'interessato o adempimento di un obbligo di legge, provvedimento del Garante di cosiddetto "bilanciamento di interessi").

2) Principio di necessità. Enunciato dall'art. 3 del Codice, impone in generale l'esclusione di ogni uso superfluo e di qualunque eccesso o ridondanza nell'impiego di impianti di videosorveglianza. Recita, infatti, il richiamato art. 3 che «i

sistemi (…) sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere perseguite mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità». In altri termini il trattamento deve essere considerato necessario per il perseguimento di finalità dichiarate e lecite e deve, altresì, riguardare solamente i dati immagini indispensabili per raggiungere quelle finalità.

3) Principio di proporzionalità. Enunciato dall' art. 11, co. 1, lett. d), del Codice, questo principio stabilisce che i dati personali oggetto di trattamento devono essere «pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati».

Il requisito della pertinenza impone che i dati trattati debbano essere rilevanti rispetto alle finalità di cui sopra; quello di completezza, che gli stessi debbano possedere tutti gli elementi necessari ed opportuni per attuarle; quello della non eccedenza che non devono essere estranei alle finalità perseguite. Il rispetto del principio di proporzionalità va verificato, da parte del titolare, in ogni fase del trattamento. Nella fase preliminare, ad esempio, per attivare gli impianti audiovisivi solo come *extrema ratio*, ritenendosi altre misure inattuabili o insufficienti, per non adottare la scelta semplicemente meno costosa o meno complicata o di più rapida attuazione e per evitare la rilevazione in aree o con riferimento ad attività non soggette a concreti pericoli ma solo per fini di mera apparenza o prestigio.

Nella fase successiva, invece, per stabilire, ad esempio, se sia sufficiente, ai fini della sicurezza, rilevare immagini che non rendano identificabili i singoli cittadini, anche tramite

ingrandimenti ovvero se sia realmente essenziale ai fini prefissi raccogliere immagini dettagliate.

4) Principio di finalità. Questo principio trova fondamento nell'art. 11, comma 1, lett. b) del Codice. Esso stabilisce che i dati personali devono essere trattati «per scopi determinati, espliciti e legittimi» ossia specifici, manifesti e conformi a legge.

Con il provvedimento generale del 2004 l'Autorità Garante per la protezione dei dati personali ha formulato una vera e propria disciplina generale applicabile alle attività di rilevamento d'immagini che è stata poi sostituita dal Provvedimento generale del 2010 la cui struttura richiama in realtà quella del precedente, ma il Garante ne modifica l'assetto sia per la proliferazione di nuove tecniche audiovisive particolarmente invasive della *privacy*, sia per le modifiche al concetto di sicurezza dei cittadini recepito in alcuni provvedimenti di natura governativa. Sotto quest'ultimo profilo si registra, infatti, un aumento dell'uso della videosorveglianza come deterrenza per prevenire forme di illegalità e degrado da parte delle pubbliche amministrazioni e sono chiari i riferimenti ai nuovi poteri degli enti locali in tema di sicurezza ed incolumità pubblica. Per quanto riguarda il settore privato, il provvedimento del 2010 riproduce sostanzialmente (pur con alcune modifiche che però non sono di interesse in questa sede) il provvedimento del 2004.

Fra le nuove regole vi è, per esempio, quella concernente l'informativa semplificata da rendere all'interessato anche in caso di videosorveglianza notturna con strumenti *ad hoc* come pannelli luminosi, *display*, *led* e insegne luminose.

Ancora, per quanto riguarda il mancato obbligo di rendere l'informativa da parte degli organi pubblici, il Garante specifica che ciò è possibile solo in presenza di una norma che tale

obbligo escluda, come ad esempio nel caso dell'art. 53 del Codice, inerente il trattamento di dati personali per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. Fuori da questa ipotesi, dunque, anche i Comuni, per le finalità previste dal c.d. decreto sicurezza, devono rendere l'informativa.

Nel settore della circolazione stradale, il Garante avverte che i conducenti dei veicoli e le persone che accedono o transitano in aree dove sono attivi sistemi elettronici di rilevazione automatizzata delle infrazioni, devono essere previamente informati circa il trattamento dei dati personali.

Molto più particolareggiata, rispetto al 2004, è la parte che stabilisce le prescrizioni tecniche attinenti alla videosorveglianza.

L'art. 31 e seguenti del Codice impongono un'adeguata protezione dei dati mediante l'adozione di tutte le misure di sicurezza idonee a garantire la riservatezza, l'integrità e la disponibilità dei dati stessi.

In particolare, le misure minime di sicurezza previste all'art. 34 del Codice sono richiamate anche nel provvedimento del 2010 al punto 3.3.1 e concernono il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali volte a contrastare i rischi che incombono sui dati. I rischi da contrastare sono la distruzione, la perdita, la sottrazione (*identity theft* o furto di identità) o indebita appropriazione dei dati stessi, l'accesso non autorizzato, il trattamento non consentito o non conforme alle finalità della raccolta.

È opportuno, a questo punto, precisare che le misure di sicurezza possono essere distinte in misure minime e misure idonee.

Per misure minime si intende il complesso delle misure che configurano il livello minimo di protezione richiesto dalla legge. Sono obbligatorie a prescindere da qualsiasi valutazione del rischio e la loro mancata adozione comporta una sanzione penale (ai sensi dell'art.169 del Codice) oltreché amministrativa (ai sensi dell'art. 162, co. 2-bis del Codice).

Per misure idonee, si intendono quelle adeguate a ridurre al minimo i rischi di cui sopra e la loro mancata adozione può comportare una sanzione amministrativa (ai sensi dell'art. 162, co. 2-ter, del Codice). L'idoneità è valutata in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento. Non si tratta di misure codificate dalla legge; la loro scelta è rimessa al titolare in base alla valutazione del rischio. È importante evidenziare che la mancata adozione di misure idonee può dar luogo anche a responsabilità civile laddove si riscontrino danni all'interessato per effetto del trattamento di dati personali, ai sensi dell'art. 2050 c.c. richiamato dall'art. 15 del Codice.

Le misure minime da adottare per trattamenti effettuati con strumenti elettronici (con ciò intendendo gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico, compresi i sistemi di videosorveglianza), contemplate dall'art. 34 del Codice, sono le seguenti.

a) L'autenticazione informatica, ossia l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità, al fine di impedire l'accesso ai dati da parte di chi non è autorizzato. È necessario, infatti, l'utilizzo di apposite credenziali di autenticazione per accedere ai dati.

b) L'adozione di procedure di gestione delle credenziali di autenticazione, intendendo con quest'ultima locuzione i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o

ad essa univocamente correlati, utilizzati per l'autenticazione informatica (ad esempio, *user id* e *password*, *badge*, chiave *hardware* o altro dispositivo; caratteristiche biometriche quali l'impronta digitale, la voce, la struttura della retina, ecc.). Le procedure di gestione delle credenziali di autenticazione riguardano, ad esempio, l'attribuzione all'incaricato della credenziale, la sua modifica al primo utilizzo, la conservazione della copia presso la persona designata come custode della *password*, la definizione della periodicità della sua sostituzione, i criteri per la scelta della parola chiave, la definizione delle procedure di disattivazione della stessa, le istruzioni all'incaricato circa la necessità di mantenere segreta la parola chiave;

c) L'utilizzazione di un sistema di autorizzazione, ossia l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente. Per profilo di autorizzazione si intende l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti. Il sistema di autorizzazione è generalmente un programma che permette ad ogni incaricato, riconosciuto il suo profilo di autorizzazione per mezzo della *password* utilizzata, di compiere solo alcune operazioni di trattamento oppure di accedere solo ad alcune banche dati o una combinazione delle due limitazioni.

d) L'aggiornamento periodico della individuazione dell'ambito del trattamento. Con frequenza almeno annuale deve essere effettuata la verifica e se necessario la revisione degli ambiti dei trattamenti consentiti agli incaricati (ovverosia dei loro poteri e

autorizzazioni) per modificarli e/o revocarli in caso di mutamenti organizzativi.

e) La protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici. Come noto, i dati personali devono essere protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici, da aggiornare con cadenza almeno semestrale, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne eventuali difetti. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-*ter* del Codice penale, mediante l'utilizzo di idonei strumenti elettronici. Quando il trattamento concerne dati sensibili o giudiziari è richiesto l'utilizzo di un *firewall* (dispositivo *hardware* o software che protegge il *computer* da accessi non autorizzati provenienti da Internet). Si ritiene che tale misura dovrà essere adottata solo qualora il *computer* sia dotato di connessione ad Internet o sia connesso ad una rete nella quale vi sono computer dotati di connessione a *Internet*.

f) L'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi. Si tratta, in particolare, di procedure di *back-up* mediante il salvataggio dei dati con frequenza almeno settimanale. Per i dati sensibili/giudiziari, in caso di perdita o distruzione o danneggiamento, il sistema deve poter garantire il ripristino (recupero) degli stessi in un tempo che non può essere superiore a 7 giorni.

g) La tenuta di un aggiornato documento programmatico sulla sicurezza "DPS". L'obbligo esiste per tutti i titolari che trattano dati personali con strumenti elettronici. Da tale obbligo sono tuttavia esclusi i soggetti che trattano soltanto dati personali

non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale, rispetto ai quali la tenuta del DPS è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte.

Il DPS, laddove obbligatorio, va predisposto e aggiornato annualmente affinché si attesti la corretta adozione delle previste procedure che riguardano il trattamento dei dati personali. Nel documento sono indicati:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità

che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare;

- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, i criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Per quanto riguarda, invece, i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici, le misure minime da adottare sono invece le seguenti (ai sensi dell'art. 35 del Codice).

a) L'aggiornamento periodico della individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative. Esso va effettuato almeno annualmente, analogamente a quanto avviene per i trattamenti con strumenti elettronici.

b) La previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti. Agli incaricati devono essere impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

c) La previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati. In particolare, quando l'art. 35 si riferisce a «determinati atti» significa atti e documenti contenenti dati sensibili e/o giudiziari. L'accesso agli archivi contenenti quest'ultimo tipo di dati deve essere sempre controllato e le

persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

Il profilo della sicurezza è particolarmente importante qualora il trattamento di dati presenti, ai sensi dell'art. 17 del Codice, rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato (come ad esempio nel caso dei dati biometrici). In tali situazioni, ai sensi dell'art. 37 del Codice, corre l'obbligo di notificare al Garante il trattamento a cui si intende procedere.

Il titolare, pertanto, è tenuto a notificare al Garante l'inizio del trattamento di tali dati, specificando le finalità dello stesso e includendo una descrizione delle categorie delle persone interessate. Anche nel provvedimento del 2010, il Garante ha ribadito che il trattamento effettuato tramite sistemi di videosorveglianza e che sia riconducibile all'art. 37 del Codice debba essere preventivamente notificato a pena di sanzione amministrativa.

Per quanto riguarda l'ambito delle forze di polizia, tuttavia, il Codice, ai sensi dell'art. 53, esenta dal sopracitato obbligo. Qualora, però, per il trattamento di dati si ricorra all'uso di «particolari tecnologie» (come ad esempio i sistemi di videosorveglianza che raccolgono immagini associate a dati biometrici), ai sensi dell'art. 55 del Codice, tale trattamento potrà essere effettuato esclusivamente sulla base di una preventiva comunicazione al Garante, ai sensi dell'art. 39 del Codice, mediante la quale si innesca l'obbligatoria richiesta di verifica preliminare prevista dal punto 3.2.1 del provvedimento generale in materia di videosorveglianza.

Per quanto riguarda, poi, il tempo di conservazione delle immagini, l'Autorità reitera le precedenti disposizioni applicandole però a tutti coloro che non siano Amministrazioni

Comunali, dal momento che solo queste ultime usufruiscono della previsione normativa in materia di sicurezza urbana. Particolare rilievo, inoltre, assume nel nuovo provvedimento del 2010 il ricorso alle sanzioni amministrative nel caso di infrazioni alle norme.

In conclusione, può dirsi che la nuova normativa se da un lato non apporta evidenti novità dal punto di vista degli adempimenti richiesti ai privati, evidenzia un concetto più maturo di videosorveglianza nel settore pubblico, laddove la costante pressione esercitata dagli Enti Locali, interessati come non mai ad installare impianti di videosorveglianza, sostenuta a livello politico con il varo delle norme dei vari pacchetti sicurezza, ha di certo inciso sull'impianto sicuramente più garantistico del precedente provvedimento generale del 2004.

CAPITOLO II

La videosorveglianza nelle attività di polizia giudiziaria: ambiti di applicazione e limiti di ammissibilità nel procedimento penale

di Claudio Cappellieri e Giovanni Mandato

1. Videoriprese in luoghi pubblici o aperti al pubblico

La materia delle riprese visive e delle prove che ne scaturiscono non è regolata specificamente dalla legge ed è stata da più parti rappresentata l'esigenza di un intervento del legislatore, anche rispetto alle riprese che non avvengano in ambito domiciliare e non incontrano perciò i limiti posti dall'art. 14 della Costituzione.

Nella pratica, il problema è quello di definire quando un luogo sia da considerare aperto al pubblico, esposto al pubblico e pubblico, incidendo tali definizioni sulle attività di videoripresa e sui limiti di ammissibilità delle stesse.

Si dice che il concetto di luogo aperto al pubblico si definisca con riferimento all'accessibilità di un numero indeterminato di persone, sia pur limitato o individuato in ragione dell'appartenenza a determinate categorie di soggetti che per qualsiasi motivo hanno la possibilità di accedervi (cfr. Corte Cass., sez. III, sent. 11 novembre 1999, n. 3771; Corte Cass., sez. IV, sent. 10 ottobre 1989, n. 13316; Corte Cass., sez. III, sent. 20 febbraio 1986, n.1567; Corte Cass., sez. III, sent. 20 ottobre 1983, n. 8616; Corte Cass., sez. V, sent. 6 ottobre 1972, n. 769).

Esso è pertanto uno spazio in cui chiunque può accedere, limitatamente e regolatamente (secondo regole che possono ad esempio essere un orario d'apertura, il pagamento di un

biglietto d'ingresso, l'obbligo d'iscrizione ad un'associazione che lo gestisca) stabilite dal proprietario (sia esso un privato o un ente pubblico) o da altre norme.
Discorso diverso va fatto, invece, per il luogo esposto al pubblico che è uno spazio dove lo spazio stesso, ciò che vi si trova e ciò che vi accade, può essere esposto alla visione di un generico pubblico di persone.
Infine, è da considerare pubblico il luogo cui può accedere chiunque senza alcuna particolare formalità, essendo quello il suo scopo ed utilizzo normale (ad esempio strade, piazze, giardini pubblici, spiagge demaniali).
La distinzione risulta importante non solo agli effetti di varie norme previste nel nostro ordinamento giuridico ma anche per la risoluzione di alcune problematiche affrontate dalla dottrina e dalla giurisprudenza che saranno di seguito esaminate. Si pensi al bagno di un locale pubblico, caratterizzato da una frequenza assolutamente temporanea e non stabile degli avventori, condizionata unicamente alla soddisfazione di un contingente bisogno personale (cfr. Corte Cass., sez. VI, sent. 10 gennaio 2003, n. 6962), ed in quanto la permanenza del soggetto in quel luogo non ha una durata tale da poter giustificare la tutela della esplicazione della vita privata che lì si svolge. Anche il *privé* di un locale pubblico non rappresenta un ambiente tutelato dall'art. 14 Cost. (cfr. Corte Cass., sez. unite, sent. 28 marzo 2006, n. 26795).
In tale contesto, per certi versi, lasciano sconcertati talune proposte di modifica legislativa (come quella contenuta nel disegno di legge governativo n. 1415 del 30 giugno 2008) per le quali la disciplina delle intercettazioni di conversazioni o comunicazioni dovrebbe trovare applicazione indistintamente per qualsivoglia forma di intercettazione «di immagini

mediante riprese visive», indipendentemente dal luogo di effettuazione e dunque anche in luoghi pubblici o aperti al pubblico.

Nell'attualità il ricorso a videoriprese in luoghi pubblici costituisce un sistema sempre più frequente, adottato sia da soggetti pubblici sia da privati.

Il legislatore ne ha dato prova autorizzando, con la legge n. 38/2009, i Comuni ad impiegare sistemi di videosorveglianza nei luoghi pubblici o aperti al pubblico, ai fini della tutela della sicurezza urbana. La promozione degli apparati di videosorveglianza nei Comuni si inserisce, in particolare, nell'ambito dei profili operativi dei Patti per la Sicurezza tra le Prefetture e le Istituzioni locali, quali modelli operativi capaci di favorire la collaborazione interistituzionale per la definizione condivisa di linee di azione in materia di sicurezza.

Basti pensare all'allarmante crescita dei reati che stanno inevitabilmente generando un diffuso stato di allarme sociale, o ancora a molteplici ed eterogenei episodi di criminalità realizzati in luoghi pubblici, come ad esempio nel corso di manifestazioni di protesta riprese dall'alto da elicotteri della Polizia.

Sempre più frequentemente, l'identificazione degli autori di siffatti episodi è stata possibile sulla base delle riprese effettuate attraverso telecamere installate lungo le strade cittadine a sorveglianza del traffico veicolare o, ancora, telecamere attivate da privati, da istituti bancari o riprese operate dalla polizia giudiziaria con finalità investigative per reprimere attività illecite di vario genere.

La videoripresa è certamente un mezzo di prova al quale non si può rinunciare per il fortissimo contenuto informativo che possiede e che, assai più di quanto possano esserlo gli altri

mezzi, lo fa portatore di certezze processuali, come ha riconosciuto in modo significativo lo stesso legislatore quando nell'art. 8, co. 1-*ter*, della legge n. 401/1989 e successive modificazioni, per i reati commessi in occasione di manifestazioni sportive, ha stabilito che «si considera in stato di flagranza colui il quale, sulla base di documentazione video fotografica o di altri elementi oggettivi dai quali emerga inequivocabilmente il fatto, ne risulta l'autore».

In mancanza di regole probatorie specifiche, la giurisprudenza e la dottrina hanno fatto riferimento alle disposizioni riguardanti altre prove e ai principi processuali per trarre indicazioni sulla disciplina applicabile alle riprese visive e alla utilizzabilità dei risultati ottenuti.

Sono emerse nel tempo opinioni non univoche, non solo sulla questione più complessa relativa alle riprese in ambito domiciliare, ma anche più in generale sulle caratteristiche del mezzo di prova e sulle norme alle quali deve essere ricondotto.

Il tema da affrontare propone dunque due questioni: quella relativa alle riprese visive in genere e quella, più specifica, relativa alle riprese visive in ambito domiciliare rispetto alle quali la mancanza di una regolamentazione normativa aggiunge ai dubbi sulla natura e la formazione della prova, altri e ben più consistenti dubbi sulla loro legittimità, data la doppia riserva, di legge e di giurisdizione, che l'art. 14, co. 2, della Costituzione ha posto a tutela del domicilio.

La giurisprudenza di legittimità ritiene pacificamente utilizzabili come prova le immagini tratte da riprese visive in luoghi pubblici, tanto se avvenute al di fuori del procedimento (si pensi alle videoriprese effettuate con impianti di videosorveglianza installati in esercizi pubblici), quanto se avvenute nell'ambito delle indagini di polizia giudiziaria.

Secondo un orientamento giurisprudenziale, le videoriprese effettuate in luoghi pubblici vanno incluse nella categoria dei documenti, dato che l'art. 234 c.p.p. comprende in tale categoria le rappresentazioni di fatti, persone o cose, mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo (cfr. Corte Cass., sez. V, sent. 18 ottobre 1993, n. 10309; Corte Cass., sez. III, sent. 15 giugno 1999, n. 11116; Corte Cass., sez. V, sent. 20 ottobre 2004, n. 46307).

Varie decisioni hanno fatto riferimento all'art. 234 c.p.p. anche per riconoscere il valore probatorio a riprese effettuate dalla polizia giudiziaria nel corso delle indagini preliminari (cfr. Corte Cass., sez. IV, sent. 13 dicembre 1995, n. 1344; Corte Cass., sez. V, sent. 25 marzo 1997, n. 1477; Corte Cass., sez. VI, sent. 10 dicembre 1997, n. 4997).

Secondo un diverso orientamento, le riprese visive effettuate in tali luoghi devono invece essere inquadrate nell'ambito delle prove atipiche, previste dall'art. 189 c.p.p., tanto se effettuate al di fuori del procedimento (cfr. Corte Cass. sez. V, sent. 26 ottobre 2001, n. 43491), quanto se avvenute nell'ambito delle indagini.

In particolare, con riferimento a questa ipotesi, si è detto che astrattamente il risultato delle riprese visive costituisce una prova documentale *ex* art. 234, co. 1, c.p.p. e, come tale, può essere utilizzato a fini probatori sebbene il Codice non ne disciplini le modalità di acquisizione e le regole di utilizzazione. Ciò in quanto il legislatore ha avuto di mira esclusivamente il documento cinematografico precostituito e non il frutto di una ripresa visiva costituente mezzo di ricerca della prova.

Secondo altro consolidato orientamento, le riprese visive costituirebbero una prova atipica (art. 189 c.p.p.) da acquisire con modalità che non si pongano in conflitto con norme di

legge e, qualora venissero effettuate in un luogo pubblico o aperto al pubblico, non incontrerebbero alcun limite perché la natura del luogo in cui si svolge la condotta implicherebbe una implicita rinunzia alla riservatezza. In tal senso si è orientata la Corte di Cassazione con sentenza del 16 marzo 2000, n. 7063.

Il principio è stato ribadito dallo stesso giudice di legittimità nel 2004 (cfr. Corte Cass., sez. VI, sent. 21 gennaio 2004, n. 37561) affermando che le riprese visive effettuate dalla polizia giudiziaria in luoghi pubblici o aperti al pubblico sono un mezzo atipico di ricerca della prova e non necessitano della preventiva autorizzazione della Autorità Giudiziaria, in quanto le garanzie previste dall'art. 14 della Costituzione si applicano solo per le captazioni visive che riguardano luoghi di privata dimora.

Nello stesso senso si è espresso con sentenza n. 24715 del 7 maggio 2004, con riferimento a riprese effettuate dalla polizia giudiziaria mediante telecamere installate in un garage condominiale aperto al transito di un numero indeterminato di persone.

Ipotesi più specifica è quella dell'attività captativa di immagini nell'ambito delle operazioni di osservazioni e pedinamento da parte della polizia giudiziaria, delle quali sono state ritenute acquisibili agli atti del dibattimento le relazioni di servizio documentative, mediante fotografie e filmati, delle attività svolte (cfr. Corte Cass., sez. II, sent. 26 marzo 1997, n. 4095).

2. Le videoriprese in ambito domiciliare

Il problema della legittimità delle videoriprese in ambito domiciliare e conseguentemente la loro utilizzabilità probatoria è stato più volte dibattuto in dottrina e in giurisprudenza.
Si premette che ai fini della configurazione del reato di violazione di domicilio, il concetto di privata dimora è più ampio di quello di casa d'abitazione, «comprendendo ogni luogo che pur non essendo destinato a casa d'abitazione, venga usato, anche in modo transitorio e contingente, per lo svolgimento di un'attività personale rientrante nella larga accezione di libertà domestica» (cfr. Corte Cass., sez. V, sent. 17 giugno 1985, n. 60101).
Sulla nozione di domicilio *ex* art. 14 della Costituzione, così come su quella di privata dimora *ex* art. 614 c.p., non vi sono in giurisprudenza e in dottrina indicazioni univoche e si dubita persino che sussista coincidenza tra l'oggetto della garanzia costituzionale e quello della tutela penale.
In linea di approssimazione, si è talvolta fatto riferimento da più parti prevalentemente al luogo utilizzato per lo svolgimento di manifestazioni della vita privata (riposo, alimentazione, studio, attività professionale, svago) di chi lo occupa ed anche ad una certa durata del rapporto tra il luogo e la persona. Secondo altri orientamenti, invece, rileverebbe il carattere esclusivo di tali luoghi (*ius excludendi alios*) ovvero la difesa della *privacy*. Si può aggiungere che la giurisprudenza tende ad ampliare il concetto di domicilio in funzione della tutela penale prevista dagli art. 614 e 614 *bis* c.p., mentre tende a circoscriverlo quando l'ambito domiciliare rappresenta un limite allo svolgimento delle indagini.

Sono significative espressioni dei diversi orientamenti le decisioni contrastanti sulla possibilità di riconoscere un domicilio anche nell'abitacolo di un'autovettura o nella *toilette* di un locale pubblico.

Secondo un primo orientamento giurisprudenziale, uno dei requisiti che consentono di riconoscere a un luogo il carattere di privata dimora è costituito da una certa «stabilità del rapporto tra il luogo e la persona che se ne serve», requisito che non è ravvisabile rispetto alla *toilette* di un locale pubblico (cfr. Corte Cass., sez. VI, sent. 10 gennaio 2003, n. 3443; Corte Cass., sez. VI, sent. 10 gennaio 2003, n. 6962 e, più di recente, Corte Cass., sez. VI, sent. 19 novembre 2005, n. 11654).

Nel caso oggetto di quest'ultima decisione erano state installate delle telecamere nella *toilette* di un centro di smistamento della corrispondenza ed erano stati ripresi alcuni dipendenti delle Poste mentre aprivano delle buste, ne esaminavano il contenuto e talvolta se ne appropriavano.

Rispetto a questa vicenda la giurisprudenza di legittimità (cfr. Corte Cass., sez. VI, sent. 19 novembre 2005, n. 11654) ha affermato che «il luogo in questione, caratterizzato da una frequenza assolutamente temporanea e condizionata unicamente dalla soddisfazione di un bisogno personale, non può essere assimilato ai luoghi di privata dimora di cui all'art. 614 c.p., che presuppongono una relazione con un minimo grado di stabilità con le persone che li frequentano e un soggiorno che, per quanto breve, abbia comunque una certa durata, tale da far ritenere apprezzabili l'esplicazione di vita privata che vi si svolge».

Ad opposte conclusioni è pervenuta invece la Corte di Cassazione con la sentenza del 16 marzo 2000, n. 7063. In questa decisione la Corte ha affermato che la nozione di domicilio

accolta dall'art. 14 Cost. è diversa e più ampia di quella prevista dall'art. 614 c.p., finendo per coprire «tutti i luoghi, siano o meno di dimora, in cui può aver luogo il conflitto di interessi che essa regola».

La tutela costituzionale, pertanto, si estenderebbe non solo alle private dimore e ai luoghi che, pur non costituendo dimora, consentono una sia pur «temporanea ed esclusiva disponibilità dello spazio, ma anche ai luoghi nei quali è temporaneamente garantita un'area di intimità e di riservatezza». Chi si reca nel bagno di un esercizio pubblico, ha osservato la Corte, non solo non rinunzia alla propria intimità e alla propria riservatezza ma, sia pur temporaneamente, può opporsi all'ingresso di altre persone.

Preliminarmente va rilevato che sulla questione delle videoriprese in ambiti domiciliari o comunque protetti *ex* artt. 14 e 15 della Costituzione, è intervenuta la Corte Costituzionale con sentenza del 24 aprile 2002, n. 135.

La problematica era stata in verità sollevata nel corso di un'udienza preliminare rispetto a riprese visive effettuate in base ad un provvedimento del P.M.

Il giudice, infatti, aveva dubitato della legittimità costituzionale degli artt. 189 e 266-271 c.p.p. e, segnatamente dell'art. 266, co. 2, c.p.p. nella parte in cui non estendono la disciplina delle intercettazioni delle comunicazioni tra presenti nei luoghi indicati dall'art. 614 c.p. alle riprese visive o videoregistrazioni effettuate nei medesimi luoghi.

La questione mirava a ottenere una pronuncia additiva che allineasse la disciplina processuale delle riprese visive in luoghi di privata dimora a quella delle intercettazioni di comunicazioni tra presenti nei medesimi luoghi.

La Corte Costituzionale ha sostenuto, al riguardo, che le riprese visive in ambienti domiciliari non siano precluse in modo assoluto dall'art. 14 Cost. e che il riferimento ivi operato solo alle ispezioni, alle perquisizioni e ai sequestri non è necessariamente espressivo dell'intento di «tipizzare» le limitazioni permesse, escludendo al contrario quelle non espressamente contemplate, poiché esso ben può trovare spiegazione nella circostanza che gli atti elencati esaurivano le forme di limitazione dell'inviolabilità del domicilio storicamente radicate e positivamente disciplinate all'epoca della redazione della Carta, non potendo evidentemente il Costituente tener conto di forme di intrusione divenute attuali solo per effetto dei progressi tecnici successivi.

Esclusa pertanto l'esistenza nella Carta costituzionale di un divieto assoluto della forma di intrusione domiciliare in questione, la Corte ha affermato che la ripresa visiva, quando è finalizzata alla captazione di comportamenti a carattere comunicativo (scambio di messaggi tra più soggetti in qualsiasi modo realizzati), ben può configurarsi in concreto come una forma di intercettazione di comunicazione tra presenti, alla quale è applicabile in via interpretativa la disciplina legislativa dell'intercettazione ambientale in luoghi di privata dimora.

Nel caso in cui si fuoriesca dalla videoripresa di comportamenti di tipo comunicativo non è possibile estendere la normativa dettata dagli art. 266 e s.s. c.p.p. alla captazione di immagini in luoghi tutelati dall'art. 14 della Costituzione, data la sostanziale eterogeneità delle situazioni: la limitazione della libertà e segretezza delle comunicazioni, da un lato; l'invasione della sfera della libertà domiciliare in quanto tale, dall'altro.

In conclusione, secondo la Corte, l'ipotesi della videoregistrazione che non abbia carattere di intercettazione di

comunicazioni potrebbe essere disciplinata soltanto dal legislatore, nel rispetto delle garanzie costituzionali dell'art. 14 Cost., ferma restando, per l'importanza e la delicatezza degli interessi coinvolti, l'opportunità di un riesame complessivo della materia da parte del legislatore stesso.

La decisione non è priva di ambiguità perché fa apparire inammissibili le riprese visive di comportamenti non comunicativi effettuati in ambito domiciliare ma la Corte non lo dichiara espressamente, come sarebbe stato naturale in un contesto in cui le riprese erano avvenute sul presupposto che fosse applicabile l'art. 189 c.p.p. e il giudice aveva messo in discussione la legittimità costituzionale di questa norma, oltre che degli artt. 266-271 c.p.p.

È chiaro che le regole di garanzia richieste dall'art. 14 Cost. e la disciplina dei casi e dei modi delle intrusioni domiciliari, non possono rinvenirsi nell'art. 189 c.p.p. dato che la disposizione non le contiene e, per la sua naturale genericità, non le potrebbe contenere, dovendo riferirsi a tutte le prove non disciplinate dalla legge.

In questo senso sembra doversi interpretare la sentenza della Corte che, con l'uso del condizionale nella parte conclusiva della seguente frase, «l'ipotesi in questione potrebbe essere disciplinata soltanto dal legislatore», fa intendere che allo stato una disciplina conforme all'art. 14 Cost. manca. Se ne dovrebbe dedurre che tale mancanza renda illegittima la ripresa visiva di un comportamento non comunicativo e inammissibile la prova che si fondi sui risultati della stessa ma questo la Corte non lo ha affermato, lasciando permanere un margine di incertezza.

Parte della dottrina, nel commentare la sentenza, ha sostenuto che sarebbe ammissibile l'uso processuale di documenti fotografici o cinematografici acquisiti illecitamente in quanto

relativi a comportamenti non comunicativi sino a quando l'art. 189 c.p.p. non sia dichiarato illegittimo nella parte in cui non esclude prove ottenute con interferenze indebite nella vita privata domestica.

Così, pure dopo la decisione della Corte Costituzionale, ha continuato a far riferimento all'art. 189 c.p.p. quella parte della giurisprudenza che riconosce valore probatorio alle videoregistrazioni di comportamenti non comunicativi avvenuti in ambito domiciliare (cfr. Corte Cass., sez. IV, sent. 18 giugno 2003, n. 44484).

Sul versante opposto, si è invece negata rilevanza probatoria alle videoregistrazioni in questione, facendo riferimento alla categoria delle prove incostituzionali. È stata al riguardo richiamata la sentenza della Corte Costituzionale n. 34 del 1973, con l'enunciazione del principio secondo il quale attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione e a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito.

Principio che tale sentenza ha ribadito con vigore, affermando che non possono validamente ammettersi in giudizio mezzi di prova che siano stati acquisiti attraverso attività compiute in violazione delle garanzie costituzionali poste a tutela dei fondamentali diritti dell'uomo e del cittadino.

A conclusione analoga sono pervenute anche le sezioni unite della Cassazione con le sentenze del 16 maggio 1996, del 13 luglio 1998 e del 23 febbraio 2000, le quali hanno fatto rientrare nella categoria delle prove sanzionate dall'inutilizzabilità non solo le prove oggettivamente vietate ma anche le prove formate o acquisite in violazione dei diritti soggettivi tutelati dalla legge e, a maggior ragione, quelle acquisite in violazione dei diritti

tutelati dalla Costituzione. Ipotesi, quest'ultima, sussumibile nella previsione dell'art. 191 c.p.p., proprio perché l'antigiuridicità di prove così formate o acquisite attiene alla lesione di diritti fondamentali e intangibili. Nella ricostruzione delle sezioni unite, quindi, la categoria delle prove incostituzionali si è combinata con quella della inutilizzabilità, essendosi ritenuto che i divieti ai quali fa riferimento l'art. 191, co. 1, c.p.p. siano non solo quelli sanciti dalle norme processuali ma anche quelli rinvenibili in altri settori dell'ordinamento e in primo luogo nella Carta costituzionale.

Pure questa ricostruzione, però, è tutt'altro che scontata perché altra parte della dottrina sostiene che l'art. 191 c.p.p., nel prevedere l'inutilizzabilità delle c.d. prove vietate, presuppone l'esistenza di divieti che, attenendo ad atti del procedimento, non possono che derivare da norme processuali.

Ma se il sistema processuale deve avere una sua coerenza, risulta difficile accettare l'idea che una violazione del domicilio, che la legge processuale non prevede, possa legittimare la produzione di materiale probatorio e che inoltre per le riprese di comportamenti non comunicativi possano valere le regole meno garantiste di quelle applicabili alle riprese di comportamenti comunicativi, regolate dagli artt. 266-271 del Codice di procedura penale.

Per queste, infatti, occorrerebbe l'autorizzazione del giudice, ammessa peraltro solo per determinati reati, in presenza di condizioni particolari e con vincoli di vario genere, presidiati dalla sanzione dell'inutilizzabilità, mentre per le altre sarebbe sufficiente il provvedimento del P.M. o la sola iniziativa della P.G. e mancherebbero regole di garanzia assimilabili a quelle previste per le intercettazioni di comunicazioni. Con la conclusione che mentre potrebbero essere, per varie ragioni,

colpite da inutilizzabilità le riprese di comportamenti comunicativi, ben difficilmente potrebbero esserlo le altre.

Per giungere alla determinazione che non possono considerarsi ammissibili, come prove atipiche, le videoregistrazioni di comportamenti non comunicativi effettuati in ambito domiciliare, non occorre però prendere posizione sul dibattito relativo agli effetti che la violazione delle norme costituzionali di garanzia può avere sull'attività probatoria prevista dal Codice, né stabilire se la sanzione di inutilizzabilità attenga solo alla violazione dei divieti stabiliti dalla legge processuale o riguardi anche la violazione di norme costituzionali o di altri rami dell'ordinamento e, segnatamente, di quello penale (si pensi alle intrusioni nell'ambito domiciliare *ex* art. 615 *bis* c.p.).

A ben vedere, questi aspetti non vengono in considerazione perché la soluzione passa direttamente attraverso l'interpretazione dell'art. 189 c.p.p. che è stato richiamato per legittimare processualmente l'attività probatoria incostituzionale.

Si vuole dire che il tema dell'inutilizzabilità come sanzione processuale per la violazione di regole di rango costituzionale riguarda, in linea di principio, le prove tipiche e non quelle atipiche.

Prima dell'ammissione le prove atipiche non sono prove, perciò se sorge questione sulla legittimità delle attività compiute per acquisire i materiali probatori che le fondano, ci si deve interrogare innanzitutto sulla loro ammissibilità, piuttosto che sulla loro utilizzabilità. È chiaro allora che le videoregistrazioni acquisite in violazione dell'art. 14 Cost. devono considerarsi inammissibili *ex* art. 189 c.p.p.

L'art. 189 c.p.p., infatti, in coerenza con l'art. 190, co. 1 c.p.p. (che impone al giudice di escludere le prove vietate dalla legge)

presuppone la formazione lecita della prova e soltanto in questo caso la rende ammissibile.
Si dice che in realtà il legislatore abbia inteso per lecite anche le attività probatorie «non disciplinate dalla legge» di cui all'art. 189 c.p.p. Ma si obbietta, giustamente, che con l'espressione «prova non disciplinata dalla legge» il Codice faccia riferimento alla mancanza di disciplina processuale della prova da assumere ed è perciò vero che non può considerarsi «non disciplinata dalla legge» la prova basata su attività che la legge vieta, come nel caso delle riprese visive di comportamenti non comunicativi avvenuti in ambito domiciliare.
Deve perciò concludersi che i risultati di tali riprese non possono essere acquisiti come prova atipica, non ponendosi di conseguenza alcun problema di utilizzabilità, non essendo ipotizzabile una loro ammissibilità.
Va infine rilevato che la Corte Costituzionale, con la sentenza n. 149/2008, ha sostanzialmente ribadito quanto già affermato nel 2002 con la sentenza n. 135. Nella fattispecie, il giudice rimettente aveva richiesto una sentenza additiva che estendesse la disciplina dell'art. 266, comma 2, c.p.p. (dettata per le intercettazioni di comunicazioni tra presenti) a qualsiasi captazione di immagini in luoghi di privata dimora, anche se non configurabile in concreto come forma di intercettazione di comunicazioni tra presenti.
Il P.M. del procedimento, in cui era stata sollevata la questione di costituzionalità, aveva infatti ritenuto a fondamento delle fonti di prova acquisite dalla P.G., che, in assenza di un espresso divieto o di un'esplicita regolamentazione da parte della legge ordinaria, delle riprese visive di comportamenti di tipo non comunicativo all'interno del domicilio, tale attività investigativa sarebbe esperibile anche a iniziativa della polizia

giudiziaria, con connessa utilizzabilità processuale dei relativi risultati.

L'esigenza prospettata dal giudice rimettente di sottoporre a un provvedimento autorizzatorio giurisdizionale anche le riprese visive di comportamenti non comunicativi in luoghi di privata dimora (esigenza tanto più avvertibile a fronte del progresso tecnologico, che accresce sempre più le possibilità di *inspicere* nel domicilio tramite strumenti altamente sofisticati) avrebbe imposto, dunque, la pronuncia additiva invocata.

In particolare, l'evidenziata assenza di disciplina, secondo il remittente si risolverebbe in un *vulnus* delle norme costituzionali poste a tutela della libertà personale, dell'inviolabilità del domicilio e della libertà di comunicazione.

Si determinerebbe, fra l'altro, un'inversione della «sequenza di garanzia» nel senso che, alla luce di alcuni orientamenti giurisprudenziali, il pubblico ministero e la stessa polizia giudiziaria potrebbero captare immagini all'interno di luoghi di privata dimora senza alcuna autorizzazione giurisdizionale; se poi risultassero essere state captate delle «comunicazioni», gli esiti del mezzo investigativo sarebbero inutilizzabili, altrimenti si sarebbero ottenute prove documentali utilizzabili.

Neppure, però, potrebbe accettarsi che, nella perdurante inerzia del legislatore, l'individuazione dei confini di legittimità delle molteplici forme di intrusione nei luoghi di privata dimora resti affidata «alla mera interpretazione giurisprudenziale»; e ciò soprattutto ove si tenga conto della rapida evoluzione tecnologica che rende aggredibile il domicilio con strumenti sempre più sofisticati, quali le immagini satellitari a elevatissimo livello di definizione o la termografia a raggi infrarossi.

La Corte Costituzionale ha però affermato, rigettando la questione di legittimità sollevata nel caso di specie, che in mancanza di una norma che consenta e disciplini il compimento dell'attività in parola (soddisfacendo la doppia riserva, di legge e di giurisdizione, alla quale l'art. 14, co. 2, Cost., subordina l'eseguibilità di atti investigativi nel domicilio) l'attività stessa dovrebbe ritenersi radicalmente vietata, proprio perché lesiva dell'inviolabilità del domicilio, sancita dal primo comma del suddetto art. 14 Cost. I risultati delle riprese effettuate in violazione del divieto rimarrebbero, quindi, inutilizzabili. Si tratta, in effetti, di una soluzione interpretativa già sostenuta dalle sezioni unite della Corte di Cassazione (cfr. sentenza 28 luglio 2006, n. 26795).

In conclusione, in assenza di una riforma legislativa, da molti auspicata, il vuoto normativo concernente alcuni aspetti delle videoriprese con particolare riferimento a quelle concernenti comportamenti non comunicativi, rimane provvisoriamente "colmato" dalle sezioni unite della Cassazione con l'enunciazione di principi più articolati, fondati su argomentazioni in parte "creative". In pratica, si è affermato che:

a) se la ripresa visiva viene effettuata da privati, la stessa è consentita solo in luoghi pubblici o aperti al pubblico e i relativi risultati, in quanto acquisiti fuori dal procedimento penale, vanno considerati come "documenti" *ex* art. 234 c.p.p.;

b) se la ripresa visiva viene, invece, effettuata dalla polizia giudiziaria occorre distinguere a seconda della natura dei comportamenti filmati. Se i comportamenti filmati sono di tipo comunicativo, è sempre necessaria l'applicazione della disciplina delle intercettazioni. Se, invece, i comportamenti filmati sono di tipo non comunicativo, la polizia giudiziaria,

anche d'iniziativa, può senz'altro disporne l'effettuazione in luoghi pubblici o aperti al pubblico, dovendosi qualificare il relativo strumento in termini di prova atipica *ex* art. 189 c.p.p.;

c) se, però, la ripresa di comportamenti non comunicativi riguarda luoghi protetti dal diritto alla riservatezza, tale attività di indagine non è mai consentita, perché comporterebbe una violazione del diritto alla inviolabilità del domicilio di cui all'art. 14 Cost. in una situazione in cui la violazione del domicilio non è regolata dalla legge processuale, non essendo applicabile, in siffatte ipotesi, l'art. 189 c.p.p. che riguarda sì l'attività probatoria atipica in quanto non disciplinata dalle legge, ma che, comunque, non deve essere vietata dalla legge stessa.

È stata dunque definitivamente superata la precedente concezione secondo cui le riprese visive, eseguite dagli inquirenti in luoghi pubblici o aperti al pubblico, costituirebbero sempre meri documenti (cfr. Corte Cass., sez. VI, sent. 10 dicembre 1997, n. 210579; Corte Cass., sez. V, sent. 25 marzo 1997, n. 208137).

Il problema delle videoriprese in ambiti domiciliari o di luoghi di privata dimora si è posto per quelle effettuate in strutture carcerarie e per quelle inerenti i c.d. spazi condominiali.

Con particolare riferimento al primo aspetto, la tutela del domicilio si è affievolita per le strutture carcerarie, essendo ritenuta ammissibile e legittima l'intercettazione delle conversazioni e delle riprese di comportamenti (comunicativi) dei detenuti anche se non sussiste il fondato timore che all'interno della cella si stia svolgendo attività criminosa, come richiesto generalmente dalle norme sulle intercettazioni per i luoghi di privata dimora laddove non vengano in rilievo reati di criminalità organizzata o in materia di stupefacenti. La

Suprema Corte, infatti, ha recisamente escluso «che l'ambiente carcerario, sia esso la cella o la sala colloqui dell'istituto di detenzione, rientri nel concetto di privata dimora nel possesso e nella disponibilità dei detenuti, in quanto è pur sempre un luogo sottoposto ad un diretto controllo dell'Amministrazione penitenziaria che su di esso esercita la vigilanza ed a cui soltanto compete lo *ius excludendi*» (cfr. Corte Cass., sez. I, sent. 5 agosto 2008, n. 241228).

Per quanto concerne, invece, il più delicato aspetto degli spazi condominiali, va preliminarmente rilevato che il delitto di illecite interferenze nella vita privata, previsto dall'art. 615 *bis* del Codice penale, richiede un duplice presupposto fattuale, rappresentato dalla indebita interferenza in uno dei luoghi indicati nell'art. 614 c.p. e dall'attinenza delle notizie o immagini, così indebitamente captate, alla vita privata che si svolga in quei luoghi.

La *ratio* della norma incriminatrice è, come risulta anche dalla sua collocazione sistematica, quella di salvaguardare la libertà domestica, assicurando che la sfera ambientale in cui questa si svolge resti al riparo da qualsiasi intromissione altrui (realizzata mediante l'uso di strumenti di ripresa visiva o sonora atti a captare notizie od immagini) che possa attentare alla pace, alla tranquillità e alla sicurezza di quell'ambito di riservatezza in cui si esplica la personalità (cfr. Corte Cass., sez. V, sent. 4 giugno 2001, n. 35947).

La fattispecie incriminatrice è stata d'altronde inserita dalla legge n. 98/1974 in un contesto che offriva risposta alla sentenza della Corte Costituzionale n. 34/1973, disciplinando positivamente le intercettazioni telefoniche mediante l'introduzione dei nuovi art. 226 *bis* e 226 *sexies* del c.p.p. ed era espressamente richiamata dall'art. 226 *quinquies*, che

sanzionava, a pena di nullità assoluta, l'utilizzazione di intercettazioni ottenute nei modi di cui all'art. 615 *bis* c.p.

La dottrina ha concordemente sottolineato come emergesse, dai lavori preparatori, la ponderata decisione di legare la nuova fattispecie di reato all'art. 14 della Costituzione e, sotto il profilo della legge ordinaria, all'art. 614 c.p., elaborandola quale prolungamento della fattispecie di violazione di domicilio già sanzionata dall'art. 614 del Codice penale.

La previsione incriminatrice trova radice, dunque, nella convinzione che sfera privata e domicilio sono termini correlativi: l'inviolabilità del domicilio, fungendo da strumento di tutela di una manifestazione specifica della vita privata e solo in relazione a tale manifestazione specifica, risultando circoscritta la tutela penale esclusiva e diretta riconosciuta dall'art. 615 *bis* c.p.

È stato così rilevato in dottrina che le notizie e immagini la cui conoscenza esclusiva è protetta dalla predetta norma, non possono che essere le medesime la cui conoscenza esclusiva è tutelata in via solo eventuale dall'art. 614 c.p. che difende l'indebita intrusione nella vita privata attuata mediante la penetrazione nel domicilio *invito domino*.

Anche per l'integrazione del delitto di cui all'art. 615 *bis* c.p. è stato ritenuto necessario l'uso di apparecchiature in grado di cagionare quella medesima offesa alla vita privata, arrecata dalla cognizione diretta di notizie o immagini da parte di un estraneo che si trovi fisicamente nel domicilio, escludendosi che la percezione di alcune notizie o immagini mediante l'utilizzo di strumenti di ripresa possa essere punita laddove la loro percezione diretta sia invece lecita.

Secondo alcuni, invece, sarebbe proprio l'utilizzo di strumenti di ripresa a rendere illecita l'attività di osservazione di

immagini all'interno di luoghi che rientrano nella nozione di domicilio, ma la cui vista è facilmente accessibile dall'esterno (terrazze, balconi, cortili).

La stessa giurisprudenza ha sostenuto che non può escludersi la sussistenza del reato laddove esista un diritto di veduta, giacché tale diritto incontra limiti civilistici solo in relazione alla possibilità di nuove aperture e non può confondersi con un diritto di documentazione dei fatti di vita privata altrui, concepibile solo con il consenso dell'avente diritto, ovvero in presenza di cause di giustificazione (cfr. Corte Cass., sez. V, sent. 23 gennaio 2001, n. 8573) o quando la videoripresa insista su aree condominiali a uso e visibilità comune (cfr. Corte Cass., sez. V, sent. 15 ottobre 2004, n. 16189) o, ancora, in situazioni in cui l'autore della violazione abbia egli stesso la disponibilità del domicilio a causa del suo rapporto di convivenza coniugale (cfr. Corte Cass., sez. V, sent. 8 novembre 2006, n. 39827).

Del resto, la stessa Corte Costituzionale con la sentenza n. 349/1999 aveva sostenuto, con riferimento al bilanciamento tra esigenze di riservatezza e uso normale del diritto di proprietà privata, che l'acquisto del diritto di veduta in ambiti domiciliari confinanti giustifica la corrispondente compressione dell'altrui diritto alla riservatezza.

Le sezioni unite della Cassazione avevano già affermato, con la sentenza n. 26795/2006, che l'art. 14 della Costituzione tutela il domicilio sotto due distinti aspetti: come diritto di ammettere o escludere dal luogo in cui si svolge la vita intima e come diritto alla riservatezza su quanto si compie nei medesimi luoghi.

Nel caso di riprese visive, la sfera di riservatezza verrebbe lesa attraverso l'utilizzo di strumenti tecnici, anche senza la necessità di un'intrusione fisica.

Pertanto, affinché scatti la protezione dell'art. 14 della Costituzione non è sufficiente che un determinato comportamento sia realizzato in un luogo di privata dimora ma occorre anche che esso avvenga in condizioni tali da renderlo non visibile a terzi.

E così se l'azione, pur svolgendosi in luogo di privata dimora, può essere liberamente osservata dagli estranei, senza ricorrere a particolari accorgimenti, il titolare del domicilio non può accampare una pretesa alla riservatezza.

Analogamente, autorevole dottrina affermava, con riferimento all'art. 226 *quinquies* c.p.p. che erano inammissibili le prove ottenute mediante riprese indebite attraverso spie elettroniche clandestinamente introdotte nel luogo di privata dimora; di contro, sarebbero stati ammissibili immagini o suoni captati *ab extra*. Si è detto al riguardo che lo *home watching* è indiscreto ma non indebito.

In giurisprudenza si sostiene anche che deve escludersi un'intrusione, tanto nella privata dimora quanto nel domicilio, con riferimento a videoriprese aventi ad oggetto comportamenti tenuti in spazi di pertinenza nell'abitazione di taluno ma di fatto non protetti dalla vista degli estranei, ritenendosi per tale ragione questi spazi assimilabili ai luoghi esposti al pubblico. Sarebbero percettibili dall'esterno i comportamenti in essi tenuti, venendo meno le ragioni della tutela domiciliare.

Con particolare riferimento alle riprese visive effettuate in spazi condominiali, la Suprema Corte di Cassazione, con la sentenza n. 44156/2008, ha affermato la liceità dell'osservazione elettronica su zone ad uso comune non protette, benché effettuata contro la volontà dei condomini.

Nella fattispecie esaminata dal giudice di legittimità, appariva evidentemente che la ripresa effettuata dal ricorrente con proprie telecamere sull'ingresso comune dell'edificio in cui dimorava, sul vialetto d'accesso e su di una piccola parte esterna di proprietà di altri condomini, non era stata effettuata né clandestinamente né fraudolentemente e non era neppure idonea a cogliere di sorpresa i predetti in momenti in cui potevano credere di non essere osservati.

La Corte ha pertanto posto il principio secondo il quale la videoripresa delle aree comuni di proprietà non può ritenersi in alcun modo indebitamente invasiva della sfera privata dei condomini, ai sensi dell'art. 615 *bis* c.p., giacché la indiscriminata esposizione alla vista altrui di un'area che costituisce pertinenza domiciliare ma che non è deputata a manifestazioni di vita privata esclusive, è incompatibile con una tutela penale della riservatezza, anche ove risultasse che manifestazioni di vita privata in quell'area siano state in concreto realizzate.

Discorso diverso è, invece, quello concernente l'installazione di telecamere che benché osservino parti esterne di balconi o davanzali, riescano, grazie alla loro potenzialità di *focus*, a penetrare il luogo di privata dimora osservandone i comportamenti realizzati in base a una presunzione di riservatezza. Riprese di tale specie sarebbero da considerarsi evidentemente illecite e ben integrerebbero la fattispecie prevista e punita dall'art. 615 *bis* c.p. Sarebbero, peraltro, sottoposte al regime previsto dal Codice della *privacy* e ai provvedimenti emanati in materia dal garante per la protezione dei dati personali.

3. L'attività di videoripresa nei locali *privé*

L'effettuazione di videoriprese in luoghi di privata disponibilità ha posto problematiche di ordine giuridico con particolare riferimento ai camerini di locali commerciali.

In particolare, ci si è chiesti se i c.d. *privé*, ove avvengono incontri privati, possano o meno considerasi un domicilio e la videoripresa di comportamenti comunicativi rilevati in tale ambito debbano di conseguenza ottenere l'autorizzazione dell'A.G.

Che la nozione di domicilio accolta dall'art. 14 Cost. sia più ampia di quella desumibile dall'art. 614 c.p. è opinione prospettata in dottrina ma non incontrastata; in ogni caso, quale che sia il rapporto tra le due disposizioni, il concetto di domicilio non può essere esteso fino a farlo coincidere con un qualunque ambiente che tende a garantire intimità e riservatezza.

Non c'è dubbio che il concetto di domicilio individui un rapporto tra la persona e un luogo, generalmente chiuso, in cui si svolge la vita privata, in modo anche da sottrarre chi lo occupa alle ingerenze esterne e da garantirgli quindi la riservatezza. Ma il rapporto tra la persona e il luogo deve essere tale da giustificare la tutela di questo anche quando la persona è assente.

In altre parole, la vita personale che vi si svolge, anche se per un periodo di tempo limitato, fa sì che il domicilio diventi un luogo che esclude violazioni intrusive, indipendentemente dalla presenza della persona che ne ha la titolarità, perché il luogo rimane connotato dalla personalità del titolare, sia o meno questi presente.

Diversamente, nel caso della *toilette* e nei casi analoghi, il luogo in quanto tale non riceve alcuna tutela. Chiunque può entrare in una *toilette* pubblica, quando è libera, e la polizia giudiziaria ben potrebbe prenderne visione indipendentemente dall'esistenza delle condizioni processuali che legittimano attività ispettive. Perciò, con ragione, la giurisprudenza ha introdotto il requisito della "stabilità", perché è solo questa, anche se intesa in senso relativo, che può trasformare un luogo in un domicilio, nel senso che può fargli acquistare un'autonomia rispetto alla persona che ne ha la titolarità.

Deve quindi concludersi che una toilette pubblica non può essere considerata un domicilio, neppure nel tempo in cui è occupata da una persona.

È vero però che una *toilette* pubblica o un camerino, se non sono un domicilio, sono tuttavia un luogo che dovrebbe tutelare l'intimità e la riservatezza delle persone, e che quindi, ai fini delle riprese visive, non possono essere trattati come un luogo pubblico o esposto al pubblico. La caratteristica e le funzioni di questi luoghi, se da un lato, come si è detto, non giustificano un ampliamento del concetto di domicilio fino a ricomprenderli in esso, dall'altro non consentono che le attività che vi si svolgano possano rimanere esposte a qualunque genere di intrusioni.

Si ritiene comunemente che anche il diritto alla riservatezza o più in generale il diritto al rispetto della vita privata abbia un riconoscimento costituzionale nell'art. 2 Cost., al quale si aggiungono come norme più specifiche l'art. 8 della Convenzione europea dei diritti dell'uomo e l'art. 17 del Patto internazionale sui diritti civili e politici. Sul piano costituzionale, tuttavia, il diritto alla riservatezza non gode di una tutela analoga a quella apprestata dall'art. 14 Cost. per il domicilio ed è per questa ragione che anche in mancanza di una

disciplina specifica le riprese visive che lo sacrificano devono ritenersi consentite e suscettibili di utilizzazione probatoria a norma dell'art. 189 c.p.p.

In altre parole quell'applicazione dell'art. 189 c.p.p. che erroneamente una parte della giurisprudenza ha ritenuto di poter fare con riferimento a riprese visive in ambito domiciliare è invece possibile per le riprese effettuate in luoghi che pur non costituendo un domicilio vengono usati per attività che si vogliono mantenere riservate.

Sono queste, e non quelle in ambito domiciliare, le riprese che possono avvenire sulla base di un provvedimento motivato dell'A.G., sia essa il P.M. o il giudice; provvedimento che non può mancare perché, come è stato già affermato dalla giurisprudenza, è necessario che la limitazione del diritto alla riservatezza venga disposta con decreto motivato dell'Autorità Giudiziaria (cfr. Corte Cass., sez. IV, sent. 16 marzo 2000, n. 562).

Alcuni autori hanno assimilato le riprese visive alle ispezioni e ai rilievi. Questi in realtà sono mezzi che si differenziano dalle riprese visive sia perché non hanno carattere continuativo, sia soprattutto perché nella disciplina processuale presuppongono una esecuzione palese (le riprese visive sono invece nascoste) ma l'assimilazione dà conto della ragione per cui anche le riprese visive devono essere legittimate da un provvedimento dell'A.G.

Questo, infatti, rappresenta secondo la Corte Costituzionale un livello minimo di garanzia (cfr. sentt. n. 81/1993 e n. 281/1998) e ad esso si è fatto riferimento anche per regolare, in mancanza di una specifica normativa, l'acquisizione dei tabulati contenenti i dati identificativi delle comunicazioni telefoniche (cfr. Corte Cass., sez. unite, sent. 23 febbraio 2000, n. 6).

È da aggiungere che nel motivare il provvedimento che dispone le riprese visive, l'A.G. non potrà fare a meno di identificare lo scopo di queste, vale a dire gli elementi probatori che attraverso l'atto intrusivo essa ritiene che possano venire utilmente acquisiti.

Orbene, le riprese visive nei camerini, i c.d. *privé*, non sono inibite, perché i camerini non costituiscono un domicilio. Essi tuttavia costituiscono un luogo nel quale si svolgono attività destinate a rimanere riservate, rispetto alle quali indagini con le modalità intrusive richiedono un congruo provvedimento giustificativo.

In mancanza di un provvedimento autorizzativo è da ritenere che la prova atipica, costituita dalle videoregistrazioni effettuate, si prospetti carente di un presupposto di ammissibilità e che quindi non possa essere utilmente addotta a giustificazioni di una prognosi di responsabilità sorretta da gravi indizi di colpevolezza.

4. Il comportamento non comunicativo e la comunicazione con se stessi: spunti di riflessione

Appare opportuno, in via preliminare, operare una distinzione tra comportamenti comunicativi e non comunicativi captati in luogo pubblico, aperto al pubblico o esposto al pubblico, in coerenza con i recentissimi orientamenti della giurisprudenza di legittimità e costituzionale.

Nessun problema particolare si pone con riferimento alle c.d. videoriprese di comportamenti non comunicativi in un luogo pubblico, aperto al pubblico o esposto al pubblico. Deve, infatti, escludersi decisamente che tali attività investigative possano essere definite come ispezioni (artt. 244-246 c.p.p.) o come

rilievi sulle persone effettuati dalla polizia giudiziaria a norma dell'art. 354, co. 3, c.p.p., trattandosi con evidenza di operazioni da svolgersi in segretezza e normalmente in maniera continuativa che, del resto, non potrebbero essere attuate (positivamente) rispettando le garanzie difensive imposte dalle citate disposizioni. Deve pertanto ravvisarsi, in tale tipo di attività investigativa, una c.d. prova innominata o atipica, dovendosi interpretare il disposto dell'art. 189 c.p.p. «in senso ampio, come comprensivo dei mezzi di ricerca della prova e dei mezzi di indagine non previsti dalla legge».

Le condizioni alle quali l'art. 189 c.p.p. subordina l'ammissibilità delle prove atipiche (ossia l'assenza di pregiudizi per la libertà morale delle persone coinvolte e l'obbligo del giudice di sentire le parti sulle modalità acquisitive della prova) non appaiono di ostacolo all'esecuzione di videoriprese nascoste come strumento (atipico) di indagine. Non si verifica, infatti, nessuna lesione di diritti individuali «inviolabili», cioè aggredibili unicamente nel rispetto della riserva di legge e di giurisdizione.

Se le videoriprese nascoste vengono operate in luogo pubblico, aperto od esposto al pubblico, al fine di documentare una "condotta comunicativa" tutelata *ex* art. 15 Cost., la stessa attività investigativa si trasforma, invece, in una vera e propria video intercettazione ed è dunque necessario, per l'uso probatorio del documento visivo, che sia stata autorizzata *ex* art. 266 c.p.p., come qualunque altra intercettazione di colloqui (*rectius*, comunicazioni) tra persone presenti, intercorsi in luogo diverso dal domicilio. L'art. 15 Cost., infatti, assicura l'inviolabilità della segretezza unicamente delle c.d. comunicazioni riservate (cioè effettuate con modalità che

dimostrino l'intento del mittente di consentirne la percezione a una sfera limitata di destinatari).

Diverso e più complesso risulta il problema delle videoriprese effettuate invece in ambito domiciliare ovvero in luoghi di privata dimora equiparati.

La definizione di comportamenti non comunicativi è desumibile in parallelo, considerando in via preliminare ciò che la giurisprudenza definisce come comunicazione.

Già nel 1997 la giurisprudenza di legittimità (cfr. Corte Cass., sez. VI, sent. 10 novembre 1997) affermò che «la nozione di comunicazione consiste nello scambio di messaggi fra più soggetti, in qualsiasi modo realizzati (ad esempio, tramite colloquio orale od anche gestuale)» e che «l'attività di intercettazione è appunto diretta a captare tali messaggi».

Nel corpo della medesima pronunzia il Supremo Collegio sostenne, poi, che attività del tutto differente dall'usuale azione intercettativa è quella di «captare immagini relative alla mera presenza di cose o persone o ai loro movimenti, non funzionali alla captazione di messaggi».

All'evidenza emerse, quindi, che nella prima fattispecie lo scopo era quello di percepire sul piano uditivo ed interpretativo conversazioni, onde inferire da esse contenuti illeciti (già di per sé prove di reato oppure prodromiche a successivi ulteriori condotte criminose anche di terzi), mentre nella seconda ipotesi l'attività di indagine, prettamente visiva, era finalizzata a provare la presenza di uno o più soggetti in un luogo, in un preciso momento (circostanza che può fungere da elementi di conferma di altri e diversi elementi di prova).

Si è già detto che alle riprese visive concernenti comportamenti non comunicativi in ambiti domiciliari o di privata dimora non si applica la disciplina prevista dagli artt. 266 e ss. c.p.p. e che

la Corte Costituzionale ha da ultimo ribadito la necessità di una disciplina legislativa al riguardo, in coerenza con la riserva assoluta di legge sancita dagli artt. 14 e 15 della Costituzione. Va altresì rilevato che riprese di comportamenti non comunicativi, in ambiti "protetti" sotto il profilo della riservatezza, presuppongono necessariamente, a monte, un'autorizzazione del Giudice alla captazione di comportamenti comunicativi nell'ambito di un'attività di indagine, qualificandosi, diversamente, illecite costituenti reato e non ammissibili quali prove *e*x art. 191 c.p.p.

Orbene, *quid iuris* se nel corso delle operazioni di videoripresa in ambito domiciliare saranno captate immagini relative a comportamenti non comunicativi, che non evidenziano gestualità od esternazioni relazionali? Ovviamente il problema si pone analogamente per le intercettazioni tra presenti nel domicilio o luoghi equiparati, laddove la captazione sonora non sia accompagnata dallo strumento investigativo della registrazione di immagini.

La giurisprudenza di legittimità, si è già detto, ha più volte ribadito il principio della inammissibilità delle prove atipiche assunte in violazione di norme procedurali, sostanziali e dei principi costituzionali. Tale consolidato orientamento condurrebbe a ritenere che quanto acquisito in relazione a condotte non comunicative poste in essere da un soggetto nel luogo osservato debba essere ritenuto inutilizzabile in quanto lesivo dell'art. 14 Cost. e, come tale, non utilizzabile neanche in sede cautelare (cfr. Corte Cass., sez. unite, sent. 28 luglio 2006, n. 26795). Pertanto, nel caso di riprese visive di comportamenti di tipo non comunicativo, venendo in considerazione soltanto l'intrusione nel domicilio in quanto tale e non l'intercettazione delle comunicazioni interpersonali, non sarebbe possibile

estendere alla captazione delle immagini nei luoghi tutelati dall'art. 14 Cost., la normativa dettata dagli artt. 266 e ss. c.p.p., data la sostanziale eterogeneità delle situazioni: l'invasione della sfera della libertà domiciliare in quanto tale, da un lato; la limitazione della libertà e segretezza delle comunicazioni, dall'altro. La Corte Costituzionale, pur recependo la detta interpretazione in ordine alle riprese visive di comportamenti non comunicativi in ambiente "riservato", non ritenendo però di affrontare la questione controversa, se comunque vi possa o no essere spazio per un provvedimento autorizzatorio della autorità giudiziaria, ha ritenuto di dover ammetterne comunque l'utilizzabilità, quando partecipe dell'attività videoripresa sia un soggetto titolare del diritto di essere presente nel luogo "riservato". In tal caso, infatti, non essendo configurabile alcuna intrusione ingiustificata nell'altrui domicilio, la videoripresa di comportamenti non comunicativi, anche se non autorizzata dall'autorità giudiziaria, sarebbe utilizzabile come prova atipica, non sussistendo alcuna lesione dei principi espressi dall'articolo 14 della Costituzione (in termini, cfr. anche Corte Cass., sez. II, sent. 13 dicembre 2007). Da queste premesse, nella specie, è stata ritenuta utilizzabile la videoripresa effettuata sul luogo di lavoro, da intendere come "domicilio" per l'arco temporale della giornata lavorativa, da una persona che si assumeva vittima di vessazioni e molestie sessuali da parte del proprio datore di lavoro.

Il problema si pone tuttavia per quelle forme di comunicazione c.d. con se stessi, che non possono integrare vere e proprie fattispecie di comportamenti comunicativi, concernenti potenziali fonti di prova di estrema rilevanza in relazione a procedimenti penali da cui è generata l'attività di captazione

elettronica. Si pensi alle espressioni verbali di auto accusa esternate dal soggetto dinanzi allo specchio dell'abitazione sorvegliata o alla redazione di uno scritto di proprio pugno con cui lo stesso ammette ogni responsabilità in ordine all'evento di reato e che la telecamera installata ben riesce a visualizzare attraverso un particolare *focus* o raggio di azione.

Per quanto concerne le esternazioni verbali, evidentemente non possono configurarsi quali comunicazioni che presuppongono necessariamente una relazione tra due o più soggetti. Non importa se la comunicazione sia orale o gestuale, ma occorre necessariamente una pluralità soggettiva che si ponga in relazione. Discorso diverso andrebbe effettuato, invece, per quanto concerne la redazione di documenti. Al riguardo va rilevato che soltanto una valutazione effettuata *ex post* dal P.M. ed eventualmente dal giudice, potrà attribuire dignità probatoria alla captazione visiva del manoscritto redatto nel luogo di privata dimora. Quest'ultimo, infatti, non avrà valore di prova e sarà considerato prova atipica inutilizzabile laddove non sia neppure indirizzato *ad incertam personam*. In altri termini, mentre la redazione di un documento scritto dall'osservato che non è destinato ad alcun soggetto (si pensi alla scrittura di una pagina di un diario segreto) sarà valutabile quale comportamento non comunicativo, discorso diverso dovrebbe effettuarsi se il cartaceo visualizzato nella ripresa sia destinato ad altri soggetti (si pensi ad una lettera redatta dal soggetto, ma non sottoscritta, che si accusa del reato o che incolpa taluno dei fatti oggetto del procedimento, perché a conoscenza dei medesimi). In tale fattispecie, la condotta ha invero natura comunicativa anche se l'interrelazione richiesta dalla giurisprudenza di legittimità non è immediata.

Al contrario, va sicuramente riconosciuta natura di comunicazione allo scambio silenzioso di c.d. pizzini da un soggetto all'altro che, per timore di essere ascoltato, ha preferito tale modalità di interrelazione, ignorando l'esistenza di parallele attività di osservazione.

Nulla impedisce ovviamente di attribuire alle circostanze non destinate a ricevere dignità probatoria quanto meno un'utilità investigativa, potendo la polizia giudiziaria porre in essere tempestive attività di assicurazione della prova a mezzo sequestri documentali nelle forme e nei limiti previsti dal Codice di procedura penale, potendo, nondimeno, prendere spunto da quanto osservato o ascoltato per ogni utile prosecuzione delle indagini.

Analogamente è a dirsi per tutte quelle ipotesi in cui venga consumata o lavorata sostanza stupefacente nel luogo privato monitorato. Anche in tal caso la condotta non comunicativa sarà necessariamente estrapolata dall'attività di intercettazione e resa inutilizzabile al termine delle indagini preliminari.

L'assenza di una disciplina legislativa sulle videoriprese investigative, come si è visto, ha determinato in più occasioni l'intervento prudenziale della giurisprudenza di legittimità e della stessa Corte Costituzionale. Le copiose sentenze sopra commentate hanno in realtà inteso salvaguardare l'inviolabilità del domicilio e la segretezza delle comunicazioni in ossequio ai dettati della nostra Costituzione negli art. 14 e 15. E se da una parte si è proceduto alla fondamentale equiparazione delle videoriprese in ambiti protetti alla disciplina delle intercettazioni tra presenti, estendendo l'applicazione delle norme degli artt. 266 e ss. c.p.p. per i comportamenti comunicativi, dall'altra sono state evidentemente penalizzate tutte quelle altre fattispecie di condotte non comunicative, che

potrebbero avere un'eccezionale utilità investigativa laddove si consideri che le strumentazioni tecnologiche di ascolto e osservazione consentono oggi di ottenere maggiore qualità di suoni e immagini, sino a qualche tempo fa inimmaginabili.

De iure condendo è pertanto auspicabile un rapido intervento del legislatore che scriva in tal modo la parola fine sull'annosa questione dei comportamenti non comunicativi, precisando limiti di ammissibilità ed utilizzabilità degli stessi. Ciò consentirebbe di evitare la perdita di prezioso materiale investigativo assunto, soprattutto in un'epoca, come quella attuale, connotata da conoscenze collettive delle strumentazioni di indagini a disposizione e, pertanto, da meticolose attenzioni da parte della criminalità organizzata alle captazioni elettroniche operate dalla P.G. in luoghi di privata disponibilità, preferendo la stessa adottare proprio tutte quelle condotte di tipo non comunicativo al fine esclusivo di eludere intercettazioni telefoniche o tra presenti.

CAPITOLO III
L'integrazione tra biometria e videosorveglianza: un *case study*

di Angela Catapano e Fabrizio Mancini

1. La biometria, il processo biometrico e le tecnologie biometriche nella videosorveglianza

1.1. La biometria

Con il termine "biometria", dal greco *bios* (vita) e *metros* (misura), seppure usato anche in altri contesti scientifici, nell'odierna accezione informatica si intende l'identificazione automatica o la verifica dell'identità di un soggetto sulla base di caratteristiche fisiche e/o comportamentali. Bio-metria significa, infatti, "misurare la vita". Si tratta, dunque, di una disciplina che considera statisticamente i fenomeni biologico-vitali dal punto di vista quantitativo.

Possiamo classificare la biometria in fisica e comportamentale.

La biometria fisica è basata su dati derivati dalle misure effettuate sulle caratteristiche fisiche di una persona. Tra queste, si possono menzionare la verifica delle impronte digitali, l'analisi dell'immagine delle dita, il riconoscimento dell'iride, la scansione retinica, il riconoscimento del volto, la geometria della mano, il riconoscimento della forma dell'orecchio, il rilevamento dell'odore del corpo, il riconoscimento vocale, l'analisi della struttura del D.N.A., l'analisi dei pori della pelle o della struttura delle vene.

La biometria comportamentale è invece basata su aspetti riconducibili a caratteristiche comportamentali. Tra queste

possiamo annoverare la verifica della firma autografa, la misurazione del tempo di battitura della tastiera, l'analisi dell'andatura.

Il dato biometrico rappresenta una caratteristica dell'individuo unica e inscindibile dal proprietario e, in tal senso, costituisce un dato personale inteso come informazione riferibile a una persona fisica, identificata o identificabile anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Tale aspetto rappresenta il punto di forza a sostegno dell'impiego di sistemi biometrici per il riconoscimento certo degli individui.

Le stesse peculiarità di unicità e inscindibilità del dato biometrico dell'individuo rappresentano, al contempo, un elemento di debolezza dei sistemi biometrici che richiedono misure di protezione accurate e sofisticate.

Infatti, mentre una *password* non più sicura o violata può essere sostituita, lo stesso non può dirsi per una caratteristica biometrica: non è pensabile la sostituzione dell'iride o dell'impronta digitale; al massimo è possibile rilevare un nuovo dato biometrico dello stesso tipo, per un numero limitato di volte (l'impronta di un altro dito, l'iride di un altro occhio).

La storia della biometria inizia intorno al 1879 quando Alphonse Bertillon, un ispettore della polizia francese, propose un sistema di misurazioni anatomiche per identificare i criminali recidivi. Alcuni anni dopo degli studiosi britannici scoprirono che le impronte delle dita hanno un disegno unico da persona a persona e non mutano nel tempo. Nel 1896, grazie a questa sensazionale scoperta, venne inaugurato il sistema di classificazione di impronte digitali; i primi a servirsi di questo sistema furono gli Ispettori di Scotland Yard.

Non essendo le impronte digitali il dato più pratico da usare, negli ultimi anni sono stati sviluppati sistemi di identificazione basati su caratteristiche quali il volto, le mani, la voce e l'iride. I tratti usati dai sistemi biometrici devono avere due caratteristiche: essere unici per ogni persona e non cambiare eccessivamente nel tempo. Alcuni tratti fisici permettono una precisione relativamente alta, mentre altri hanno maggiore praticità e costi inferiori. Non esiste, tuttavia, una misurazione biometrica ottimale per tutte le applicazioni e, dunque, la scelta dei dati da usare in un sistema di identificazione dipende dagli obiettivi perseguiti.

L'interesse diffuso intorno alle tecnologie biometriche ha portato un considerevole numero di *forum* internazionali ad analizzare la biometria sia per gli aspetti più propriamente tecnici che per quelli sociali, etici e inerenti il delicato tema della *privacy*.

La difficile situazione internazionale ha indotto un sensibile rafforzamento dei controlli atti a garantire la sicurezza dei cittadini e, negli ultimi anni, i governi di tutto il mondo hanno promosso il potenziamento delle azioni di controllo del territorio e delle frontiere nell'ambito delle quali sono spesso emerse difficoltà legate alla identificazione certa degli individui.

L'impiego della biometria a rafforzamento della sicurezza è testimoniato da iniziative internazionali, quali il nuovo passaporto europeo e il permesso di soggiorno elettronico e, per ciò che attiene all'Italia, la nuova Carta d'Identità Elettronica (CIE), che hanno come denominatore comune l'uso di identificatori biometrici a sostegno dell'autenticità. L'utilizzo delle tecnologie biometriche non si limita comunque agli ambienti investigativi o di controllo delle frontiere, ma registra

una rapida diffusione anche in altri importanti settori privati e pubblici.

Come è noto, i metodi basati sull'uso di *password*, attualmente i più diffusi, non sempre sono in grado di assicurare una adeguata garanzia; per queste ragioni molte amministrazioni stanno decisamente orientandosi verso l'utilizzo di tecniche di tipo biometrico.

Nella pubblica amministrazione italiana, fino a qualche anno fa, escludendo le applicazioni A.F.I.S., le tecnologie biometriche avevano trovato un utilizzo limitato per lo più ad applicazioni finalizzate al controllo dell'accesso fisico del personale a luoghi sensibili (ad esempio ai siti militari). Recentemente, invece, sta crescendo l'interesse da parte delle amministrazioni pubbliche verso l'utilizzo di tecnologie biometriche per il controllo dell'accesso fisico a edifici e aree riservate o per l'accesso logico ad applicazioni informatiche critiche.

Sebbene la maggior parte delle applicazioni biometriche utilizzate si caratterizzino per la conoscenza della operatività del sistema da parte degli utenti che sono, quindi, cooperativi (biometria interattiva), alcune applicazioni con finalità di carattere investigativo e governativo possono prevedere l'uso di sistemi biometrici senza che l'utente ne sia a conoscenza (biometria passiva). Tipica è l'applicazione della sorveglianza nei luoghi caratterizzati da un largo afflusso di pubblico.

La biometria, quindi, può avere un uso multiforme: per i sistemi di controllo degli accessi, per la rilevazione di presenze in aree riservate, sedi governative e nella produzione di documenti.

1.2. Il processo biometrico

Nell'ambito del trattamento dei dati personali con strumenti elettronici, le credenziali di autenticazione biometriche costituiscono un valido strumento per farsi riconoscere da un sistema informatico, da un *computer* e così via, nonché per poter conseguentemente accedere alle risorse dello stesso.
La prima fase del processo biometrico è la registrazione (*enrollment*) attraverso la quale la persona fornisce al sistema elettronico una sua caratteristica fisica o comportamentale per mezzo di un dispositivo di acquisizione che può variare a seconda del dato biometrico utilizzato (ad esempio, uno *scanner* per le impronte digitali o per la retina ovvero una video-camera per il riconoscimento facciale).
Il dato o campione di dato viene analizzato dal sistema, ossia "processato" (usando un termine tecnico), al fine di estrarre da esso informazioni/caratteristiche distintive. Tali informazioni andranno poi a formare il cd. *template*, che altro non è se non una rappresentazione o ricostruzione in termini matematici, numerici, digitali dei dati biometrici acquisiti.
Concluso il processo di *enrollment*, il *template* viene archiviato su di un *database* centralizzato ovvero su di un dispositivo quale una *smart-card*, una tessera plastificata o una scheda ottica (supporti dunque "decentralizzati" e che l'utilizzatore può portare al seguito).
La fase successiva consiste nella cosiddetta verifica dell'utente/identificazione, che determina l'acquisizione, da parte del sensore, del relativo dato biometrico per la comparazione con il *template* precedentemente depositato/registrato. Nel processo di verifica, detto anche "uno a uno", i dati acquisiti sul momento dal sensore

biometrico vengono comparati con un unico dato biometrico depositato dall'utente nella fase di registrazione e indicizzato da un codice identificativo. In quello di identificazione, detto anche "uno a N", i dati acquisiti sul momento dal sensore vengono comparati con un insieme di dati biometrici contenuti in un archivio precostituito.

In conclusione, la locuzione "riconoscimento biometrico" fa riferimento all'identificazione o alla verifica automatica di identità degli individui attraverso la valutazione di caratteristiche fisiche e comportamentali.

Gli obiettivi del processo biometrico sono due:

1) la verifica della dichiarazione di identità di un soggetto;
2) l'attribuzione di una identità a un soggetto.

Per questo, in biometria sono ricorrenti le seguenti procedure:

a) quella di accertamento della titolarità del soggetto ad accedere (accesso fisico) in un locale, comprensorio o area;

b) quella di accertamento della titolarità del soggetto a usufruire di una risorsa informatica (accesso biometrico).

1.3. Le tecnologie biometriche nella videosorveglianza

L'uso sempre più diffuso di nuove tecnologie legate alla sicurezza, come la videosorveglianza o la biometria, sta alimentando appassionati dibattiti sull'esigenza da parte dello Stato di assicurare un imprescindibile livello di tutela collettiva senza che ciò incida in maniera troppo marcata sui diritti fondamentali dei cittadini (c.d. bilanciamento degli interessi).

Le nuove tecniche di sicurezza per il controllo del territorio e delle aree sensibili, vedono nella biometria e nella videosorveglianza un nuovo strumento dalle enormi potenzialità. L'impiego delle più moderne tecnologie

informatiche, unito a idonee misure preventive, rappresenterà un'arma vincente per realizzare un più efficace controllo del territorio sia in ambito pubblico sia in ambito privato, incontrando la crescente domanda di sicurezza delle aziende e, soprattutto, dei cittadini.

Gli impianti di videosorveglianza possono essere composti di singole telecamere ovvero da una rete di telecamere collegate tra loro. Le immagini rilevate dalle telecamere vengono quindi convertite in un adeguato formato digitale e trasferite nella memoria di un sistema informatico che effettua le elaborazioni.

La straordinaria capacità del sistema visivo umano di interpretare un'immagine, è spesso considerata un'operazione semplice e normale. L'interpretazione dell'immagine, tuttavia, diviene anche per l'uomo estremamente difficoltosa quando questa è rappresentata come una sequenza di numeri: questo tipo di rappresentazione è esattamente quella che deve essere elaborata e analizzata da un *computer* in un ambito di visione artificiale.

Attraverso le elaborazioni dei dati (corrispondenti alle immagini acquisite) è possibile riconoscere movimenti, oggetti depositati, folle di gente, etc. Questi sistemi possono allarmare il personale addetto alla sorveglianza, effettuare *zoom* nella situazione osservata e ottimizzare la registrazione di quanto accade aumentando la qualità/densità di registrazione.

Sempre più rilevanza assume la tecnica di videosorveglianza che consente il riconoscimento biometrico del volto; tecnica ritenuta una delle più importanti risorse di autenticazione biometrica che, tuttavia, presenta specifiche difficoltà di realizzazione e applicazione.

Il riconoscimento biometrico può avvenire attraverso la comparazione con una immagine fissa o con sequenze di

immagini in movimento e, a seconda del tipo di immagine, si opera generalmente una distinzione fra "riconoscimento statico" e "riconoscimento dinamico".

Il riconoscimento statico è impiegato, in linea di massima, nelle applicazioni inerenti l'accesso fisico o logico ed è caratterizzato, generalmente, da una buona qualità dell'immagine di riferimento memorizzata contestualmente alla rilevazione. La posa del soggetto, disposto frontalmente e su sfondo controllato, consente di semplificare notevolmente le operazioni matematiche alla base del metodo biometrico. Tale applicazione presuppone, quindi, la collaborazione del titolare del dato biometrico che è consapevole della rilevazione e non si oppone, con travestimenti o altri espedienti, alla estrazione dello stesso. L'applicazione della stessa, inoltre, assume rilievo nel settore della cosiddetta ricerca dei duplicati. Essa consente, infatti, di comparare i dati biometrici di immagini contenute in un *database* fotografico per individuare potenziali soggetti a cui risultano abbinate più identità. Nelle applicazioni per la ricerca dei duplicati, le fotografie contenute nel *database* sono quelle usate nei documenti o quelle del foto-segnalamento.

Il riconoscimento dinamico, caratteristico della modalità "sorveglianza", può invece avvenire attraverso l'analisi di immagini di soggetti inconsapevoli, e dunque non collaborativi, che possono assumere pose irregolari, ovvero essere in movimento, comportando notevoli problemi di tipo computazionale aggravati dalla necessità di dovere operare in tempo reale.

I sistemi di videosorveglianza dotati di *software* che permette l'associazione di immagini a dati biometrici (ad esempio un *software* per il riconoscimento facciale) o che sono in grado di riprendere e registrare automaticamente comportamenti o

eventi anomali segnalandoli all'operatore (c.d. *motion detection*), sono chiamati "sistemi intelligenti". Per l'utilizzo degli stessi, il Garante per la protezione dei dati personali ha previsto l'obbligatorietà della verifica preventiva (sulla quale si rinvia al successivo paragrafo 2.1).

2. Le criticità nell'utilizzo di soluzioni integrate videosorveglianza-biometria

2.1. I fattori tecnici

I dati biometrici maggiormente utilizzati attraverso specifiche applicazioni informatiche sono le impronte digitali, il volto e l'iride. Ogni applicazione, tuttavia, presenta vantaggi e svantaggi.

Le impronte digitali, ad esempio, oltre ad avere applicazioni in campo legale, sono anche usate in molti paesi per controlli automatici alle frontiere. Negli Stati Uniti il programma US-VISIT del Ministero responsabile della sicurezza interna, dal 2004 ha elaborato i dati di oltre 75 milioni di visitatori. Uno dei vantaggi di tali sistemi è il basso costo dei sensori; tuttavia, essi hanno margini di errore superiori rispetto a quelli più costosi usati della polizia, perché coprono una porzione minore del polpastrello e l'immagine ottenuta ha una definizione inferiore.

Per quanto riguarda l'iride, il cui disegno sembra essere unico e permanente per ogni persona, il riconoscimento è estremamente preciso e veloce. Si utilizza uno *scanner* che acquisisce la sequenza numerica dell'individuo comparandola con quella preregistrata in una banca dati. Un famoso sistema di identificazione basato sul riconoscimento dell'iride è l'I.R.I.S. (*Iris Recongnition Immigration System*) adottato nel Regno Unito,

che consente ai viaggiatori che forniscono i propri dati, di evitare le file estenuanti in aeroporto. Ciononostante, anche il riconoscimento dell'iride presenta dei problemi. È ragionevolmente possibile che esso non funzioni con persone non vedenti o per le quali si siano perse in maniera massiccia le proprietà morfologiche o geometriche dell'iride. Bisogna inoltre sottolineare che il costo dei sensori, anche se in calo, è nettamente più alto di altri dispositivi quali, ad esempio, i lettori per impronte digitali.

I contesti applicativi connessi al riconoscimento biometrico del volto ne evidenziano gli intrinseci aspetti positivi e negativi. L'impiego in settori per così dire "ordinari" di attività presenta un buon grado di accettazione della tecnologia da parte degli utenti per la natura non invasiva di acquisizione della caratteristica biometrica, che avviene senza contatto con il sensore e senza una particolare partecipazione.

Nel settore investigativo un punto di assoluta forza è rappresentato dalla possibilità di effettuare specifiche verifiche e accertamenti, non altrimenti esperibili se non ricorrendo ad altre tecniche, quali la rilevazione delle impronte digitali o dell'iride, che, però, necessitano della collaborazione del soggetto "attenzionato" laddove, invece, l'esigenza investigativa richiede un approccio riservato.

Come già detto precedentemente, per "sorveglianza" si intende il tentativo di identificare un soggetto attraverso il confronto tra le immagini acquisite da una telecamera e quelle contenute in un archivio.

A tale proposito un problema concreto consiste nella corretta determinazione della "soglia di somiglianza" fra il soggetto ripreso e le immagini precedentemente archiviate in un *database.* Se la soglia di somiglianza è stata tarata su di un livello

troppo elevato, nel senso di ricercare la somiglianza massima, è possibile che il sistema non segnali soggetti che, invece, sarebbe opportuno sottoporre a verifica; se, al contrario, la soglia è stata attestata su livelli troppo bassi, si incorre nel rischio opposto, ossia di ricevere dal sistema una serie di falsi allarmi.

Proprio il problema dei falsi allarmi ha ridimensionato in qualche modo il ruolo del riconoscimento biometrico del volto per ciò che attiene alle attività di sorveglianza in tutti i luoghi aperti e/o particolarmente affollati (stadio, aeroporti, stazioni, etc.), ovvero quando l'uso di tali applicazioni è finalizzato alla prevenzione e al controllo del territorio.

Specifica quanto ultronea incidenza sulla gestione dei falsi allarmi è ascrivibile ad altri fattori non collegati a quello puramente tecnologico; tra questi, un ruolo di preminente rilievo assume il problema della variabilità temporale della caratteristica biometrica, dal momento che le qualità specifiche del viso, oltre che per accadimenti accidentali, si modificano ineluttabilmente con l'età.

Un secondo rilevante problema può essere, inoltre, individuato nella forte incidenza delle condizioni ambientali e, in particolare, l'illuminazione le cui variazioni possono condizionare i risultati.

Le tecnologie attualmente impiegate per il riconoscimento del volto utilizzano la rilevazione delle immagini 2D e, quelle più avanzate, 3D. Le prime consentono di ottenere elevate prestazioni quando l'immagine è frontale: infatti, se la posa del volto cambia, le *performance* decrescono. Un limite del sistema bidimensionale di riconoscimento facciale proviene dalla tipologia di dati utilizzati per verificare la somiglianza tra due volti, atteso che le immagini registrate sono mancanti della componente della profondità.

Per ridurre gli effetti negativi di tali criticità, sono stati implementati i sistemi basati su acquisizione tridimensionale del volto. A differenza di quelli per applicazioni bidimensionali (2D), i sensori dei sistemi di riconoscimento tridimensionale (3D) sono in grado di analizzare molte più informazioni. Rispetto alle 2D, le tecniche 3D sono meno sensibili alle condizioni di illuminazione; le stesse variazioni di posa del soggetto possono essere risolte con il riallineamento. Esse, inoltre, consentono la ricostruzione della superficie del viso, con informazioni geometriche su caratteristiche fondamentali**,** che rappresentano la base di partenza per le successive elaborazioni.

Gli svantaggi connessi all'utilizzo di tale tecnologia sono rappresentati innanzitutto dai costi elevati per l'acquisizione degli *hardware* 3D e per la sostituzione delle apparecchiature dotate di tecnologia 2D (videocamere, macchine fotografiche, etc.), oppure per la sospetta invasività di specifiche applicazioni. I tempi di acquisizione del riscontro biometrico sono inoltre più lunghi.

In conclusione, si può affermare che i sistemi basati sul riconoscimento del volto sono precisi quando l'immagine è registrata in condizioni controllate, ma diventano inaffidabili se l'immagine originale e quella nuova differiscono a causa di cambiamenti di posizione, illuminazione, espressione, età o aggiunta di accessori. Questa eccessiva sensibilità diventa un effettivo problema soprattutto per la videosorveglianza.

Si precisa, infine, che ad oggi non sono ancora state sviluppate tecnologie che permettano di effettuare riconoscimenti del volto completamente automatizzati e in tempo reale, a prescindere che vi siano condizioni controllate o no.

2.2. Gli aspetti legati alla *privacy*

L'elemento biometrico, in quanto dato personale e considerato quale aspetto della identità fisica dell'uomo, trova una tutela, come già evidenziato nel primo capitolo del presente lavoro, nei principi contenuti nella Carta Costituzionale, come ad esempio nell'art. 13 inteso «con riferimento anche alla libertà di salvaguardia della propria salute e della propria integrità fisica» (cfr. Corte Cass., sez. III, sent. 25 novembre 1994, n. 10014).

La possibilità, dunque, di acquisire un dato biometrico coattivamente e contro la volontà del soggetto cui appartiene, incontra precisi limiti imposti dalla Carta Costituzionale che osteggia le condotte invasive della sfera privata se non in correlazione a poteri o doveri specificamente individuati.

Le norme a tutela dell'ordine e della sicurezza pubblica e il sistema processuale penale, in taluni casi, prevedono la facoltà per l'autorità di acquisire dati biometrici dei cittadini, pur nel rispetto della dignità umana e per gli scopi propri definiti dalle disposizioni che introducono tali poteri.

In mancanza di una legale definizione, può essere richiamato il concetto espresso dal Gruppo dei Garanti Europei (istituito sulla base dell'art. 29 della direttiva 95/46/CE sulla protezione dei dati personali, e pertanto noto come *Working Party Art.* 29) che, nel documento adottato il 1° agosto 2003, evidenzia come «i dati biometrici possono sempre essere considerati come informazioni concernenti una persona fisica in quanto sono dati che, per la loro stessa natura, forniscono indicazioni su una determinata persona».

Tenuto conto della rapida espansione dell'impiego di tecnologie biometriche e delle preoccupazioni in merito al loro

possibile incontrollato utilizzo, nel Documento di lavoro sulla biometria, il predetto Gruppo ha formulato specifiche raccomandazioni in forma di linee-guida. Lo scopo era quello di contribuire ad un'omogenea ed efficace applicazione delle norme nazionali rispetto alla direttiva 95/46/CE in materia di sistemi biometrici, atteso che gli stessi possono essere utilizzati come strumento di autenticazione (informatica), *rectius* di identificazione. Tali dati, infatti, presentano qualità del tutto peculiari, e precisamente:

- l'universalità: l'elemento biometrico è presente in ogni persona;
- l'esclusività: l'elemento biometrico è unico, assolutamente inequivoco e distintivo di ogni persona;
- la permanenza: ogni persona conserva i propri elementi biometrici nel corso del tempo (salvo lesioni dell'integrità fisica).

Le credenziali biometriche consentono di accedere a un sistema per procedere a determinate operazioni, tra le quali per l'appunto quelle di trattamento dei dati personali. Ma gli stessi dati biometrici sono dati personali ai sensi dell'art. 4, co. 1, lett. b), del d. lgs. n. 196/2003 recante il Codice in materia di protezione dei dati personali e come tali sono soggetti, quanto a tutela, garanzie, modalità e finalità di trattamento, alle disposizioni del Codice stesso.

Il Codice in argomento, nel prevedere che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali nonché della dignità dei soggetti interessati, sottopone a un regime di maggiore severità i trattamenti che comportano rilevazioni di dati biometrici.

Questi ultimi, infatti, devono avvenire nel rispetto, oltre che dei principi generali di necessità, finalità, proporzionalità e liceità, anche di altre disposizioni specifiche eventualmente indicate dal Garante e/o prescritte da ulteriori disposizioni di legge rivolte a particolari ambiti applicativi.

In materia di trattamento dei dati personali connessi a dati biometrici è necessario innanzitutto osservare il principio di necessità (art. 3, d. lgs. n. 196/2003). Nelle attività e nei contesti che non sono soggetti a concreti pericoli o per le quali non ricorrono effettive esigenze di identificazioni certe, infatti, la rilevazione biometrica è da evitare. I sistemi biometrici, quindi, possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili. Ciascun sistema informativo e il relativo programma informatico, devono essere conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi o codici identificativi. Se il sistema prevede l'acquisizione e l'elaborazione del dato biometrico e la relativa conservazione in una banca dati, inoltre, il *software* applicativo deve essere configurato in modo da prevedere la cancellazione periodica e automatica dei dati che non siano più necessari agli scopi per i quali sono stati acquisiti.

I dati raccolti devono, altresì, essere utilizzati per scopi determinati (specifici), espliciti (trasparenti) e legittimi, ossia non contrastanti con le leggi e con l'ordinamento giuridico, e devono essere pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati (c.d. principio di proporzionalità, sancito *ex* art. 11 del d. lgs. n.196/2003). In virtù di tale principio, è necessario valutare preliminarmente se l'uso dei dati rilevati sia proporzionato agli scopi e alle finalità che si intendono perseguire, evitando

ingiustificate ingerenze nei diritti e nelle libertà fondamentali dei soggetti interessati. I dati, inoltre, non devono essere conservati per un periodo di tempo superiore a quello necessario; ogni violazione di siffatta disciplina comporta l'inutilizzabilità dei dati stessi.

Il trattamento dei dati biometrici è possibile solo se è fondato su uno dei presupposti di liceità che il Codice espressamente prevede per i soggetti pubblici (svolgimento di funzioni istituzionali, *ex* artt.18-22 del d. lgs. n.196/2003) e per i soggetti privati ed enti pubblici economici (consenso espresso, adempimento ad un obbligo di legge, provvedimento del Garante in tema di bilanciamento di interessi, *ex* artt. 23-27 del d. lgs. n. 196/2003).

Non può prescindersi, inoltre, dal rispetto di quanto prescritto da altre disposizioni di legge rivolte a specifici trattamenti come quelli che, ad esempio, possono aver luogo nell'ambito lavorativo e per i quali vanno tenute presenti le norme riguardanti la tutela dei lavoratori.

Come dinanzi accennato, oltre ai principi di carattere generale, il Codice evidenzia particolari prescrizioni qualora il trattamento dei dati personali possa comportare «rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato». Poiché i sistemi di raccolta di dati biometrici mediante sistemi di videosorveglianza rientrano proprio in tale specifica casistica, in quanto l'indebito uso può determinare pregiudizi rilevanti per i soggetti interessati, attesa la particolare e intrinseca natura degli stessi, il provvedimento generale emanato dal Garante nel 2010 in materia di videosorveglianza assoggetta tali attività alla cosiddetta verifica preliminare (*prior checking).* La verifica preliminare si sostanzia

in una richiesta di consenso preventivo al Garante che deve essere presentata prima dell'inizio del trattamento.
In particolare, la verifica preliminare è contemplata nell'art. 17 del Codice in relazione a trattamenti che, pur non riguardando dati sensibili, hanno caratteristiche, come detto, di particolare delicatezza. In tal caso i trattamenti di dati personali a mezzo di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti dall'Autorità con il provvedimento generale come esito di una verifica preliminare attivata d'ufficio o su richiesta del titolare. In particolare, a questo fine, saranno da sottoporre a verifica preliminare i sistemi di videosorveglianza che prevedono una raccolta di immagini:

– collegata e/o incrociata e/o confrontata con altri dati personali (es. biometrici) oppure con codici identificativi di carte elettroniche o con dispositivi che rendano identificabile la voce;

– digitalizzata o indicizzata che renda possibile una ricerca automatizzata o nominativa;

– dinamico/preventiva che non si limiti a riprendere staticamente un luogo ma rilevi percorsi o caratteristiche fisiognomiche (ad esempio il riconoscimento facciale) o eventi improvvisi oppure comportamenti anche non previamente classificati.

In tema di verifica preliminare, essa viene estesa ai casi di conservazione dei dati per l'eventuale termine ulteriore rispetto a quello settimanale originariamente previsto. La stessa verifica attiene, inoltre, ai casi di utilizzo di sistemi di rete condivisi o integrati di videosorveglianza territoriale tramite i quali, diversi titolari, sfruttano la medesima infrastruttura per raccogliere

immagini. In tal caso vengono elevate anche le misure di sicurezza minime richieste, descritte nel capitolo I del presente lavoro.

Anche le Forze di polizia, qualora effettuino trattamenti mediante sistemi di raccolta di immagini associate a dati biometrici, sono tenute, ai sensi dell'art. 55 del Codice, a richiedere la verifica al Garante la quale si innesca sulla base della preventiva comunicazione ai sensi dell'art. 39 del Codice (sul punto si rinvia a quanto specificato nel paragrafo 3 del capitolo I).

Al contrario, il semplice impiego di strumenti di videosorveglianza non associati a dati biometrici (o che comunque non presenti rischi specifici a norma dell'art. 17 del Codice e che non rientri nella casistica *ex* art. 39 del Codice stesso) non necessita né di comunicazione né di verifica preventiva, pur dovendo comunque rispettare i principi generali sopra richiamati.

3. Un caso di studio

3.1. Il modello "Fiumicino"

L'incremento del traffico passeggeri facilmente registrabile presso un aeroporto internazionale di una capitale europea ha determinato, in generale, l'adeguamento nel corso degli anni delle strutture esistenti.
La stessa applicazione dell'Accordo di Schengen, con il conseguente obbligo di distinguere i flussi passeggeri a seconda delle provenienze/destinazioni, evitando commistioni tra quelli *intra* ed *extra*-Schengen (soltanto i primi esenti da controlli sistematici di frontiera), ha reso obbligatoria la predisposizione e l'attuazione di specifici interventi finalizzati a conferire seguiti concreti ai presupposti operativi dell'Accordo.
In tale contesto, non sono mancate implicazioni connesse alla sempre più crescente necessità di garantire livelli di sicurezza elevati; le opere nel tempo realizzate, tuttavia, hanno successivamente evidenziato l'assenza di criteri di omogeneizzazione ed integrazione.
La maggiore complessità delle funzioni legate alla sicurezza, richieste dalle nuove normative internazionali emanate a seguito dei ben noti fatti criminosi, ha indotto le Autorità aeroportuali, d'intesa necessariamente con la società di gestione aeroportuale, ad affrontare in maniera organica le scelte connesse a nuovi interventi volti ad armonizzare la struttura sotto il profilo della maggiore fruibilità dei servizi aeroportuali e della esigenza di sicurezza, intesa come sicurezza e tutela dell'incolumità delle persone e delle stesse strutture aeroportuali.

In tale quadro, anche per confrontarci concretamente con gli aspetti analizzati nel presente lavoro, si è ritenuto interessante descrivere un progetto per l'adozione di un nuovo sistema di videosorveglianza, al passo con i tempi sia sotto l'aspetto tecnologico sia sotto l'aspetto della rispondenza ai sopra richiamati presupposti e, ancor più, in grado di garantire un efficace supporto agli organi di sicurezza nel rispetto dei principi normativi sanciti in materia.
A tal fine, prendendo spunto dal sistema di videosorveglianza realizzato all'aeroporto di Fiumicino, si è provveduto a suddividere la progettazione del lavoro nelle seguenti fasi:

1) analisi delle criticità esistenti e individuazione delle finalità degli interventi;
2) analisi delle conseguenti soluzioni logistiche e tecniche;
3) attribuzione degli oneri finanziari;
4) individuazione della/e ditta/e e attribuzione degli incarichi.

3.1.1. La prima fase dello studio: analisi delle criticità esistenti e individuazione delle finalità degli interventi

Nella predisposizione di un sistema di videosorveglianza per il controllo di un'area particolarmente complessa ed articolata, come appunto un aeroporto, ove operano enti di Stato e organizzazioni private diverse, motivate da diverse finalità, è opportuno ricercare la massima condivisione delle scelte da operare. Per tale motivo è opportuno procedere alla istituzione di un Gruppo di lavoro con rappresentanti degli enti interessati. La preliminare attività che il Gruppo è chiamato a svolgere è, senz'altro, l'analisi della situazione contingente al fine di esaminare le criticità e le difficoltà operative rilevate nel tempo.

Ciò, infatti, consente di rilevare:

a) quale sia stato lo sviluppo dei sistemi di video-controllo avvenuto in tempi diversi e l'esistenza, conseguentemente, di sistemi non omogenei quali:

- telecamere analogiche e digitali;
- differenti sistemi di TVCC;
- diverse modalità di gestione dei sistemi TVCC;

b) quale sia l'architettura informatica, molto probabilmente obsoleta poiché caratterizzata da una rete dati non adeguata o da sistemi non ridondati;

c) la conseguente ridotta efficacia operativa del sistema, non rispondente alle mutate esigenze;

d) i costi, spesso troppo elevati, di gestione.

L'eventuale inadeguatezza delle dotazioni informatiche disponibili, intese come rete trasmissione dati, telecamere, *software*, etc., nonché l'eterogeneità delle stesse utilizzate per finalità tra loro diverse, determina la necessità di creare un sistema servente contemporaneamente più utenti, capace dunque di consentire, pur nella sua unicità, la gestione dell'impianto per finalità sì diverse ma non concorrenti.

Il presupposto per conseguire la finalità descritta, si sostanzia nell'assicurare contiguità fisica ai due utenti incaricati di gestire, per finalità diverse, l'impianto aeroportuale, ossia la Polizia di Frontiera e la *Security* aeroportuale (particolari guardie giurate dell'istituto di vigilanza privata, incaricato dalla Società di gestione aeroportuale, di svolgere le attività di sicurezza e controllo che non comportano l'esercizio di pubbliche potestà, munite della prevista autorizzazione del Prefetto). Innanzitutto, quindi, è necessaria una contiguità delle aree ove realizzare le

sale operative in cui attestare la centralità del sistema di videosorveglianza.
Sussiste, dunque, una duplice finalità. Da una parte, la necessità di implementare il sistema per corrispondere alle esigenze di prevenzione e controllo del territorio, consentendo alle Forze di Polizia localmente operanti il monitoraggio costante e intelligente delle aree videoriprese e adeguando gli interventi alle situazioni di pericolo segnalate dal sistema di rilevazione del *motion detection*. Dall'altra parte, la necessità di garantire alla Società di gestione aeroportuale la visualizzazione dei settori di specifica competenza sotto il profilo della fruibilità dei servizi aeroportuali e dei sistemi integrati di sorveglianza e sicurezza interagendo, fin dove consentito, con le forze di polizia.
Quanto sopra si ritiene fattibile mediante la realizzazione di una idonea piattaforma centralizzata per consentire un uso dei sistemi TVCC in linea con le più variegate esigenze, assicurando:
- l'utilizzo di sistemi condivisi,
per garantire
- la sinergia tra operatori della Polizia di Stato e della *Security* aeroportuale**.**
La scelta di realizzare sale operative attigue dotate di strumenti di utilizzo condivisi, infatti, permetterebbe alla Polizia di Stato e alla *Security* di lavorare sinergicamente, realizzando concretamente quella sicurezza partecipata, che rappresenta la soluzione più all'avanguardia nella gestione integrata delle problematiche di sicurezza in qualsiasi teatro operativo.
Tale sistema, centralizzato e contemporaneamente condiviso, consentirebbe anche la gestione operativa dei sistemi aeroportuali con un'ottimizzazione dell'impiego delle risorse umane.

Per la Polizia di Frontiera, ciò si traduce nella possibilità di rilevare le criticità connesse all'espletamento dell'attività di istituto e di predisporre con tempestività ed efficacia gli interventi di competenza, ovvero:

- controllo di frontiera: si fa riferimento alla rilevazione della regolarità delle operazioni e, ove necessario, intervento con tempestività;
- supervisione sui controlli di sicurezza svolti dal personale della *security* aeroportuale: il Decreto del Ministro dei Trasporti e della Navigazione del 29 gennaio 1999, in particolare, elenca, all'art. 2, i servizi affidati al gestore aeroportuale che li svolge direttamente o tramite impresa di sicurezza (tra i quali il controllo dei passeggeri in partenza e in transito, il controllo radioscopico o con altri tipi di apparecchiatura del bagaglio al seguito, dei bagagli da stiva, della merce e dei plichi dei corrieri espressi); tali servizi sono svolti sotto la vigilanza dell'Ufficio di Polizia di Stato presso lo scalo aereo, che assicura gli interventi che richiedono l'esercizio di pubbliche potestà;
- vigilanza del sedime aeroportuale e vigilanza interna delle aerostazioni: di norma, nell'arco delle 24 ore le pattuglie (automontate) del dispositivo di sicurezza aeroportuale (Polizia di Stato, Arma dei Carabinieri, Guardia di Finanza) assicurano la vigilanza ed il controllo delle aree esterne e delle vie di scorrimento interne (prospicienti le piste di atterraggio/decollo); servizi di vigilanza e controllo possono essere assicurati, in via continuativa anche all'interno delle aerostazioni e ai punti considerati a rischio quali: le aree check-in di voli considerati sensibili.

Non può escludersi che, in futuro, l'ulteriore estensione del concetto di sicurezza partecipata, possa determinare il

concorso, nell'attività di vigilanza del sedime aeroportuale, anche di unità costituite da personale dell'ente gestore in analogia a quanto già attualmente avviene presso alcuni aeroporti ove dette unità assicurano il controllo di esercizi commerciali/agenzie bancarie ivi presenti.

Per la società di gestione quanto prospettato si traduce nella possibilità di ottimizzare l'impiego delle risorse umane migliorando l'efficienza dei servizi di propria pertinenza e intervenendo per:

a) garantire l'incremento delle postazioni di lavoro ai banchi *check-in* per smaltire le file dei passeggeri in attesa;

b) segnalare al responsabile di scalo la necessità di movimentare personale da un punto all'altro di carico/scarico bagagli per velocizzare il ritiro dei propri effetti personali ai viaggiatori e, in generale, per movimentare il personale all'interno dei vari *terminal* a seconda delle necessità al fine di migliorare la qualità del servizio offerto;

c) assicurare la vigilanza del patrimonio immobiliare contro danneggiamenti/furti.

Risulta evidente che la progettazione e la successiva realizzazione di un siffatto sistema di videosorveglianza, che comporta la registrazione, la conservazione e l'eventuale raccolta di immagini associate a dati biometrici, impone l'adozione di quelle specifiche misure disciplinate dalla normativa vigente in materia di protezione dei dati personali e soprattutto dal più volte citato provvedimento generale del Garante adottato nel 2010.

Si fa riferimento, in particolare, alla richiesta *prior checking* (qualora ovviamente ne ricorrano le condizioni che la rendano obbligatoria) o, ancora, alle misure di sicurezza disciplinate

dall'art. 34 del Codice e dal punto 3.3.1 del provvedimento generale, di cui sono state già delineate le specificità.

3.1.2. La seconda fase dello studio: analisi delle conseguenti soluzioni logistiche e tecniche

Una volta individuata la finalità degli interventi, andranno analizzate le soluzioni logistiche primarie, tra cui ovviamente la scelta dei locali destinati alle due sale operative, locali rispondenti all'esigenza di mantenere le due strutture sì indipendenti, ma tra loro fisicamente vicine.

Nell'ottica di rendere vivibili le postazioni di lavoro del personale di polizia e della *security* aeroportuale, nel rispetto della normativa in materia di sicurezza dei luoghi di lavoro, si rende necessario prevedere innanzitutto la realizzazione di una sala apparati (sala CED opportunamente protetta) per l'allocazione dei *server*, della rete LAN, adeguatamente dimensionata in considerazione di eventuali futuri ampliamenti, con un sistema di climatizzazione autonomo rispetto a quello delle attigue sale operative. Ciò in quanto è necessario garantire il microclima interno ideale per il corretto funzionamento degli apparati stessi, prescindendo dalle condizioni termo climatiche esterne.

Lo scopo, dunque, è quello di razionalizzare il lavoro e per far ciò è necessario che Polizia di Stato e *Security* aeroportuale operino in sale attigue utilizzando i medesimi strumenti.

Il sistema da realizzare, inoltre, dovrà consentire di poter disporre di una piattaforma unica di gestione e archiviazione di tutti i dati rilevati dal sistema di videosorveglianza; per supportare l'intera dinamica aeroportuale, inoltre, sarà necessaria la realizzazione di una rete dati dedicata e in quanto

tale separata dal resto della rete dati aeroportuale, in grado di supportare tutte le telecamere con indirizzo IP connesse alla piattaforma TVCC[2].

In fase di progettazione dovranno essere previste, a seconda dell'area da sottoporre a videosorveglianza e delle criticità rilevate, tipologie di TVCC necessarie per l'ottimizzazione del sistema in parola (DOME ossia camere di videosorveglianza protette da una cupola plastica, con *zoom* molto potenti, in grado di permettere alla centrale operativa, da remoto, di controllare il movimento e l'immagine in *live*, ovvero telecamere MegaPixell ossia con alta risoluzione necessaria per evidenziare in *live* il dettaglio di una immagine e di effettuare tale procedura anche a seguito di registrazione). L'analisi dell'area, non disgiunta dalle finalità che si intendono perseguire, potrebbe suggerire di "integrare" il sistema predisposto per aree aperte al pubblico ovvero per le sale di transito/imbarco, con altri sistemi deputati a rilevare comportamenti anomali, segnatamente l'analisi video e il *motion detection*. Tali sistemi, infatti, rivelano la propria intrinseca utilità quando riguardano aree ove l'accesso è consentito solo in determinati periodi o frazioni di periodi, accesso peraltro consentito solo a personale appositamente autorizzato. L'eventuale accesso a tali aree in modalità non autorizzata, viene rilevata dalla telecamera (che in tal caso funzionerà come un sistema di allarme) e segnalata al personale addetto alla centrale operativa. È evidente, quindi, che il posizionamento di tali tecnologie in aree con alta densità

[2] Per piattaforma TVCC *over* IP si intende la tipica centrale di videosorveglianza (televisione a circuito chiuso, da qui l'acronimo TVCC) le cui telecamere non sono collegate con un cavo normale o analogico, ma inviano le immagini su un cavo di rete (come quella dei computer) ad un sistema che le acquisisce e le ritrasmette alle varie console di gestione anche a molti chilometri di distanza, usando il protocollo IP (quello che consente di usare *internet*).

di persone, determinerebbe una sovrapproduzione di allarmi, svilendone la funzione.
Il punto fondamentale di tutta la realizzazione è quello di dare centralità all'operatore: con la realizzazione delle sale operative in tal modo ipotizzate, ogni operatore potrà utilizzare, dalla propria postazione, qualunque strumento messo a sua disposizione, evitando quindi che lo stesso si muova all'interno della sala operativa per raggiungere i vari sistemi.
Per quanto riguarda l'impiantistica, tutti i sistemi devono essere infine ridondati, al fine di garantire il perfetto funzionamento della stessa anche in caso di *black-out* elettrico, di rottura dell'impianto di condizionamento, di taglio della rete dati, di rottura degli apparati di rete, etc.

3.1.3. La terza fase dello studio: attribuzione degli oneri finanziari

La realizzazione di un tale articolato impianto determina, evidentemente, oneri finanziari di non poco conto.
Il sistema aeroportuale è caratterizzato dalla titolarità della gestione infrastrutturale in capo alla società di gestione a seguito di concessione governativa disposta con apposito decreto. La concessione in parola impone la manutenzione, la gestione e lo sviluppo delle infrastrutture aeroportuali; non comprende, invece, la realizzazione di impianti/sistemi utilizzati dalle FF.PP. per finalità di ordine e sicurezza pubblica.
In alcuni aeroporti internazionali, come quelli di Roma e Milano, la società di gestione aeroportuale, in virtù del principio di economicità ed efficienza, ha ritenuto più conveniente la predisposizione di un unico sistema centralizzato, utilizzabile da più soggetti, ognuno per le

specifiche finalità istituzionali e per il raggiungimento degli scopi prefissati, in luogo di più impianti TVCC che avrebbe dovuto, comunque, realizzare quanto meno per garantire il più efficace espletamento delle specifiche attribuzioni.
La realizzazione di un sistema unico, che presenta i vantaggi descritti e che sotto il profilo economico investe evidentemente l'ente con maggiori disponibilità finanziarie ossia la Società di gestione, concretizza ulteriormente anche il concetto di sicurezza partecipata che vede coinvolti soggetti pubblici e privati.

3.1.4. La quarta fase dello studio: individuazione della/e ditta/e e attribuzione degli incarichi

Un accenno doveroso va fatto, preliminarmente, in relazione alla necessità di procedere sin dalla fase di progettazione alla "secretazione" dell'architettura di un impianto/sistema in tal modo strutturato. Appare del tutto evidente, infatti, come l'esigenza di garantire la sicurezza di determinati siti "sensibili" non consenta la pubblicazione del progetto e lo svolgimento delle ordinarie procedure di aggiudicazione. Tutto ciò comporta, inoltre, che la individuazione della ditta da incaricare della realizzazione dell'impianto avvenga tra quelle munite di NOS.
Una volta individuata l'impresa dovrà essere redatto un documento analitico delle esigenze e delle finalità che si richiedono al sistema. Andranno inoltre verificate le credenziali e le certificazioni ISO (certificato di qualità) delle società operanti nel settore della progettazione e distribuzione di tecnologia in quella complessa fetta del mercato caratterizzata

dalla "contaminazione" fra l'elettronica e l'informatica, negli ultimi anni enormemente proliferate.

Stabilite le finalità che il sistema dovrà consentire di perseguire, e definito (anche se per linee generali) il budget di spesa da destinare alla realizzazione dell'opera, alla società prescelta andrà attribuito l'onere di individuare le tecnologie di ripresa, gli apparati di codifica IP, i sistemi di archiviazione e così via, da utilizzare per garantire le più alte prestazioni. Sarà tenuta, inoltre, all'acquisto del *software*[3] di centrale applicabile per garantire un risultato finale di altissima qualità. In tal senso, il *software* dovrebbe possedere caratteristiche innovative quali la matrice virtuale, la completa protezione dai guasti, la videosorveglianza a livello geografico, nonché disporre di scalabilità intesa come dimensionamento del sistema che va dalla gestione di una sola telecamera a N telecamere. Dovrà inoltre rendere possibile gestire, da qualsiasi postazione di lavoro (*client)*, tutte le strumentazioni applicate.

Le caratteristiche del *software* dovranno essere le seguenti.

1) La scalabilità: ossia consentire di aggiungere telecamere, *workstation* o qualsiasi altro componente del sistema in qualsiasi punto della rete e in qualsiasi momento. Oltre a incrementare il sistema con l'aggiunta di una singola telecamera, il *software* dovrà permettere una maggiore estensione grazie all'innovativo concetto di *federation*.

2) L'integrabilità: ossia una piattaforma aperta tale da consentire la gestione di diversi sistemi quali il controllo accessi, la *building automation*, e le tecnologie di analisi video. Qualora già si disponga di telecamere analogiche e non, il *software* dovrà avere anche la capacità di gestire tali diverse

[3] È opportuno che si tratti di un *software* disponibile sul mercato. Questo a garanzia di una costante disponibilità di aggiornamenti, implementazioni, etc.

tecnologie.

3) La massima affidabilità: dovrà, cioè, essere progettato per garantire l'assenza di punti di criticità per quanto riguarda possibili guasti. Per tale motivo dovrà presentare una tecnologia di *failover* (sistema primario affiancato da un sistema secondario che entra in funzione quando si verificano guasti a carico del primo) e di ridondanza.

Per quel che concerne le telecamere, in assenza di dotazioni preesistenti, sarà necessario verificare che quelle da acquisire *ex novo* consentano la visualizzazione di immagini a colori, dotate di meccanismo che consenta il passaggio in automatico in bianco e nero per ottenere una buona immagine nel caso di scarsa luminosità.

Un fattore estremamente qualificante dell'intera realizzazione, che non può essere trascurato e che pertanto è opportuno contemplare nel conferimento di incarico alla società prescelta, è rappresentato dalla necessità di qualificare adeguatamente i futuri utilizzatori del sistema. Al fine di consentire l'utilizzo dell'intero impianto al massimo delle potenzialità, sarà infatti opportuno organizzare appositi corsi di formazione che dovranno, innanzitutto, consentire all'operatore un vero e proprio cambio di mentalità.

3.2. Considerazioni conclusive

La realizzazione del descritto impianto di videosorveglianza consente, fondamentalmente, di donare all'operatore un nuovo senso: la vista.

Fuor di metafora, può affermarsi che altri sistemi che utilizzano impianti TVCC, privi della caratteristica della centralità e della condivisione, determinano, durante eventuali criticità, la

necessità per l'operatore addetto al sistema di inviare una pattuglia sul posto ovvero nell'area interessata dall'allarme. Ciò in quanto l'utilizzo di sistemi TVCC non centralizzati e soprattutto parcellizzati, non consente di disporre di una visione di insieme che comprenda anche le aree limitrofe a quelle interessate dalla criticità rilevata, al fine di modulare compiutamente l'intervento.

Possono determinarsi, dunque, notevoli e inutili dispendi di energia. Con le soluzioni descritte, viceversa, oltre agli enormi vantaggi legati alla vivibilità del posto di lavoro, l'operatore dispone di tutti gli strumenti che gli necessitano per lo svolgimento di un compito delicato che richiede, comunque, costante attenzione e che lo sottopone a enorme stress.

La videoregistrazione delle immagini in una piattaforma unica, in *real-time* e ad alta qualità, porta inoltre a migliorare notevolmente le operazioni di verifica e analisi delle situazioni. Il *software* applicato permette, infatti, di visualizzare in *live* le telecamere del sistema e contemporaneamente rivedere le registrazioni archiviate sfruttando la funzione di *replay* istantaneo.

Anche il sistema descritto, adeguatamente e tecnologicamente dimensionato alla realtà operativa di un aeroporto internazionale, presenta un limite: non consente, infatti, di procedere alla comparazione automatica dei dati biometrici del volto, acquisiti attraverso l'impianto di videosorveglianza, con un *data base* precostituito, in applicazioni diverse da quelle di tipo investigativo.

Si fa riferimento alla possibilità, allo stato solo futuristica, di realizzare un *software* che, applicato ad un sistema di videosorveglianza installato in un luogo accessibile a migliaia di persone (quali, appunto, un aeroporto o uno stadio, oppure

in una metropolitana di una grande città) che non sono collaborative in quanto non tenute ad assumere una posizione per così dire "fronte telecamera" tale da consentire la ripresa in modalità ottimale e che anzi potrebbero volutamente travisare il proprio aspetto (indossando occhiali, cappello o barbe/baffi posticci), consenta di attivare verifiche e controlli con finalità di prevenzione e non solo di repressione.

Corrisponde senz'altro al vero che la tecnica di riconoscimento del volto stia guadagnando sempre più popolarità in considerazione dell'enorme vantaggio che offre rispetto ad altri sistemi di identificazione. La tecnica in argomento e i sistemi sino ad oggi realizzati, sono, tuttavia, precisi quando l'immagine è registrata in condizioni controllate, ma diventano inaffidabili se l'immagine originale e quella nuova differiscono a causa di cambiamenti di posizione, di illuminazione, di espressione, età o aggiunta di accessori. Questa eccessiva sensibilità diventa un problema soprattutto per la videosorveglianza finalizzata al controllo e alla prevenzione di reati presso obiettivi sensibili, laddove si impone la immediata predisposizione di interventi mirati e adeguati alla rilevazione della criticità o della minaccia.

Per adesso non sono ancora state sviluppate tecnologie che permettano di effettuare riconoscimenti del volto completamente automatizzati e in tempo reale, a prescindere che vi siano condizioni controllate o no.

Né potrebbe ipotizzarsi l'uso in un aeroporto di un sistema di videosorveglianza che, pur basandosi sul riconoscimento del volto, risulti carente della caratteristica dell'automaticità. La movimentazione di persone e merci mediante l'uso del mezzo aereo rappresenta oggi un'esigenza ineludibile, attesa la necessità di ridurre le distanze tra popoli lontani tra loro nel

minor tempo possibile. Conseguentemente, cresce di pari passo l'obbligo degli Stati di tutelare la sicurezza dei trasporti e l'incolumità delle persone da possibili "attacchi" di varia natura perpetrati ai danni di aerei adibiti al traffico passeggeri nonché alle aerostazioni di un aeroporto che, in quanto luoghi aperti al pubblico, diventano obiettivi sensibili per il gran numero di persone che possono a vario titolo accedervi.

Un sistema di vigilanza e controllo di un siffatto obiettivo, è innanzitutto caratterizzato dalla evidente impossibilità di procedere alla sistematica verifica di tutte le persone (passeggeri, avventori, personale aeroportuale, etc.) che quotidianamente "popolano" tali aeree, poiché le tecniche utilizzabili ne determinerebbero la completa paralisi dell'operatività. Attualmente, infatti, la certezza della titolarità ad accedere in aeroporto e la "innocuità" della presenza all'interno di detta aerea, potrebbe essere perseguita soltanto attraverso l'impiego di sistemi intelligenti che consentano rilevazioni biometriche altamente affidabili, quali: la rilevazione dell'impronta digitale e/o dell'iride, la rilevazione della voce, il riconoscimento biometrico del volto, associando agli stessi la verifica dell'assenza di oggetti e materiali pericolosi (armi ed esplosivi) nascosti sulla persona ovvero all'interno di qualsiasi custodia. Sarebbe ottimale poter dotare tutti gli accessi alle aree aeroportuali, sia quelle aperte al pubblico sia quelle riservate a personale autorizzato, di *metal detector*[4], per visualizzare

[4] In realtà sarebbe ottimale poter installare, in luogo del metal detector, ovvero unitamente a questo, un cosiddetto *boody scanner*. Tali apparecchiature possono utilizzare onde millimetriche oppure sistemi a radiazioni ionizzanti. La prima modalità, meno invasiva rispetto alla seconda (adottata in America e certificata dalla TSA - *Transportation Security Administration*, applicabile, tuttavia, in esclusivo ambito sanitario) stante la necessaria compatibilità con le prescrizioni vigenti in materia di tutela della *privacy*, non consente di rilevare l'eventuale possesso di oggetti proibiti, occultati sulle parti intime maschili e femminili. Fa registrare, inoltre, un'elevata percentuale di falsi

l'assenza di materiali e oggetti pericolosi sulla persona, integrando il sistema in parola con sistemi TVCC in grado di rilevare e comparare i dati biometrici del volto con quelli contenuti in un *database* precostituito e, ancora, implementare dette applicazioni con la rilevazione delle impronte digitali (quantomeno per il controllo del personale aeroportuale). Forse, allora, potremmo affermare di aver approntato una serie di misure idonee a prevenire l'azione criminale di gruppi di terroristi o di *kamikaze*. In tale caso, tuttavia, avremo anche fatto lievitare a dismisura il prezzo dei biglietti aerei, sovraccaricati dei costi di gestione di un tale complesso sistema di sicurezza. Senza considerare i tempi necessariamente lunghi (e quindi inaccettabili) connessi all'espletamento di tali verifiche da attuare nei confronti di migliaia di passeggeri, di accompagnatori, di centinaia di operatori aeroportuali, fermi in fila per accedere in aeroporto o anche per spostarsi all'interno di aeree cosiddette "sterili".

In conclusione, può affermarsi che, in assenza di tecnologie idoneamente testate in grado di corrispondere alle esigenze di sicurezza senza "blindare" il sistema di gestione, è doveroso procedere a un bilanciamento tra opposte necessità sfruttando, al massimo delle potenzialità, gli strumenti operativi disponibili sul mercato in costante sinergia con la professionalità, l'esperienza operativa e l'intelligenza delle persone deputate a produrre e garantire sicurezza.

allarmi determinati dalla posizione assunta dal passeggero, da particolari indumenti indossati, dalla elevata sudorazione dello stesso, da fattori correlati alla struttura corporea nonché dalla presenza di alcuni accessori apposti sugli indumenti, con il conseguente innalzamento delle tempistiche di processamento dei passeggeri.

APPENDICE

Normativa di riferimento

Decreto Legislativo 30 giugno 2003, n. 196 - "Codice in materia di protezione dei dati personali";

Provvedimento in materia di videosorveglianza, emanato dal Garante per la protezione dei dati personali in data 8 aprile 2010.

Giurisprudenza di riferimento:

Corte Cost., sent. n. 34/1973;

Corte Cost., sent. n. 81/1993;

Corte Cost., sent. n. 281/1998;

Corte Cost., sent. n. 349/1999;

Corte Cost., sent. n. 135/2002;

Corte Cost., sent. n. 149/2008;

Corte Cass., Sez. V, sent. n. 769/1972;

Corte Cass., Sez. III, sent. n. 8616/1983;

Corte Cass., Sez. III, sent. n. 1567/1986;

Corte Cass., Sez. IV, sent. n. 13316/1989;

Corte Cass., Sez. V, sent. n. 10309/1993;

Corte Cass., Sez. IV, sent. n. 1344/1995;

Corte Cass., Sez. Unite, sent. n. 5021/1996;

Corte Cass., Sez. V, sent. n. 1477/1997;

Corte Cass., Sez. V, sent. n. 208137/1997;

Corte Cass., Sez. II, sent. n. 4095/1997;

Corte Cass., Sez. VI, sent. n.5649/1997;

Corte Cass., Sez. VI, sent. n. 4997/1997;
Corte Cass., Sez. IV, sent. n. 210579/1997;
Corte Cass., Sez. Unite, sent. n. 21/1998;
Corte Cass., Sez. III, sent. n. 11116/1999;
Corte Cass., Sez. III, sent. n. 3771/1999;
Corte Cass., Sez. Unite, sent. n. 6/2000;
Corte Cass., Sez. IV, sent. n. 562/2000;
Corte Cass., Sez. VI, sent. n. 7063/2000;
Corte Cass., Sez. V, sent. n. 8573/2001;
Corte Cass., Sez. V, sent. n. 35947/2001;
Corte Cass., Sez. V, sent. n. 43491/2001;
Corte Cass., Sez. VI, sent. n. 3443/2003;
Corte Cass., Sez. VI, sent. n. 6962/2003;
Corte Cass., Sez. IV, sent. n. 44484/2003;
Corte Cass., Sez. VI, sent. n. 37561/2004;
Corte Cass., Sez. V, sent. n. 16189/2004;
Corte Cass., Sez. V, sent. n. 46307/2004;
Corte Cass., Sez. VI, sent. n. 11654/2005 ;
Corte Cass., Sez. V, sent. n. 39827/2006;
Corte Cass., Sez. Unite, sent. n. 26795/2006.

BIBLIOGRAFIA ESSENZIALE

C.N.I.P.A., *Linee guida per l'impiego delle tecnologie biometriche nelle Pubbliche Amministrative*, novembre 2004.

CISTERNA A., *I filmati nel privé di un locale pubblico possono rientrare tra le prove atipiche*, in *Guida al Diritto*, n. 33/2006, p. 60.

DITTA E., *Tutela della riservatezza e videosorveglianza in condominio*, in *Consulente Immobiliare*, n. 825/2008, p. 2024.

FROSINI A., *La disciplina generale della videosorveglianza nell'ordinamento italiano*, in M. MANETTI, R. BORRELLO (a cura di), *Videosorveglianza e privacy*, Pontecorboli, Firenze, 2010, p. 101 e ss.

GAGLIARDI V., *Art. 134*, in C.M. BIANCA, F.D. BUSNELLI, (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, Cedam, Padova, II, 2007, 1617 e ss.

SARZANA DI S. IPPOLITO F., *La nuova videosorveglianza per gli enti locali, le imprese e i privati*, Maggioli, Rimini, 2010.