This is the peer reviewd version of the followng article:

Intervento su "Domanda di sicurezza urbana e videosorveglianza" / Pighi, Giorgio. - ELETTRONICO. - (2009), pp. 13-18.

Terms of use:

The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

12/10/2024 04:28

(Article begins on next page)

Presente e futuro dei sistemi di videosorveglianza per la sicurezza urbana

Atti del Convegno

Auditorium Fondazione Universitaria Marco Biagi
largo Marco Biagi, 10
venerdì 20 febbraio 2009

Videosorveglianza 2009

Indice

Prefazione e Saluti **5**

Intervento del sindaco di Modena **13**
Prof. Giorgio Pighi

Sicurezza partecipata, sicurezza integrata, sicurezza urbana **19**
Dr. Antonio Manganelli
Capo della Polizia - Direttore Generale della Pubblica Sicurezza

La videosorveglianza come strumento di contrasto della criminalità **25**
Dr. Elio Graziano
Dirigente Superiore della Polizia di Stato

L'efficacia della videosorveglianza nella prevenzione della criminalità. Alcune esperienze locali e internazionali **33**
Dr. Gian Guido Nobili
Responsabile delle attività di ricerca e progettazione della Regione Emilia Romagna in materia di sicurezza urbana.

Utilizzo, in ambito forense, di metodologie biometriche e informatiche per l'analisi e la sintesi di scene, eventi e soggetti. **49**
Prof. Nello Balossino
Università di Torino

Tutela della privacy e sicurezza urbana. Le regole della videosorveglianza e l'uso processuale dei dati acquisiti. **77**
Dr. Marco Dall'Olio
Giudice del Tribunale di Pescara

Progetti di ricerca in fase di sperimentazione in laboratori internazionali e in diversi contesti urbani europei ed americani **91**
Prof. Rita Cucchiara
Università di Modena e Reggio Emilia

Analisi dei dati multimediali nelle tecniche investigative **111**
Dr. Vittorio Rizzi
Dirigente Squadra Mobile Questura di Roma

Organizzatori e Sponsor **116**

Negli ultimi anni, l'utilizzo dei sistemi di videosorveglianza per la prevenzione della criminalità in ambito urbano ha conosciuto un grosso sviluppo, sia a livello nazionale che internazionale. Nella città di Modena, nel 2001, è stato installato uno dei primi sistemi italiani di videosorveglianza urbana, dove immagini e video sono utilizzati dalle Forze dell'Ordine e dalla Polizia Municipale; contestualmente presso l'Università di Modena e Reggio Emilia nei laboratori Imagelab del Dipartimento di Ingegneria dell'Informazione da dieci anni si svolgono attività di ricerca sulle nuove tecnologie informatiche per la analisi di video e in particolare per la videosorveglianza.

Il connubbio tra enti pubblici per la sicurezza e enti di ricerca, e le grandi aspettative e richieste da parte dell'opinione pubblica sono stati la spinta per l'organizzazione di un convegno sulla video sorveglianza dove si potessero incontrare città, istituzioni ed enti di ricerca.

Del "Presente e Futuro della Videosorveglianza per la sicurezza urbana" si è quindi parlato il giorno 20 Febbraio 2009 presso la sala della Fondazione Biagi di Modena, in un convegno organizzato dall'Università di Modena e Reggio Emilia in collaborazione col Comune di Modena.

Gli argomenti trattati sono stati appunto la videosorveglianza e il trattamento dei dati video sia in tempo reale, per la prevenzione e la salvaguardia del cittadini, sia a posteriori per l'analisi forense e il supporto nelle fasi processuali. Durante la giornata sono state presentate alcune esperienze significative di sistemi di videosorveglianza in ambiente urbano, collegando aspetti investigativi, tecnologici, giuridici

e sociali che implicano l'utilizzo dello strumento. Per questo motivo sono intervenuti al convegno il Dr. Giorgio Pighi, Sindaco di Modena, il Dr. Antonio Manganelli, Capo della Polizia, insieme a membri della Polizia, giuristi e professori universitari.

Questa pubblicazione raccoglie gli interventi presentati dai relatori durante la giornata e viene distribuita come atti del convegno. Non ha la pretesa di affrontare l'argomento in forma esaustiva, ma vuole comunque essere un valido supporto a sviluppatori, installatori, e utenti dei sistemi di videosorveglianza urbana, a chi vuole conoscere l'argomento e ai ricercatori informatici e giuridici.

Crediamo infatti che i video raccolti dalle telecamere urbane possano essere una preziosa risorsa se utilizzati correttamente e in rispetto della privacy per la sicurezza e la salvaguardia degli individui. Possono costituire una ineguagliabile fonte di informazioni come supporto alle indagini, possono fornire utile materiale processuale, e possono quindi costituire un deterrente per azione criminose. Ancor più crediamo che possano essere utilizzate, mediante l'intervento di nuove tecnologie di visione artificiale, per ottenere un monitoraggio automatico, prevenire situazioni di pericolo e fornire un ausilio alle forze dell'ordine e polizie locali, costante nel tempo e ubiquo sul territorio.

Rita Cucchiara
Antonio Assirelli
Roberto Vezzani

Saluto del Rettore dell' Università degli Studi di Modena e Reggio Emilia

Prof. Aldo Tomasi

L'attenzione prestata dal nostro Ateneo, e in particolare dal Dipartimento di Ingegneria dell'Informazione, al cruciale sviluppo delle tecnologie collegate alla videosorveglianza rivelano un interesse certamente non contingente, solo in quanto dettato dalla crescente pressione dell'opinione pubblica e dei cittadini per la creazione di efficaci sistemi di controllo e sicurezza del territorio, ma piuttosto la ferma convinzione scientifica del mondo accademico sulla utilità ed opportunità di coltivare competenze e professionalità nell'ambito della cosiddetta "Visione Artificiale" (computer vision).

Da questa intuizione è nato una decina di anni fa, prima ancora che le varie Istituzioni comprendessero e sviluppassero l'apporto della videosorveglianza alle politiche di sicurezza urbana, ImageLab, un'iniziativa che ha visto promotrice la prof. ssa Rita Cucchiara, specificamente dedicata agli studi ed alle applicazioni della visione artificiale, come disciplina informatica che realizza strumentazioni tecnologiche con comportamenti percettivi e visivi simili a quelli di un sistema umano applicabili a vari settori, che vanno dalla medicina allo studio dell'arte, fino ad arrivare alla videosorveglianza.

Proprio perché il tema del confronto, svoltosi a Modena nel febbraio scorso, "Presente e futuro dei sistemi di videosorveglianza per la sicurezza urbana" era focalizzato sulle questioni delle potenzialità offerte dal loro supporto a finalità di contrasto della criminalità e, quindi, di risorsa per lo sviluppo di politiche istituzionali e sociali di prevenzione, non va trascurato che il campo d'azione

della visione artificiale può e deve concorrere al progresso di molte altre attività. Esso – è nostra convinzione – è giusto debba trovare altre applicazioni, al di fuori dell'ambito della sicurezza urbana o delle indagini investigative.

Ciò nonostante, ci rendiamo conto che l'interesse oggi prevalente per questa disciplina, su cui convergono e a cui sono indirizzati cospicui finanziamenti locali, nazionali ed internazionali, è rivolto proprio alla videosorveglianza, anche se il trattamento dei dati video che se ne fa ai fini della salvaguardia dei cittadini non deve mai essere separato dall'esigenza di tutela più generale della privacy.

Si tratta di trovare, come spesso accade, i giusti equilibri nella difesa di diritti che hanno la medesima dignità e la stessa valenza.

L'appuntamento ha concorso a rispondere ad un duplice obiettivo: il primo come confronto scientifico tra i ricercatori che in numero sempre maggiore si occupano con successo di nuove soluzioni di sistemi di videosorveglianza automatica; il secondo come confronto con la società civile, con gli enti pubblici ed il mondo dell'impresa per mostrare quale grado di competitività e di avanzamento abbia raggiunto in questo settore, la ricerca italiana e modenese.

Le presenze e le tante autorevoli testimonianze e contributi portati a questo convegno stanno a testimoniare l'attualità dell'argomento, e più ancora il prestigio nazionale ed internazionale goduto dal gruppo dei nostri ricercatori dediti a questa disciplina, che ci ha posto in collaborazione coi più importanti centri di ricerca europei e statunitensi.

Saluto del Questore di Modena

Dr. Salvatore Margherito

La necessità di un controllo di vaste aree territoriali ha determinato nelle istituzioni pubbliche e private un sempre maggiore ricorso all'utilizzo di sistemi di videosorveglianza e al loro potenziamento fornendo alle forze dell'Ordine un utile strumento di contrasto della criminalità.

Il convegno è stato un'importante occasione di confronto sulle innovazioni relative al monitoraggio tecnologico tra esperti delle forze dell'ordine e ricercatori del settore della visione artificiale. L'incontro è stato particolarmente utile per evidenziare quali risultati abbia conseguito la ricerca italiana sino ad oggi e quanto essa possa contribuire nell'ambito della sicurezza pubblica.

Per fare fronte alla crescente e pressante richiesta di interventi, una delle possibili strategie deve essere quella di un approccio integrato che contrasti il fenomeno della criminalità urbana attraverso l'impiego di una vasta gamma di programmi preventivi, tra i quali i sistemi di video sorveglianza, appunto, nonché un nuovo approccio sistematico e razionalmente orientato sul tema sicurezza. Ovvero una sicurezza partecipata, cercata attraverso il concorso fattivo di tutti gli attori sociali, che nasca da un comune senso di appartenenza, da un processo di scambio. Più le società sono costituite da gruppi disposti a confrontarsi, più le persone si sentono sicure.

Saluto del Prefetto della provincia di Modena

Dr.ssa Giuseppina Di Rosa

Ritengo doveroso, in primo luogo, ringraziare gli enti organizzatori di questo convegno, Comune di Modena e Università degli Studi di Modena e Reggio Emilia, rappresentati dal Sindaco Giorgio PIGHI e dal Magnifico Rettore Aldo TOMASI, per l'opportunità offerta di approfondire aspetti relativi alla sicurezza nelle città ed alle nuove strumentazioni offerte dalla tecnica per la prevenzione dei fenomeni criminosi.

Un caloroso benvenuto in provincia di Modena desidero altresì porgere al Capo della Polizia, Dr. Antonio MANGANELLI, ringraziandolo per la Sua presenza ad una iniziativa dedicata a temi oggi al centro del dibattito pubblico, quali quelli della sicurezza pubblica ed in particolare della sicurezza urbana e della sua percezione da parte dei cittadini.

La presenza del Capo della Polizia è diretta testimonianza dell'interesse che l'Amministrazione dell'Interno e i vertici della Polizia di Stato riservano a tali problematiche nel territorio modenese.

La questione posta ad oggetto del convegno, "presente e futuro dei sistemi di videosorveglianza per la sicurezza urbana", si inscrive tutta all'interno della discussione sui mezzi e sulle risorse destinate alla prevenzione e repressione della criminalità ed è importante, anzi, direi, quasi naturale che essa sia trattata in Modena, luogo nel quale Stato e Autonomia Locale, il Comune, hanno sottoscritto il primo "protocollo d'intesa" e, poi, il primo "contratto di sicurezza" per individuare, condividere e realizzare politiche e progetti a tutela della legalità e della tranquillità della cittadinanza.

Possiamo, al riguardo, affermare con certezza che i sistemi, ai

quali è dedicata l'odierna giornata di studi, sono elementi portanti di quei documenti e dell'attuale "Patto per la Sicurezza", voluto per concretizzare i noti concetti di sicurezza partecipata ed integrata, affidati alla attuazione di diversi soggetti istituzionali nell'ambito delle proprie attribuzioni e rispettive competenze.

Si tratta di strumenti evoluti e efficaci che consentono di prestare un forte ausilio alla Forze di Polizia nel quotidiano servizio di controllo del territorio e permettono alle Amministrazioni Comunali di monitorare le situazioni di criticità all'interno delle aree urbane prevenendone il degrado.

Con fiducia si può, quindi, guardare alla utilizzazione di siffatte moderne tecnologie,che, impiegate con sapienza e non disgiunte dal mantenimento e dall'incremento delle tradizionali attività di polizia, non potranno che migliorare l'azione di contrasto al crimine.

Saluto del Sindaco Di Modena

Prof. Giorgio Pighi

Ringrazio anzitutto per la sua partecipazione al convegno il Capo della Polizia, Dott. Manganelli. Un ringraziamento all'Università e alla Questura di Modena, che assieme a noi hanno contribuito all'organizzazione della giornata. Un saluto alle Autorità e ai presenti in sala ed un grazie particolare alla Signora Marina Biagi, che ha fortemente voluto il convegno in questi ambienti, così pieni di significato per la città.

Il tema della videosorveglianza come strumento di ausilio per il controllo del territorio da parte delle Forze dell'Ordine e delle Polizie Locali è un tema che sul territorio è stato affrontato ormai da alcuni anni e pertanto abbiamo avuto modo di sperimentarne potenzialità e criticità.

A fronte di una domanda di sicurezza crescente che si esprime anche nella richiesta di installazione di nuove telecamere, e di risorse sempre più ridotte, abbiamo anzitutto il dovere di fare un'analisi attenta sull'efficacia delle misure che mettiamo in campo, anche in considerazione dell'investimento che molti Comuni sostengono per la realizzazione e per la manutenzione e gestione di sistemi di videosorveglianza urbana.

Per questo abbiamo colto volentieri l'idea di organizzare il convegno di oggi per cercare proprio di focalizzare, grazie all'aiuto degli esperti che interverranno oggi, quali conclusioni possiamo trarre dalle esperienze condotte, quali sviluppi possiamo prefigurarci e come la tecnologia potrà aiutarci a migliorare ancora di più le attività di controllo del territorio, facilitando le operazioni delle Forze dell'Ordine e delle Polizie Locali.

Provo quindi a fare alcune considerazioni che ci derivano dalla nostra esperienza. La peculiarità del progetto di videosorveglianza

del territorio, realizzato a Modena, è quella di essere nato come un sottoprogetto di un più complessivo programma di interventi di riqualificazione urbana dell'area della fascia ferroviaria, finalizzato a migliorarne le condizioni di sicurezza.

Questa idea di videosorveglianza traduce un po' il nostro approccio alle politiche di sicurezza urbana come politiche che vedono la partecipazione di diversi soggetti, istituzionali e no, e l'integrazione di azioni di carattere strutturale, di prevenzione sociale, di presidio formale del territorio da parte degli organi di polizia, anche avvalendosi di strumenti tecnologici.

Nello specifico, la realizzazione e la gestione del sistema di videosorveglianza installato è finalizzata a

- prevenire fatti criminosi attraverso un'azione di deterrenza che la presenza di telecamere è in grado di esercitare,
- sorvegliare in presa diretta zone che di volta in volta presentano particolari elementi di criticità o in concomitanza di eventi rilevanti per l'ordine e la sicurezza pubblica,
- favorire la repressione degli stessi fatti criminosi qualora avvengano nelle zone controllate dalle telecamere ricorrendo alle informazioni che il sistema sarà in grado di fornire e rassicurare i cittadini attraverso una chiara comunicazione sulle zone sorvegliate.

All'avvio del progetto, nel 2002, proprio per quanto già ribadito in precedenza, si è convenuto di sperimentare un sistema con un primo nucleo di circa 40 telecamere nella zona della fascia ferroviaria, spazio in cui erano previsti gli interventi di riqualificazione urbana. Su questo, come su altri progetti relativi alla sicurezza urbana, la collaborazione già esistente fra Comune e Prefettura/Forze dell'Ordine, nell'ambito dell'allora Contratto di sicurezza, ha agevolato la definizione di un progetto condiviso fin dall'inizio.

In particolare è stato attivato un gruppo di lavoro interistituzionale sul tema del controllo tecnologico del territorio, tuttora attivo, con il compito di monitorare dal punto di vista tecnico la funzionalità del sistema, rilevarne costantemente le criticità, migliorare gli elementi gestionali e suggerire sviluppi.

E' stata questa la sede per la definizione della collocazione delle telecamere e la definizione degli aspetti gestionali. Oltre alle conoscenze specifiche degli operatori di polizia circa le zone più problematiche, sono stati analizzati e mappati, da parte del Comune, alcuni dati, relativamente alle segnalazioni alla Polizia Municipale, alla raccolta delle siringhe, alla percezione dei cittadini attraverso il sondaggio d'opinione sui temi della sicurezza che annualmente viene realizzato, che nella maggior parte dei casi hanno confermato le valutazioni degli operatori di polizia sull'opportunità di installare una telecamera.

Dal 2002 ad oggi il sistema è stato notevolmente modificato, sia dal punto di vista qualitativo al fine di tenere il nostro sistema al passo con il miglioramento delle applicazioni tecnologiche, che quantitativo: il sistema di videosorveglianza urbano è attualmente composto da 70 telecamere di cui 57 di tipo brandeggiabile (7 di queste sono wireless con collegamento radio) e 13 fisse.

Nel corso degli anni e sulla base di una attenta analisi sulle aree che di volta in volta sono stata individuate dalle forze di polizia, anche a fronte di richieste da parte dei cittadini, il sistema è stato via via implementato, anche con finalità antiterrorismo, andando a monitorare anche obiettivi sensibili come ad esempio la Sinagoga e a protezione di alcune opere d'arte – Duomo e Cimitero Monumentale S.Cataldo.

Un percorso quindi condiviso e cogestito da Polizia Municipale, Polizia di stato, Carabinieri, ognuna dotata di una centrale di controllo per la visione e utilizzo in diretta delle telecamere. A breve verrà attivata una centrale di controllo anche presso la nuova sede della Guardia di Finanza.

Forte attenzione è stata prestata anche al tema della gestione del sistema in ordine agli aspetti relativi alla privacy in ottemperanza a quanto previsto dal decreto legislativo 30 giugno 2003 n. 196 e dal "Provvedimento generale sulla videosorveglianza " del 29 aprile 2004.

Per quanto concerne le attività di utilizzo della strumentazione da parte della Polizia Municipale, mi preme sottolineare che in questi anni, molte operazioni finalizzate al contrasto della prostituzione e

dello spaccio di sostanze stupefacenti, sono state realizzate con l'ausilio di questa strumentazione. Cito come modalità operativa spesso utilizzata dalla Polizia Municipale l'ultima operazione nei giorni scorsi in zona cittadella, dove gli operatori sul territorio, coadiuvati dai colleghi della sala operativa che visionavano in diretta le telecamere, hanno eseguito alcuni arresti per spaccio. L'attenzione con cui abbiamo individuato le aree urbane da monitorare ha fatto si che i responsabili di due omicidi avvenuti sul nostro territorio fossero individuati e arrestati nell'immediatezza degli eventi.

Le caratteristiche dell'impianto, le finalità dello strumento, le modalità di registrazione, le modalità di accesso ai dati, i responsabili del trattamento dei dati e le procedure per l'accesso alle informazioni registrate sono state definite all'interno di un Protocollo di Intesa tra Comune e Prefettura di Modena.

Tutto questo per dire che crediamo che il sistema abbia raggiunto una sua dimensione quantitativa e caratteristiche gestionali tali per cui ci sembra che una sola espansione quantitativa dello stesso sistema ci farebbe entrare in una fase di rendimenti decrescenti se confrontassimo costi e potenziali risultati.

Il costo degli investimenti finora sostenuto, completamente a carico del Comune di Modena, è di circa 1.300.000 €. A questi si aggiungono i costi della manutenzione e del canone della rete che ammontano a circa 170.000 € annui.

Per il futuro, ciò che il Comune di Modena sta cercando di realizzare, attraverso la collaborazione con l'Università di Modena e la ditta che ha in gestione l'impianto di videosorveglianza, è di sperimentare una serie di software di analisi della scena in ambiente urbano, che facilitino la rilevazione e la segnalazione agli operatori in tempo reale di eventi critici, in maniera automatica (ma di questo aspetto parlerà nel merito la prof.ssa Cucchiara), in modo da rendere più efficiente ed efficace il sistema attualmente in uso, facilitare il controllo del sistema da parte della Polizia Municipale e delle FF.OO e garantire un intervento tempestivo.

Quindi per il futuro credo che andranno sempre più ricercate soluzioni diversificate e maggiormente flessibili per frenare la tendenza ad un progressivo ampliamento dei sistemi a cui difficilmen-

te potrà corrispondere un impiego di personale dedicato all'utilizzo e alla gestione del sistema e che richiederebbe un investimento e soprattutto costi di manutenzione insostenibili per le Amministrazioni Comunali.

E' in questa direzione che stiamo quindi concentrando gli sforzi. Mi avvio alla conclusione citando un progetto cofinanziato dalla Regione Emilia-Romagna e che prevede la realizzazione di una stazione mobile di videosorveglianza che potrà garantire l'utilizzo della videosorveglianza in zone non coperte dall'attuale sistema garantendo quelle necessaria flessibilità e diversificazione degli strumenti a disposizione degli organi di polizia.

Prima di lasciare la parola al dott. Manganelli, approfittando della sua presenza, voglio fare una piccola divagazione dal tema del convegno.

La nostra città è caratterizzata in questi mesi da un confronto, a volte anche aspro, tra le forze politiche sul tema della sicurezza dei cittadini. Le Istituzioni, in primis il Comune, hanno messo in campo una serie di iniziative, di azioni e di investimenti particolarmente significativi; le sfide nuove non ci hanno mai spaventato, e non ci spaventano neppure ora. Siamo abituati ad affrontarle con pragmatismo, orientamento all'innovazione e alla soluzione dei problemi. Se non fosse così, non saremmo stati i primi a firmare un Protocollo, poi un Contratto e poi la prima città media a sottoscrivere un Patto per la sicurezza. E devo dire che la collaborazione con le Istituzioni decentrate dello Stato è sempre stata massima ed ha, pertanto, saputo sempre produrre risultati importanti.

Affinché realtà come le nostre, che noi consideriamo virtuose, possano però operare al meglio, ed ottenere risultati significativi occorre che dal livello nazionale arrivino alcuni segnali precisi:

- la nostra città, la nostra provincia non possono più contare su un organico delle forze dell'ordine fermo al 1989; il Sottosegretario Mantovano ci ha recentemente descritto il quadro di difficoltà in cui il Ministero si muove: ne prendiamo atto, ma non possiamo dichiararci soddisfatti. So che richieste di natura politica non le posso fare al Capo della polizia: al dott. Manganelli però chiedo di supportare i nostri operatori di po-

lizia con strumenti e con l'ausilio di reparti specializzati per fronteggiare, col contributo di tutti, alcuni fenomeni nuovi per la nostra realtà come le rapine in villa e nei locali pubblici, e per incidere in zone particolarmente critiche per problemi di ordine pubblico.

- occorre che il Parlamento approvi in fretta la riforma della Polizia locale: ci sono due proposte di legge simili, una di queste vede l'adesione compatta del sistema delle autonomie locali. Non si può aspettare oltre
- politiche locali di sicurezza, come l'istallazione di sistemi di videosorveglianza o come le azioni di riqualificazione urbana, non possono essere attuate senza risorse: occorre che lo Stato sostenga l'iniziativa degli enti locali anche con risorse finanziarie.

Siamo consapevoli che queste decisioni non dipendono dalla volontà del Capo della polizia ma, poiché sappiamo che egli è un convinto sostenitore della cooperazione tra soggetti istituzionali e dell'integrazione delle azioni, gli chiediamo di farsi promotore di un'azione verso il Governo e il Parlamento di sostegno a queste richieste.

"Sicurezza partecipata, sicurezza urbana, sicurezza integrata"

Dr. Antonio Manganelli
Capo della Polizia - Direttore Generale della Pubblica Sicurezza

Desidero, innanzitutto, porgere un saluto a tutti i presenti, oltre che un doveroso ringraziamento per l'invito a partecipare a questo incontro che ho accettato con molto entusiasmo. Sentimento questo che si unisce ad una certa emozione dovuta ai miei trascorsi presso questa Università, dove ho conseguito la specializzazione in criminologia clinica. Ed è per questo motivo che desidero, altresì, rivolgere un sentito ringraziamento al mio maestro Salvatore Luberto con il quale avviammo, anni fa, un comune percorso di ricerca in questo campo. Ringrazio, naturalmente, anche la fondazione Biagi, il cui nome deve richiamare il nostro Paese al dovere di sentire il peso quotidiano delle proprie responsabilità.

Quello della video sorveglianza è sicuramente un tema interessante, che si inquadra nel più ampio contesto della cosiddetta sicurezza partecipata ed integrata. Ciò mi consente di parlare delle politiche di sicurezza del nostro Paese, approfondendo il nuovo concetto di sicurezza, che non può più essere ricondotto soltanto alle attività di polizia, come comunemente si era soliti pensare.

Sicurezza oggi significa vivibilità dei nostri quartieri, qualità della vita, condizione per lo sviluppo socio-economico e per la crescita di una comunità. Per queste ragioni la sicurezza oggi non può essere vissuta un costo per il nostro Paese, ma deve essere considerata come un investimento. Investire per ottenere sicurezza rappresenta un'opportunità per migliorare gli standard di vivibilità di un Paese e dei suoi cittadini.

Ma il problema va affrontato anche cercando di comprendere le

ragioni dell'attuale interesse per la questione sicurezza. In genere, un dibattito pubblico cresce esponenzialmente quando si affronta un tema visto e vissuto con ansia e con angoscia dalla gente. Viene da credere, quindi, che i cittadini non si sentano sicuri. Potrà poi essere oggetto di uno specifico approfondimento la ricerca delle ragioni di questa insicurezza diffusa. In genere noi operatori di polizia le cerchiamo nelle statistiche sulla criminalità. All'aumento dei reati colleghiamo la paura della gente, le intenzioni ad armarsi, la volontà di non uscire la sera, il diffuso allarme che viviamo in questa società.

Credo però che in questo periodo più che sull'andamento della criminalità occorra riflettere su altri fenomeni che alimentano, in modo generalizzato, la paura, influenzano le profonde incertezze vissute quotidianamente, che non sono riconducibili sempre al concetto tradizionale di crimine. In effetti, la sola osservazione dell'andamento della delittuosità in Italia basata su confronti per macro periodi porterebbe a ritenere ingiustificato questo aumento della paura della gente. Il nostro Paese è stato travolto dalla mafia; se solo si pensa che trenta anni fa, nel giro di poco tempo, vennero barbaramente uccisi nella stessa città il Prefetto, il Procuratore della Repubblica, il Consigliere Istruttore, il Capo della Squadra Mobile, parlamentari impegnati nella lotta alla mafia. Così come, in un determinato periodo della nostra storia, il terrorismo interno colpiva quotidianamente o, ancora, accadeva che i sequestri di persona inondavano il nostro Paese, arrivando addirittura a 77 in un solo anno.

Quello attuale, invece, è un periodo in cui ci allarma il lavavetri, che comunque rappresenta un motivo di disagio, ma che deve far riflettere sulle reali motivazioni sottese all'incertezza diffusa dei nostri giorni.

È pur vero, peraltro, che la risposta alla domanda di sicurezza non può essere affidata ai riscontri statistici che, sia pur positivi, non possono rassicurare la gente. Né d'altra parte la risposta può essere fornita dalla militarizzazione del territorio, anche perché un territorio "blindato" genera ulteriori paure. La città sicura è quella che vive, che produce, che ha le luci accese, che vibra ed entusia-

sma, che motiva e che dà stimoli.

I cittadini hanno bisogno di risposte sociali e di legalità. Esiste la necessità, sicuramente, di prosciugare le sacche di degrado, in particolare urbano, che ancora umiliano il nostro Paese. Le risposte di legalità sono numerose e possono essere fornite da molti soggetti, soprattutto pubblici. Da parte nostra, indubbiamente, occorre migliorare le forme di controllo del territorio, soprattutto attraverso un rafforzamento degli strumenti di coordinamento e di interazione.

Occorre, poi, far funzionare meglio la giustizia, velocizzando i processi e dando concretezza al concetto di certezza della pena, dove credo i risultati siano stati talmente deficitari da poter affermare l'esistenza di una sorta di "certezza dell'impunità". Non serve promettere un castigo più duro, che inevitabilmente non arriva, quanto, invece, ottenere una pena effettiva e tale da neutralizzare, con le dovute forme di detenzione, l'autore del reato.

Ritengo sbagliato pensare che la prevenzione sia cosa completamente avulsa dalla repressione. Sono due momenti che necessariamente si interconnettono. Soltanto una concreta ed efficace azione repressiva riesce a prevenire effettivamente l'ulteriore offesa per la collettività: sia perché il criminale viene neutralizzato per un tempo adeguato, sia perché non si ingenera quel sentimento di illegalità che determina tanta insicurezza nella gente.

Un'altra risposta di legalità deve essere fornita sul fronte dell'immigrazione clandestina, tema da affrontare con determinazione e senza barriere ideologiche. Non si tratta né di confondere né di mettere a confronto le tendenze solidaristiche e di accoglienza, da una parte, con quelle di rigore, dall'altra. Occorre saper valorizzare l'apporto positivo degli immigrati regolari, che sono una grande risorsa per il nostro Paese, nel quadro di un necessario rigore per il rispetto delle regole. Evidentemente qualsiasi società civile presuppone delle regole, che vanno rispettate al di là di steccati di carattere ideologico.

Quello dell'immigrazione clandestina è un problema di legalità perché la popolazione carceraria è ormai costituita per circa il 34% da immigrati clandestini. Se poi andiamo a proiettare questo dato

nazionale nelle diverse realtà constatiamo che qui a Modena, ad esempio, la presenza straniera nelle carceri cresce a due detenuti su tre

E non basta l'impegno di magistrati e forze di polizia nel combattere il fenomeno; occorre risolvere, a monte, il problema della clandestinità. Per questa ragione stiamo in questo periodo completando un programma di accordi internazionali, sempre particolarmente complessi. Rimpatriare un clandestino è infatti un'operazione non facile; occorre, innanzitutto, identificarlo con la collaborazione dell'autorità consolare del presunto Paese di provenienza, che ovviamente deve essere disponibile a riprenderlo. È necessario, poi, individuare un vettore gradito a quel Paese, perché non sempre i Governi stranieri accettano i voli charter, pretendendo, a volte, che gli accompagnamenti avvengano solo su vettori di linea o che se ne trasportino solo due per vettore. Altri Paesi, inoltre, pretendono che non venga superato un certo numero mensile o annuale di rimpatri.

Accanto a questioni sociali e di legalità esiste, poi, un problema di percezione di insicurezza che, indubbiamente, negli ultimi anni, soprattutto all'indomani dell'11 settembre 2001, ha subito una particolare diffusione. È un fenomeno caratterizzato da una molteplicità di fattori e non sempre perfettamente corrispondente alla realtà oggettiva di pericolo proveniente dal mondo del crimine.

Gran parte dei fattori maggiormente ansiogeni sono quasi sempre svincolati da fenomeni criminali, quelli – in altri termini – riconducibili a fattispecie penali. Stiamo parlando di un vero e proprio disagio quotidiano dovuto a problemi economici, di integrazione etnica e culturale, di spaccature sociali sempre più evidenti, di incontrollata ed incontrollabile aggressività verbale e comportamentale, e così via. Ognuno di questi fenomeni è in grado di incidere sulla percezione di sicurezza che ciascuno di noi, quotidianamente, si costruisce nel proprio intimo.

Anche il villaggio globale in cui oggi viviamo è per se stesso generatore di insicurezza: nessuno inventa i pericoli, ma certamente i media li concretizzano, facendo violentemente entrare nelle case di ognuno di noi ogni genere di violenza verificatasi in qualsiasi

parte del mondo.

Così come appare indubitabile che alcune soluzioni urbanistiche ed architettoniche determinano gravi conseguenze sotto il profilo della sicurezza e della vivibilità quotidiana. Si pensi solo ai quartieri-ghetto, dove sono concentrate, in realtà fisiche sicuramente negative, popolazioni già contraddistinte da problematiche di ordine sociale ed economico che difficilmente riescono a trovare una positiva soluzione in quei contesti.

È ovvio, quindi, che lo schieramento dei soggetti da far scendere in campo per affrontare tali problematiche non può essere costituito solo dalle Forze dell'ordine.

Credo che solo con la sicurezza partecipata si possa rispondere alle esigenze che ho, sia pur sinteticamente, prospettato. La sicurezza partecipata - che io chiamo frequentemente anche sicurezza civica – persegue l'obiettivo della tranquillità sociale attraverso la partecipazione del cittadino allo svolgere quotidiano della vita della comunità.

Il problema della sicurezza va quindi affrontato in maniera interdisciplinare, secondo le diverse responsabilità dei ruoli ricoperti da ciascun attore. Giudico molto importante che proprio cominciando da questo tavolo ci sia un prefetto, un docente, un educatore, un rettore dell'Università, un sindaco.

Parlare di sicurezza partecipata significa mettere in rete le nostre risorse, fare squadra, creare un team che metta a fattor comune i contributi di ciascuno, per giungere ad un risultato convergente. Le Regioni, le Province, i Comuni, le associazioni di categoria, quelle di volontariato, insomma, le componenti sane della società, insieme alle forze di polizia, per fare squadra nel rispetto dei propri ruoli, nel rispetto delle proprie funzioni, ciascuno per la propria parte, ma in una convergente e sinergica azione.

Questa è sicurezza partecipata, questa è la sicurezza integrata che noi vogliamo realizzare e nell'ambito della quale si collocano le azioni che realizzano il partenariato tra Stato e Comune, tra Stato e Regioni.

E' questa la ragione per cui oggi pomeriggio, insieme al Vicecapo

della Polizia, il Prefetto Cirillo, e al Direttore Centrale Anticrimine, il Dirigente Generale Gratteri, approfondiremo con il Sindaco, con il Presidente della Provincia, con il Prefetto di Modena, i temi legati ad un patto per la sicurezza che è stato attuato in questa area. Ritengo che questi accordi rappresentino concretamente quello che noi vogliamo realizzare: una sicurezza che veda partecipi tutti, a cominciare dai sindaci.

L'entrata in campo di questi ultimi ha suscitato qualche perplessità: si è parlato di sindaco sceriffo, di sindaco che invade il campo, e così via. Il sindaco è legittimamente titolare della sicurezza urbana, concetto che ha proprio a che fare con il disagio sociale, con il degrado, con l'abusivismo, con le contraffazioni; tutto quel mondo assolutamente complementare a quello della pubblica sicurezza che le Forze di polizia dello Stato devono attuare.

Dunque, la sicurezza partecipata a cui facevo riferimento si esprime e si concretizza anche in queste forme di raccordo individuabili nei patti per la sicurezza, attraverso cui entrano in campo attori istituzionali che svolgono il loro ruolo, che mantengono la propria sfera di competenza nell'ambito del perimetro loro assegnato.

La pubblica sicurezza ha una sola autorità nazionale, prevista dalla legge, individuata nel Ministro dell'Interno, mentre, a livello territoriale, la responsabilità provinciale è attribuita al prefetto e, per gli aspetti tecnico-operativi, al questore. Queste sono le figure che la legge, con assoluta chiarezza, prevede come riferimento nel campo della pubblica sicurezza; tutto ciò che sta nascendo oggi è assolutamente complementare e necessario. Attraverso la sicurezza partecipata, la sicurezza integrata, la sicurezza urbana e civica si deve innescare una virtuosa, progressiva azione di interazione del contributo di tutti.

Noi, Forze di polizia, facciamo veramente la nostra parte, con dedizione e passione, con trasparenza, lavorando con assoluta onestà ed entusiasmo, consapevoli che in un Paese democratico deve essere garantito a tutti i cittadini l'esercizio dei propri diritti, a cominciare proprio da quello di liberarsi dalla paura.

La Videosorveglianza come Strumento di Contrasto della Criminalità

Dr. Elio Graziano
Dirigente Superiore della Polizia di Stato

1. Premessa

Il progressivo espandersi della videosorveglianza richiede una rimeditazione delle tecniche di controllo del territorio e pone alle forze di polizia problemi nuovi di formazione del personale e di ammodernamento delle tecnologie impiegate al fine di utilizzare pienamente le immagini registrate. Si avverte inoltre l'esigenza di una normativa nuova che disciplini organicamente la materia, in funzione di obiettivi generali di tutela della sicurezza dei cittadini, fatte salve le competenze del Garante della Privacy.

Non c'è dubbio che la videosorveglianza sia una risorsa preziosa per la sicurezza. Essa ha un'evidente funzione di prevenzione dei reati e, più in generale, dei comportamenti illegali. Inoltre, le immagini registrate costituiscono un supporto prezioso, una volta che la violazione di una norma si sia verificata, per l'identificazione dei responsabili.

I sistemi di videoripresa a circuito chiuso sono installati, diffusamente, a presidio di strutture pubbliche e private "a rischio". Cito ad esempio impianti sportivi, musei, aeroporti, stazioni, autogrill, supermercati oltre che, naturalmente, banche e uffici postali. Inoltre, negli ultimi anni, sempre più spesso questi sistemi sono impiegati per la vigilanza e il controllo di centri cittadini o di zone periferiche degradate (Fig.1).

Fig.1 – Tipologie di telecamere più frequentemente usate all'aperto

Fig.2 – Rilevamento delle impronte digitali

2. Funzione dissuasiva della videosorveglianza

Non è agevole quantificare l'effettiva capacità di deterrenza della videosorveglianza, né esistono ancora in Italia ricerche approfondite in merito. Una cosa si può dire con certezza: la capacità dissuasiva è più accentuata se le telecamere vengono collocate all'interno di spazi ristretti o, comunque delimitati, come le stazioni ferroviarie o gli impianti sportivi o a presidio di obiettivi sensibili ben identificati (per esempio scuole, luoghi di culto, ambasciate) e raggiunge la massima efficacia per attività a rischio o di custodia di valori che sono svolte in ambienti chiusi. Sulla base della mia esperienza professionale posso affermare che, a parità di condizioni, gli istituti di credito e gli uffici postali, non dotati di impianti di videosorveglianza sono maggiormente soggetti a rapine. Per queste tipologie di ambienti l'optimum è costituito dall'abbinamento della videosorveglianza ad un sistema di

Fig.3 – Rapina effettuata a volto coperto

acquisizione di dati biometrici. In particolare, negli istituti di credito si va sempre più diffondendo la prassi “virtuosa” di subordinare l’accesso alla rilevazione di impronte digitali: in questi casi gli autori di rapine sono il più delle volte identificati (Fig.2).

Se poi questi sistemi sono implementati, come si comincia a fare, con apposito software che impedisca l’accesso in banca ai soggetti di cui non si individui attraverso la telecamera un numero sufficiente di elementi fisionomici, lo loro efficacia dissuasiva cresce notevolmente. Infatti si sa che i rapinatori si sforzano di nascondere il proprio volto alle telecamere con camuffamenti vari, mentre temono di meno i metal detector, riuscendo a mettere a segno le loro azioni criminose anche con semplici taglierini (Fig.3)

E’ stato istituito presso l’ ABI ed è in attività da più di due anni l’Osservatorio sulla Biometria, in seno al quale un comitato tecnico, alle cui riunioni ho avuto la possibilità di partecipare, sta analizzando i sistemi più avanzati per proporre soluzioni che siano al tempo stesso efficaci e rispettose della privacy.

E’ certo, quindi, che negli ambienti chiusi la videosorveglianza svolga un ruolo decisivo di dissuasione dei comportamenti illegali. Nelle aree urbane non circoscritte la videosorveglanza ha generalmente un effetto positivo sulla percezione di sicurezza dei cittadini, ma non sempre produce in tempi brevi una diminuzione significativa dei reati. Bisogna considerare, però, che l’aumento della criminalità in alcuni periodi non è necessariamente da collegarsi ad un’inadeguatezza degli strumenti di contrasto ma può essere riconducibile a fattori diversi:

- esso può trovare giustificazione in fattori generali estranei a quel territorio e non governabili dagli organi preposti alla sicurezza cittadina: si pensi agli effetti dell’ indulto tra la fine del 2006 e il 2007. In periodi come questo è difficile valutare l’efficacia della videosorveglianza e degli altri strumenti di cui si avvale l’apparato di prevenzione in base al numero di reati commessi;
- per alcune tipologie di reato come quelli connessi alla droga e alla prostituzione, il loro aumento testimonia di una maggiore efficienza dell’apparato di contrasto. Tali reati, infatti, nella quasi

totalità dei casi vengono statisticamente registrati soltanto quando ne sono identificati gli autori.

A tutto ciò si aggiunga che mentre negli ambienti chiusi la videosorveglianza ha un'autonoma capacità dissuasiva di comportamenti illegali, può cioè bastare da sola a scoraggiare i malintenzionati, nelle aree urbane essa per dare i suoi frutti deve essere associata ad altre misure tecniche ed organizzative ed interagire con esse.

Infatti, è necessario un progetto organico ed integrato per la sicurezza urbana che sia elaborato in accordo tra autorità locali e organi di polizia e preveda interventi combinati e sinergici. Anzitutto la scelta delle aree nelle quali collocare le telecamere deve tenere conto delle indicazioni degli organi di polizia, che scaturisco-

Fig.4 – Centrale di controllo

no dall'esperienza operativa e delle segnalazioni dei cittadini. Le pattuglie sul territorio devono essere in numero congruo in modo da raggiungere tempestivamente, all'occorrenza, gli obiettivi pre-

sidiati, secondo gli input della sala operativa dove sono installati i monitor (Fig.4). L'attività preventiva e di pronto intervento deve essere combinata con una mirata azione investigativa da effettuarsi con personale in abiti civili. Le misure di polizia devono integrarsi con interventi di tipo urbanistico, come l' illuminazione cittadina nelle zone in cui manca o è scarsa, iniziative per rivitalizzare aree degradate, disincentivazione e, se necessario, smantellamento di agglomerati urbani "ghetto", che producono degrado e devianza.

Se inserita in un contesto di misure appropriate, la videosorveglianza consente di ricalibrare l'attività di prevenzione attraverso un monitoraggio costante del territorio.

3. La videosorveglianza a supporto dell'investigazione

Per accrescere la sicurezza reale, e non solo quella percepita dai cittadini è necessario che le misure di tipo preventivo siano corroborate da un'incisiva azione per l'identificazione degli autori dei reati commessi. A tal fine le immagini registrate possono fornire un contributo decisivo. Sono però necessarie tecnologie e professionalità avanzate.

Le apparecchiature impiegate devono possedere caratteristiche tecniche e standard di qualità adeguati e devono essere installate correttamente. Si devono utilizzare telecamere ad alta definizione, dotate di obiettivi sufficientemente sensibili e di meccanismi di compensazione per il controluce o l'insufficienza di luce. Devono essere, in congrua parte, brandeggiabili e dotate di zoom. La trasmissione delle immagini deve avvenire in modo rapido e la registrazione deve potersi attivare, mediante motion detector, soltanto quando una cosa o una persona entrino nel campo visivo dell'obiettivo, facilitando così la successiva ricerca ed analisi delle immagini per finalità investigative.

Le telecamere, infine, devono essere posizionate in modo da riprendere in primo piano e nitidamente persone e situazioni rile-

Fig.5 – Il rapinatore lascia le impronte. Le immagini aiutano gli operatori della polizia scientifica a rilevarle

vanti per il controllo del territorio e devono essere spostate in siti diversi se emergono nuove esigenze. E' necessaria un'adeguata formazione degli operatori di polizia addetti alle sale operative e di quelli degli uffici investigativi per poter sfruttare al meglio le opportunità offerte da questi sistemi.

Non conta soltanto la tempestività degli interventi nelle zone presidiate dalle telecamere: spesso l'intervento pur tempestivo non produce nell'immediato l'identificazione o l'arresto della persona che ha commesso un reato né la soluzione di una situazione di "criticità". Se, però, le immagini registrate posseggono sufficienti requisiti di nitidezza, possono costituire un supporto prezioso per identificare, in un momento successivo, gli autori di un'azione criminosa attraverso l' esame del loro volto e delle altre caratteristiche somatiche e comportamentali nonché dell'abbigliamento. Non

solo: la tempestiva visione del filmato agevola la ricerca, in sede di sopralluogo tecnico di polizia scientifica, delle tracce dei malviventi e, talvolta, la ricostruzione di dettagli importanti della dinamica criminosa (Fig.5).

Nell'attuale ordinamento processuale, caratterizzato dalla formazione della prova nel contraddittorio delle parti, l'acquisizione di dati oggettivi attraverso l'analisi delle immagini, può conferire particolare forza ad un'ipotesi accusatoria. Le immagini sono d'ausilio agli investigatori anche quando non documentino direttamente l'azione criminosa, ma solo gli spostamenti di soggetti che abbiano commesso un crimine altrove. La circostanza che una persona si trovi in un certo giorno e ad una data ora in una determinata località può assumere di per sé un valore decisivo per scoprire l'autore di un reato. Non si deve pensare soltanto alla cosiddetta criminalità diffusa, ma anche a reati più gravi e agli attentati terroristici, come dimostra l'attività investigativa svolta in occasione degli attentati di Madrid e di Londra.

In alcuni casi non è neppure pensabile di svolgere un'attività investigativa che risponda a criteri di efficienza e di economicità senza l'ausilio della videosorveglianza. Ad esempio sarebbe molto arduo identificare i responsabili di comportamenti penalmente o amministrativamente sanzionati all'interno di impianti sportivi.

Per valutare l'efficacia della videosorveglianza, forse, più che il numero dei reati commessi, bisognerebbe considerare quello dei reati scoperti utilizzando le immagini registrate

L'efficacia della videosorveglianza nella prevenzione della criminalità. Alcune esperienze locali e internazionali

Dr. Gian Guido Nobili
Responsabile delle attività di ricerca e progettazione della Regione Emilia Romagna in materia di sicurezza urbana

Da ormai una decina di anni la videosorveglianza è uno degli strumenti di prevenzione situazionale tecnologica a cui più frequentemente fanno ricorso la amministrazioni locali in Regione Emilia-Romagna. I contributi per la sicurezza urbana previsti dalla Legge regionale 3/99, poi sostituta dalla L.R. 24/2003 hanno concorso alla diffusione dei sistemi di videosorveglianza su tutto il territorio regionale (si veda il grafico in Fig.6). In aggiunta a questo canale di finanziamento, anche le iniziative di rilievo regionale, inserite negli interventi di riqualificazione urbana previsti dalla L.R. 19/1998 e noti come progetti pilota sulla sicurezza hanno sostenuto, tra l'altro, lo sviluppo di sistemi di videosorveglianza in quasi tutti i comuni capoluogo della regione.

Il finanziamento regionale è sempre subordinato al rispetto di alcune condizioni sostanziali in coerenza con quanto stabilito dall'Autorità garante per la privacy: l'individuazione specifica delle aree da videosorvegliare, la condivisione del sistema con le forze di polizia nazionali, l'adozione di un protocollo di gestione del sistema condiviso con le autorità di pubblica sicurezza.

Naturalmente si va da impianti semplici a sistemi piuttosto complessi come quelli in uso a Modena, Reggio Emilia e Bologna.

Lo sviluppo incessante delle tecnologie di sorveglianza consente oggi di estendere, in maniera virtualmente illimitata, la capacità fisi-

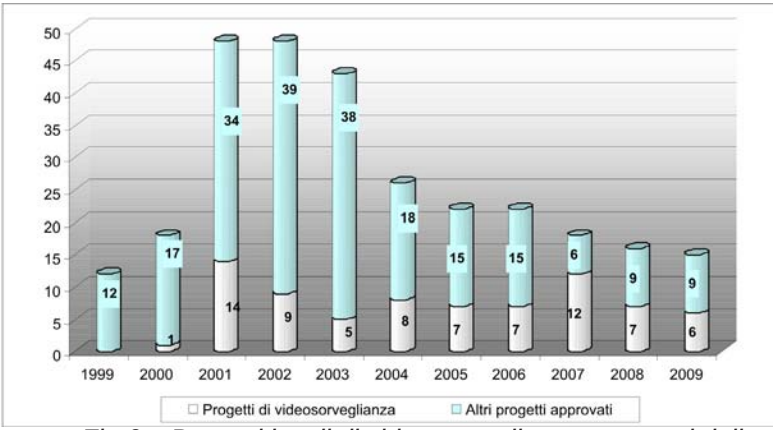

Fig.6 – Progetti locali di videosorveglianza sostenuti dalla Regione Emilia-Romagna e totale delle "iniziative di rilievo locale" in materia di sicurezza urbana finanziate dal 1999 al 2009 (valori assoluti).

ca degli operatori di polizia di vedere, sentire, riconoscere, memorizzare, conservare, incrociare, verificare, analizzare e comunicare dati e informazioni.

Le evoluzioni delle videotecnologie espandono la gamma di informazioni che possono essere raccolte e memorizzate (Chan, J.B.L.: 2003).

Tuttavia il progresso tecnologico dei mezzi di controllo non si è tradotto sistematicamente in miglioramenti delle attività di prevenzione e contrasto della criminalità. Per avanzare in maniera ragionata considerazioni circa l'efficacia della videosorveglianza, vanno necessariamente distinti due piani.

Comunemente infatti si tende a confondere i concetti di funzione di *deterrence* e funzione di *detection* esercitati dalla videosorveglianza (Caneppele S., Caso R., De Natale, F.: 2006). La prima attiene alla capacità dello strumento di prevenire il reato, la seconda attiene alla capacità dello strumento di identificare l'autore del reato, una volta che questo è stato commesso. La prima assolve una funzione tipicamente propria delle politiche di sicurezza locali,

la seconda, quella di *detection*, una funzione tipicamente propria delle politiche nazionali di sicurezza.

La prima è dunque la funzione di deterrenza esercitata dalle telecamere. In altre parole, secondo uno degli approcci più noti della criminologia attuale, quello delle attività di routine, tale funzione corrisponde a quella di "guardiano efficace" capace di impedire la convergenza nello spazio o nel tempo tra un aggressore motivato e la vittima o il bersaglio designato.

Ben diversa naturalmente è la funzione c.d. di "testimone affidabile", ossia la capacità delle telecamere di fornire un utile supporto, post evento, alle indagini investigative per individuare i responsabili.

È in particolare verso la dimensione preventiva delle telecamere, attinente alle competenze delle amministrazioni locali, che viene rivolta l'attenzione delle politiche di sicurezza urbana.

Ancor prima che in Italia, fin dall'inizio degli anni Novanta la videosorveglianza si era affermata come uno degli strumenti di prevenzione più diffusi nel Regno Unito. Una successo che ha certamente agito da volano per la diffusione della videosorveglianza nel resto d'Europa, ma che affatto paradossalmente non è legato all'ambito della prevenzione. È infatti unanimemente riconosciuto che il favore per la videosorveglianza sia stato in gran parte dovuto alla positiva pubblicità ricevuta dalla risoluzione di alcuni popolari episodi di cronaca nera grazie all'ausilio delle immagini riprese dalle telecamere (tra tutti, i casi Jamie Bulger a Liverpool nel 1993 e il Brixton-bomber "spara-chiodi" di Londra nel 1999).

Eppure l'efficacia apparentemente evidente e plausibile ha indotto il Governo centrale britannico a mettere a disposizione delle amministrazioni locali fin dal programma *Safer Cities* (1988-1995) i fondi per finanziare l'installazione di sistemi centralizzati di videosorveglianza e, in alcuni casi, offriva ai comuni che potevano documentare un aumento della criminalità un finanziamento fino ad un terzo del costo totale dell'opera.

Le stesse prime sommarie ricerche di valutazione sembravano confermare il successo delle iniziative e della complessiva strate-

gia del Governo.

È il caso del comprensorio di Swale, a sud-est di Londra, dove nel 1995 quattro piccole cittadine (Faversham, Milton Regis, Sittingbourne e Sheerness) al fine di contrastare la crescita della criminalità si erano consorziate per attivare un sistema centralizzato di videocontrollo del territorio. Secondo le statistiche ufficiali riportate, durante il primo anno di sperimentazione il totale dei reati commessi si era complessivamente ridotto del 46% rispetto ai dodici mesi precedenti.

Nuovi programmi di finanziamento ministeriale si sono succeduti fino al *Crime Reduction Programme* (CRP) che, annunciato nel 1998, ha messo a disposizione ben 170 milioni di sterline per sostenere un totale di 684 progetti di videosorveglianza nelle aree urbane.

Il convincimento che l'applicazione di una tecnologia - in questo caso le telecamere con funzione di "occhi remoti" a disposizione di operatori dedicati al controllo del territorio - possa garantire in maniera quasi meccanica maggiore sicurezza ai cittadini è peraltro smentito da tutte le ricerche più recenti.

Il determinismo tecnologico sottovaluta l'importanza del contesto fisico e sociale nel quale è calato lo strumento preventivo (Lyon, D.: 1994). Anche nel caso della videosorveglianza, l'efficacia dipende dall'interazione complessa di una serie di fattori tra cui in particolare: la gestione del sistema e l'integrazione con le attività ordinarie della polizia e di ogni altro personale di sorveglianza, oltre alla configurazione fisica e sociale del territorio.

Come anticipato, le prime indagini valutative avevano rafforzato le entusiastiche adesioni e il favore pubblico per la videosorveglianza.

Una più rigorosa analisi (Norris, C., Moran, J., Armstrong, G.: 1998; Welsh, B., Farrington, D.: 2002) ha mostrato quanto queste valutazioni fossero inadeguate: spesso realizzate da operatori coinvolti nell'implementazione dei sistemi di videosorveglianza, si basano semplicemente su dati statistici aggregati della criminalità

ufficiale raccolti dopo la realizzazione dell'intervento ed espressi frequentemente solo in percentuale, senza alcun riferimento ai valori assoluti. Inoltre la mancanza di casi controllo, la sottovalutazione dei fenomeni di dislocazione della criminalità in altre aree ed un monitoraggio solo estemporaneo degli indicatori prescelti non consentono a questi studi di dimostrare alcunché.

Per verificare se i sistemi di sorveglianza sono effettivamente in grado di ridurre la criminalità e la percezione di insicurezza e a quali condizioni, o ancora se alcune azioni devianti sono più influenzate di altre dalla presenza delle telecamere occorre rifarsi agli studi più rigorosi condotti oltremanica.

Oltre alle ricerche realizzate a livello locale, è possibile in particolare fare riferimento alla prima valutazione nazionale della videosorveglianza finanziata dal Ministero dell'Interno inglese, insieme al Dipartimento per i trasporti e gli enti locali (Gill, M., Spriggs, A.: 2005).

La presenza delle telecamere non sempre si è rivelata una misura in grado di contenere la criminalità e addirittura, in alcuni casi, gli svantaggi prodotti hanno sopravanzato i benefici.

Tuttavia, se non è possibile esprimere oggi un giudizio unanime sull'efficacia della videosorveglianza, esistono comunque sufficienti riscontri nelle ricerche effettuate in questi ultimi anni per affermare che gli effetti deterrenti delle telecamere variano significativamente a seconda del contesto di applicazione e delle tipologie di criminalità che si intende contrastare.

L'effetto della videosorveglianza sembra essere più efficace nel contenere i crimini contro la proprietà (Ratcliffe, J.: 2006; Armitage, R., Smyth, G., Pease, K.: 1999; Brown, B.: 1995), in particolare i furti di e su autoveicoli (Skinns, D.: 1998; Tilley, N.: 1993).

In questo senso i reati di tipo strumentale, come furti o rapine, che derivano da motivazioni opportunistiche, risultano essere tangibilmente influenzati dalla presenza delle telecamere, mentre nei reati di tipo espressivo, che nascono da azioni impulsive fini a se stesse, come le lesioni o le aggressioni, i benefici appaiono assenti o comunque più contenuti.

Una conclusione che sembra confermare, rispetto alle manifestazioni di criminalità predatoria, la teoria della scelta razionale sostenuta da Cornish e Clarke secondo cui un individuo delinque consapevolmente sulla base di un'analisi costi-benefici fondata su diversi fattori, quali ad esempio: la facilità a commettere un reato, la disponibilità di bersagli interessanti o la presenza o meno di testimoni.

La videosorveglianza sembra poi funzionare meglio nei piccoli centri urbani, in spazi ben delimitati. Queste dimensioni favoriscono una più adeguata informazione sullo specifica misura di prevenzione e di conseguenza l'intervento risulta, con maggiore facilità, socialmente condiviso.

Anche la recente valutazione nazionale condotta su 13 dei 352 progetti di videosorveglianza finanziati dal Ministero dell'Interno con la "Fase Due" del *Crime Reduction Programme* ha confermato molte delle conclusioni già evidenziate nelle precedenti ricerche locali.

Effettivamente l'adozione di sistemi di videosorveglianza all'interno dei parcheggi sembra esprimere in misura migliore le potenzialità preventive e i furti di autoveicoli rappresentano il reato che più di altri fa segnare un decremento significativo nelle aree coperte dalle telecamere.

Ancora una volta le ragioni dell'efficacia della videosorveglianza vanno ricercate nel contesto spaziale in cui la tecnologia è applicata.

I sistemi di videocontrollo registrano le migliori performance di riduzione della criminalità in aree caratterizzate da confini fisici ben visibili e da una quantità di accessi e di uscite ridotti e definiti che possono essere controllati in maniera ancora più agevole con l'ausilio delle telecamere (Gill, M., Spriggs, A.: 2005; Ratcliffe, J.: 2006).

Al contrario nelle aree residenziali e ancora di più nei centri cittadini, contraddistinti evidentemente da numerosi e differenti accessi aperti, gli interventi di controllo a distanza del territorio tendono a produrre risultati trascurabili.

Come era ragionevole supporre, quei sistemi che garantiscono una maggiore densità di telecamere nel territorio sottoposto a controllo a distanza, e di conseguenza una più ampia copertura, si dimostrano più efficaci nel contrasto della criminalità. Va tuttavia aggiunto che, se esiste una positiva correlazione tra densità degli "occhi elettronici" e riduzione dei reati, le ricerche realizzate dimostrano che il numero di telecamere rimane pur sempre un aspetto residuale rispetto all'importanza del loro corretto posizionamento e puntamento e ad un'adeguata conoscenza del contesto spaziale di intervento.

Una delle principali critiche alla diffusione delle tecnologie di controllo a distanza è basata sull'assunto che la presenza delle telecamere non sarebbe in grado di ridurre effettivamente la criminalità, ma solo di spostarla in altre zone urbane non coperte da sistemi di videosorveglianza (tra gli altri, Shaftoe, H: 2002).

Le ricerche recenti (Armitage, R., Smyth, G., Pease, K.: 1999; Gill, M., Spriggs, A.: 2005) sembrano smentire questa ipotesi. La dislocazione della criminalità da una zona videosorvegliata alle aree adiacenti o ad altre zone si dimostra un'evenienza piuttosto rara. Al contrario diversi studi (Poyner, B.: 1991; Skinns, D.: 1998) riportano un effetto di diffusione di benefici, in termini di contrazione della criminalità, nelle zone circostanti l'area sottoposta al videocontrollo. Tuttavia gli esiti della prima valutazione nazionale non hanno confermato queste ultime conclusioni: anche gli effetti di diffusione di benefici avrebbero dunque carattere residuale.

La scelta di ricorrere a sistemi di videosorveglianza degli spazi pubblici non è solo motivata dal proposito di ridurre la criminalità in un dato territorio, ma viene generalmente accompagnata dall'obiettivo dichiarato di attenuare la percezione soggettiva di insicurezza della popolazione.

In realtà i sistemi di videosorveglianza non sembrano esercitare significativi effetti positivi sulla valutazione personale del rischio di vittimizzazione, anzi non di rado l'introduzione delle telecamere viene interpretata come una riprova della maggiore pericolosità del territorio.

Se al contrario la più generale percezione di sicurezza tende ad accentuarsi nelle aree sottoposte a videocontrollo, le motivazioni non vanno comunque ricercate nella presenza delle telecamere. Piuttosto il miglioramento dei sentimenti di sicurezza va riferito alla riduzione dei tassi di vittimizzazione nelle aree videosorvegliate (Gill, M., Spriggs, A.: 2005).

Ancora, il grado di favore degli abitanti per la videosorveglianza rimane tendenzialmente elevato anche a seguito dell'installazione delle telecamere, tuttavia la gran parte dei sondaggi di opinione realizzati dopo l'avvio della sperimentazione riportano una diminuzione dei consensi, attorno al 20%, verso questo sistema di prevenzione. Il ridimensionamento del supporto verso la videosorveglianza è da attribuirsi non tanto al paventato timore di possibili interferenze nella vita privata dei cittadini, che in realtà rimane su dimensioni contenute, quanto ad una più realistica aspettativa nelle capacità preventive dei sistemi di controllo a distanza del territorio.

Naturalmente un giudizio completo sull'efficacia della videosorveglianza non dovrebbe tenere conto solo dell'andamento della criminalità ufficiale o della percezione di sicurezza dei cittadini, e non solo per i limiti che contraddistinguono questi possibili indici di valutazione.

Peraltro in alcuni casi il ricorso ad un sistema di videosorveglianza, anche se si accompagna ad un aumento dei tassi di criminalità registrata nella zona controllata, può essere successivamente stimato una misura di successo. Infatti, grazie alle immagini riprese dalle telecamere, un maggior numero di azioni devianti può giungere a conoscenza delle agenzie di controllo. Inoltre i cittadini possono essere maggiormente propensi a denunciare i reati subiti nella convinzione che le riprese delle telecamere possano agevolare l'identificazione dei responsabili o di eventuali testimoni.

L'efficacia della videosorveglianza dovrebbe essere misurata anche rispetto alla capacità di contrastare i fenomeni di inciviltà e disordine urbano o di agevolare le indagini per il ritrovamento di persone scomparse. Ancora, non andrebbe trascurato il fatto

che un'area videosorvegliata può attrarre una più ampia quantità di visitatori e favorire, come strumento di marketing territoriale, maggiori investimenti.

Come ormai appare chiaro, la potenziale efficacia della videosorveglianza dipende dalla sua adattabilità alle situazioni nelle quali i fenomeni di criminalità si manifestano. Ed è solo un'attenta analisi del contesto di intervento, delle tecnologie in uso ed adottabili e dei fenomeni che si intende contenere che ci permette di comprendere se esiste e qual è quel grado di adattabilità.

Una volta optato per l'attivazione di un sistema di videosorveglianza, l'installazione dei componenti - ossia telecamere, monitor, videoregistratori e mezzi trasmissivi - va sempre preceduta da una fase progettuale che preveda un adeguato sopralluogo della zona da controllare.

È auspicabile che il coinvolgimento degli utenti finali del sistema, in particolare il personale di polizia, cominci sin dalle fasi progettuali, anche per garantire una convinta adesione e un sostegno complessivo alla realizzazione dell'iniziativa.

L'attenta ispezione dell'area deve essere finalizzata a stabilire il più corretto posizionamento e orientamento delle telecamere. Occorre verificare, tra l'altro, che le fronde degli alberi non ostacolino le riprese nelle diverse stagioni dell'anno.

Va prestata attenzione all'illuminazione ambientale, sia essa naturale o artificiale, specie se sono previste riprese notturne, e va evitato, per quanto possibile, un puntamento delle telecamere nella direzione del sorgere o del calare del sole.

In generale le riprese con telecamere in bianco e nero risultano più definite e possono essere eseguite in condizioni di illuminazione decisamente inferiori rispetto a quelle a colori. Il ricorso a telecamere monocromatiche consente inoltre l'utilizzo di illuminatori a infrarosso che migliorano sensibilmente le riprese notturne.

Al contrario le telecamere a colori vanno preferite se dal sistema si desidera ottenere immagini ricche di maggiori riferimenti.

Qualora si abbiano condizioni di illuminazione variabile, come

spesso accade in ambientazioni esterne, è consigliabile ricorrere a telecamere dotate di obiettivi con regolazione automatica del diaframma. Nel caso di una intensa illuminazione retrostante il passaggio dei soggetti da sottoporre a controllo a distanza, è opportuno munire le telecamere di funzione “a compensazione del controluce”.

È evidente poi che la qualità delle riprese può essere danneggiata o resa difficoltosa a causa degli agenti atmosferici (pioggia, umidità, polveri, eccessivo calore) a cui sono esposte le telecamere. Anche per questi motivi l’ubicazione delle telecamere risulta di fondamentale importanza, naturalmente, ove necessario, è possibile ricorrere ad opportune custodie di protezione.

Per ridurre i rischi di atti vandalici o manomissioni, al di là della presenza sul mercato di apparecchiature di ripresa più o meno robuste, appare utile posizionare le telecamere di un sistema in maniera che queste si “coprano” vicendevolmente. Ogni telecamera sarà dunque in grado di mantenere sotto osservazione quella precedente e/o quella successiva. In questo modo qualsiasi eventuale aggressione alla singola unità di ripresa viene sempre registrata da almeno un altro “occhio elettronico” e, in un certo senso, il sistema assolverà anche una funzione di “autosorveglianza” (Bellintani, S., Giolfo, M.: 2002).

Ancora, possono essere privilegiate telecamere dotate di apparati per il brandeggio oppure unità di ripresa fisse. Queste ultime garantiscono generalmente immagini precise e definite dell’evento posto sotto osservazione, tuttavia, in ragione della loro staticità, possono più facilmente causare un calo di attenzione negli operatori addetti al monitoraggio delle immagini (Gill, M., Spriggs, A: 2005).

I progettisti ultimamente tendono a privilegiare le telecamere brandeggiabili, ossia dotate di un sistema di regolazione automatica dei movimenti di puntamento in senso orizzontale (PAN) e verticale (TILT) da postazione remota. Gli apparati di brandeggio, sempre caratterizzati dalla presenza di un obiettivo zoom, consentono di modificare l’inquadratura a piacimento, a seconda delle necessità del caso, al fine di ampliare il campo di azione delle telecamere

(Bellintani, S., Giolfo, M.: 2002).

La principale controindicazione dei dispositivi di brandeggio, in particolare quando la velocità di rotazione delle telecamere è automatizzata, può essere rappresentata dal fatto che le riprese rischiano di "lasciarsi sfuggire" l'insieme o parte delle azioni che hanno caratterizzato un evento criminoso.

In generale nel caso di adozione di un sistema di videosorveglianza per il controllo degli accessi è sempre consigliabile ricorrere ad un'unità di ripresa fissa che riprenda in primo piano, di fronte e di profilo destro, ogni soggetto che entra nell'area controllata. All'interno poi è utile avere una telecamera che riprenda la figura intera dei soggetti che accedono nell'area, se necessario la funzione c.d. di "esclusione zone" consentirà di oscurare alcune porzioni dell'immagine per tutelare ad esempio il rispetto del diritto alla privacy degli operatori che lavorano della struttura vigilata. Vanno inoltre previste una o più telecamere che inquadrino gli spazi esterni dell'area videosorvegliata, al fine di poter riprendere le immagini di eventuali complici o dei mezzi di fuga.

Infine non va sottovalutata la fase di gestione delle immagini.

Uno dei problemi più frequentemente segnalati dagli operatori addetti al monitoraggio delle riprese è dato dalla visione continuativa di immagini poco significative che può facilmente causare distrazioni o cali di attenzione.

Innanzitutto si consiglia un numero di monitor non superiore a sei per ciascun operatore, inoltre i sistemi di videosorveglianza digitale, grazie a strumenti di elaborazione software del segnale video, possono agevolare significativamente l'attività di controllo (Cucchiara, R.: 2008). È il caso, solo per citare uno degli esempi più noti, del *motion detector* (letteralmente: rilevatore di movimento), una funzione in grado di riconoscere automaticamente situazioni di pericolo, predefinite dall'utente del sistema, quali ad esempio: movimenti specifici all'interno della ambientazione inquadrata, la presenza di automobili in aree determinate o l'occlusione di oggetti o aree normalmente visibili.

Con questa funzionalità, quando il sistema rileva una delle si-

tuazioni a rischio, determinate in precedenza in base alle caratteristiche del luogo e alle potenziali azioni da sorvegliare, attiva automaticamente la connessione con la centrale operativa ed è in grado di inviare allarmi e immagini, e nel caso di attivare registrazioni o di salvare quelle cicliche normalmente effettuate, secondo le procedure stabilite dall'operatore.

Più in generale, va poi riconosciuto che le attuali tecnologie digitali offrono prestazioni nettamente superiori a quelle analogiche, in particolare rispetto alla qualità della registrazione e alle maggiori opportunità di analisi ed elaborazione delle immagini.

Per concludere questa breve e solo esemplificativa serie di suggerimenti, va rimarcata l'importanza del ciclo di vita della videosorveglianza, un aspetto spesso tralasciato, e che invece assume particolare rilevanza ai fini dell'efficacia preventiva dei sistemi di videocontrollo. Numerosi studi (Armitage, R., Smyth G., Pease, K.: 1999; Brown, B.: 1995; Tilley, N.: 1993) hanno rivelato che, anche a fronte di un'iniziale riduzione della criminalità, gli effetti positivi della videosorveglianza tendono a svanire se i sistemi installati non continuano ad essere adeguatamente pubblicizzati. Al contrario, ma a conferma del ruolo centrale giocato da organiche e mirate campagne di comunicazione, le stesse ricerche hanno dimostrato che gli effetti positivi indotti dalla videosorveglianza iniziano a dispiegarsi anche antecedentemente all'attivazione delle telecamere, sempre che, beninteso, la collettività ne conosca l'esistenza.

In conclusione, l'efficacia preventiva della videosorveglianza, apparentemente evidente, plausibile e immediata, dipende piuttosto dall'interazione delle circostanze in cui si manifesta il reato che si intende prevenire, dalla configurazione fisica del territorio, dal tipo di telecamere adottate, dal loro posizionamento, dalle modalità di controllo e dalla preparazione del personale di sorveglianza.

Non solo, anche la comunicazione rappresenta un fattore critico per la sostenibilità nel tempo di questa misura di prevenzione tecnologica. Inoltre, come le ultime ricerche dimostrano (Fussey, P.: 2007; Gill, M., Spriggs, A.: 2005), le probabilità di successo aumentano se la videosorveglianza viene integrata da altre misure

di prevenzione, ad esempio: il potenziamento dell'illuminazione, l'attivazione di progetti di sorveglianza del vicinato o di riqualificazione urbana.

L'importanza di combinare la videosorveglianza con altre misure di prevenzione è confermata anche da una delle poche ricerche condotte in Italia per valutare l'impatto di un diffuso sistema di videosorveglianza locale composto di oltre 200 telecamere nel Comune di Reggio Emilia. Dai primi dati forniti dalla Questura, emerge che la videosorveglianza non produce effetti significativi, se non è accompagnata da ulteriori azioni di presidio del territorio. In quelle aree dove il videocontrollo a distanza è combinato organicamente con un servizio di prossimità, si registrano invece tangibili riduzioni della criminalità, che in alcune zone raggiungono contrazioni di oltre 30 punti percentuali (Nobili,G.G.: 2009).

Lo stato attuale delle conoscenze consente dunque agli attori delle politiche di sicurezza urbana di cominciare ad orientare consapevolmente l'adozione dei sistemi di videosorveglianza verso specifiche finalità di prevenzione, nel contempo sollecita ulteriori approfondimenti sulle complessive implicazioni legate all'uso delle nuove tecnologie di controllo degli spazi pubblici.

Se possiamo dunque escludere che la videosorveglianza possa essere considerata la panacea contro la criminalità, vanno comunque riconosciute le grandi potenzialità di uno strumento in continua evoluzione che, se adeguatamente utilizzato, può contribuire, evidentemente insieme ad altre misure, a garantire condizioni di maggiore sicurezza negli spazi urbani.

Bibliografia:

ARMITAGE, R., SMYTH, G., PEASE, K.

1999 Burnley CCTV Evaluation, in Painter, K. e Tilley N. (eds.), Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention, Monsey, NY: Criminal Justice Press, pp. 225-250.

BELLINTANI, S., GIOLFO, M.,

2002 La televisione a circuito chiuso (TVCC), in Bombelli, F. (a cura di), La sicurezza negli edifici, Milano, Il Sole 24 Ore, pp. 109-129.

BROWN, B.

1995 CCTV in Town Centres: Three Case Studies, Police Research Group Crime Detection and Prevention Series, Paper n. 68, London: HMSO.

CANEPPELE, S., CASO, R., DE NATALE, F. (a cura di)

2006 I sistemi di videosorveglianza 2. Videosorveglianza e privacy: quadro normativo, casistica e aspetti tecnici. Trento: Provincia autonoma di Trento - Giunta.

CHAN, J.B.L.

2003 Police and new technologies in Newburn T. (eds.), Handbook of Policing, Devon: Willan publishing, pp. 655-679.

CUCCHIARA, R.

2008 La visione artificiale per la video sorveglianza, in “Mondo Digitale”, n. 3, pp. 38-47.

FUSSEY, P.

2007 Efficacia ed effettività della TVCC: la lezione inglese, in “Essecome”, n. 12, pp. 51-54.

GILL, M., SPRIGGS, A.

2005 Assessing the impact of CCTV, Home Office Research Study, n. 292, London: HMSO.

LYON, D.

1994 The Electronic Eyes: The Rise of the Surveillance Society, Cambridge: Polity Press.

NOBILI, G.G.

2004 La valutazione dei programmi per la sicurezza urbana. Il caso della videosorveglianza nell’esperienza britannica, in “Inchiesta”, n. 143, pp. 102-109.

2009 La videosorveglianza come strumento di prevenzione, in Il contributo della ricerca socio-criminologica alle politiche di sicurezza urbana, Atti del 2° seminario di studio organizzato dalla Regione Liguria a Genova, 29 maggio 2007, in corso di stampa.

NORRIS, C., MORAN, J., ARMSTRONG, G.

1998 Surveillance, Closed Circuit Television and Social Control, Aldershot: Ashgate.

POYNER, B.

1991 Situational Crime Prevention in Two Parking Facilities, in ”Security Journal”, n. 2, pp. 96-101.

RATCLIFFE, J.

2006 Video Surveillance of Public Places, in “Problem-Oriented Guides for Po-

lices. Response Guides Series", n. 4, pp. 1-73.

SAVONA E.U., CANEPPELE S. (a cura di)

2004 I sistemi di videosorveglianza. Trento: Provincia autonoma di Trento - Giunta.

SHAFTOE, H.

2002 The Camera never lies but, in truth, is it any use?, in "Community Safety Journal", n. 1, pp. 27-30.

SHORT, E., DITTON, J.

1996 Does Closed Circuit Television Prevent Crime? An Evaluation of the Use of CCTV Surveillance in Aidrie Town Centre, Edinburgh, SCOT: Scottish Office Central Research Unit.

SKINNS, D.

1998 Crime Reduction, Diffusion and Displacement: Evaluatingthe Effectiveness of CCTV, in: Norris C., Moran J. and Armstrong G. (eds.), Surveillance, Closed Circuit Television and Social Control, Aldershot: Ashgate, pp. 175-188.

SQUIRES, P.

1998 An Evaluation of Ilford Town Centre CCTV Scheme, Brighton, UK: Health and Social Policy Research Centre, University of Brighton.

TILLEY, N.

1993 Understanding Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities, Crime Prevention Unit Series, Paper n. 42, London: HMSO.

WELSH, B., FARRINGTON, D.

2002 Crime Prevention Effects of Closed Circuit Television: A Systematic Review, Home Office Research Study, n. 252, London: HMSO.

Utilizzo, in ambito forense, di metodologie informatiche per l'analisi e la sintesi di scene, eventi e soggetti.

Prof. Nello Balossino
M. Lucenteforte, L.Piovano, S.Rabellino, S.Siracusa, C. Mattutino
Dipartimento di Informatica - Università degli Studi di Torino

1. Introduzione

Sono molte le applicazioni in ambito forense che traggono significativi vantaggi dall'utilizzo di sistemi informatici, intesi sia nella componente hardware (sensori, dispositivi di acquisizione in zone diverse dello spettro elettromagnetico, apparecchiature di analisi e di restituzione dei risultati) sia in quella software (pacchetti per l'analisi di immagini, per la modellazione di ambienti, per la simulazione di eventi, per il trattamento statistico); lo scopo principale dell'elaborazione informatica consiste nel fornire risposte adeguate a quesiti posti da giudici (per i periti) e pubblici ministeri (per i consulenti tecnici) nell'ambito di procedimenti penali.

Va detto subito che la scelta della metodologia che si può utilizzare nell'elaborazione dei dati rilevati è fortemente legata al tipo di problema in esame e al margine di errore che può essere tollerato nei risultati. Le soluzioni proposte possono essere poi di tipo manuale (non viene utilizzato alcun dispositivo automatico ma si fa uso esclusivo della valutazione da parte dell'esperto del dominio), semiautomatico (si utilizzano sistemi informatici e di valutazioni da parte dell'operatore), automatico (il sistema informatico fornisce risultati e propone azioni da intraprendere che possono essere comunque soggette a validazione da parte dell'operatore). Le aree scientifiche coinvolte in ambito forense spaziano dalla biologia,

alla medicina, dalla fisica, alla antropometria.

Una grossolana classificazione degli ambiti investigativi [1] in cui ci si può trovare a operare mediante metodologie informatiche è la seguente:

- elaborazione di immagini: miglioramento e ripristino di qualità;
- classificazione e confronto di dati biometrici;
- ricostruzione tridimensionale di soggetti, ambienti, scene;
- animazione di scene ed eventi;
- simulazione di eventi e sistemi di realtà virtuale.

L'elencazione sopra riportata rispecchia, in ordine crescente, la complessità fisica, matematica e informatica che occorre affrontare.

Nella memoria gli autori riportano considerazioni generali sugli ambiti di cui sopra, ma principalmente le loro più significative esperienze condotte nel campo della videosorveglianza nella più ampia accezione del termine, includendo quindi l'analisi di operazioni di indagine ambientale, di riprese video e fotografiche da parte di enti e/o soggetti privati, nonché la sintesi di ambienti, eventi, fatti, fenomeni al fine di verificare l'attendibilità con quelli reali.

2. **Elaborazione di immagini: miglioramento e** ripristino di qualità

Le immagini tratte dai sistemi di videosorveglianza non sempre permettono una proficua analisi del loro contenuto che permetta di ottenere, per scopi investigativi [2], informazioni significative e prive di ambiguità. Ne segue che è sovente necessario eseguire pre-elaborazioni per compensare (quando possibile) difetti di acquisizione del sistema.

Dopo aver provveduto a effettuare una copia del materiale a disposizione in modo tale da preservare l'originale, occorre generalmente procedere all'applicazione di opportune elaborazioni di miglioramento di qualità [3] (che non considerano la modellazione della fonte effettiva di deterioramento dell'immagine).

I due casi più semplici consistono nell'eliminazione delle distorsioni geometriche (effetto botte o barile) e nel riscalamento della luminanza per immagini sotto esposte o sovraesposte (illuminazione non corretta). Relativamente alla risposta cromatica (che può sembrare corretta ma non permette comunque di asserire l'effettiva corrispondenza con la realtà), occorre sottolineare che le immagini non cromaticamente corrette non portano alcun contributo informativo importante; ne segue che è opportuno convertirle in immagini a livelli di grigio e sfruttare la migliore risposta dell'occhio alle variazioni dell'intensità luminosa, rispetto alla crominanza.

Per quanto riguarda la dimensione dell'immagine (detta sovente risoluzione anche se questa è legata alla estensione del supporto su cui l'immagine viene rappresentata), più grande è la dimensione dell'immagine più dettagliati risultano i particolari in essa presenti; una maggiore dimensione permette poi, contenendo l'effetto del tassellamento, di effettuare ingrandimenti, utili per apprezzare meglio i dettagli informativi.

I software a disposizione per l'elaborazione di immagini sono molti, ma quelli privilegiati dagli autori sono:

- Matlab [W1] con i toolbox di Image Processing e Image Acquisition, che possiede innegabili caratteristiche di versatilità e permette all'utente il completo controllo dell'azione svolta (l'utente sa qual è l'algoritmo che viene applicato ed è in grado di giustificare i risultati ottenuti)
- Nip2-Vips [W2] che oltre a possedere analoghe caratteristiche di Matlab, trattandosi di un software specifico per l'elaborazione d'immagini, è corredato di un'interfaccia che ne permette un facile utilizzo da parte dell'utente.
- Eidoslab [W3], software sviluppato dagli autori che permette di eseguire con molta facilità una serie di elaborazioni nel dominio spaziale (immagine intesa come distribuzione spaziale di luminanza) e in quello delle frequenze (dominio della trasformata di Fourier, in cui i segnali sono scomposti in una somma pesata di componenti sinusoidali e cosinusoidali).
- OpenCV [W4], libreria di classi C++ per la Computer Vision.

Fig.7 – sfocatura da movimento (sinistra) e ripristino con modello di filtraggio alla Wiener (destra)

A volte si può fare anche uso di Photoshop [4] o di altri software di fotoritocco, almeno per le elaborazioni in cui è evidente quali sono gli algoritmi utilizzati.

Occorre sottolineare come sia fondamentale in ambito scientifico che i software di elaborazione di immagini prevedano la creazione di metodi di documentazione che riportino le azioni intraprese, ciò al fine di poterle eventualmente ripetere se richiesto.

Relativamente al miglioramento di qualità occorre sottolineare che non esistono procedure standardizzate ma bisogna agire sulla base delle necessità richieste dal caso preso in esame. Vale la pena ricordare che se alcuni inestetismi possono essere risolti mediante elaborazioni tipiche del miglioramento di qualità, maggiormente complesso è il caso in cui l'immagine sia corrotta da rumore additivo o presenti, per esempio, la tipica sfocatura da movimento.

Questo effetto lo si riscontra nell'acquisizione di scene con soggetto in movimento, come per esempio mezzi di trasporto, in cui la targa risulta sovente illeggibile. In questi casi è opportuno operare nel dominio trasformato e simulare la fonte di rumore al fine di poter agire sull'immagine con azioni di ripristino di qualità (si può modellare la fonte di deterioramento).

Come esempio di ripristino di qualità, la Fig.7 riporta il caso di sfocatura da movimento e la corrispondente immagine ripristinata utilizzando il modello di filtraggio alla Wiener [3].

Il miglioramento e ripristino di qualità costituiscono il presupposto per la successiva analisi del contenuto informativo delle immagini forensi.

3. Classificazione e confronto di dati biometrici

3.1. Generalità

La videosorveglianza coinvolge il procedimento di riconoscimento di soggetti e si pone due distinti obiettivi:

- la verifica della dichiarazione di identità di un soggetto (il soggetto dichiara la sua identità posando di fronte a un sistema che acquisisce l'immagine, confrontandola con quelle precedentemente associate al soggetto stesso)
- l'attribuzione di una identità o identificazione di un dato soggetto (l'identità del soggetto non è nota e occorre associargliene una).

In entrambi i casi si tratta di stabilire se il confronto fra due soggetti, sulla base della valutazione di un insieme di descrittori (feature), cioè di elementi di caratterizzazione dei segmenti anatomici presi in esame, permetta o meno di formulare un giudizio di espressione della medesima realtà.

I descrittori utilizzati per il confronto possono essere di tipo anatomo-fisiologico ed essere quindi legati alla struttura e al funzionamento di segmenti del corpo umano (ad esempio il volto e l'orecchio) oppure di tipo comportamentale e riferiti pertanto alle modalità con cui un soggetto svolge un'azione (per esempio la postura assunta in una posizione statica o la deambulazione). I descrittori possono essere classificati come qualitativi (come esempio banale, l'altezza definita come bassa, media, alta) oppure quantitativi (per esempio altezza di 180 cm, definita come valore numerico rispetto a un'unità di misura).

La scienza che definisce e codifica i descrittori del corpo umano e stabilisce anche le regole per le elaborazioni e l' interpretazione dei risultati è la biometria. Poiché è molto variegata la casistica nella quale ci si trova a operare, non possono essere predefinite le azioni che occorre intraprendere nel procedimento di riconosci-

mento. Ciò sta a significare anche che sono diverse le tecniche biometriche necessarie per la verifica d'identità rispetto a quelle che vengono coinvolte nel processo di attribuzione di identità; il secondo caso risulta essere molto più complesso.

Il segmento anatomico che viene coinvolto nel procedimento identificativo è generalmente il volto. Come noto, il riconoscimento di un volto da parte dell'uomo è uno dei meccanismi più sofisticati della percezione ed è basato su parametri discriminatori qualitativi che non sempre sono sufficienti per giungere a classificazione certa; ne segue che può essere necessario ricorrere a dati quantitativi di tipo antropometrico. Va anche subito detto che l'approccio completamente automatico del riconoscimento di volti trova applicazione e giustificazione in ambiti di controllo di strutture tutelate da norme di sicurezza in cui il confronto deve avvenire contestualmente all'accesso (banche, enti militari e di ricerca, aziende). Si tratta del confronto uno-uno (e si cade nel caso di verifica d'identità), ma non si presta bene quando si debba procedere all'identificazione di soggetti sospettati di azioni illegali e indicati dalle forze dell'ordine o dall'autorità giudiziaria. In questo caso si esegue un confronto uno-molti (un reo e più indagati) e si tratta proprio di identificazione, che richiede un minor margine di errore nella valutazione del grado di compatibilità tra i soggetti a confronto, validata generalmente dal consulente/perito.

3.2. Confronto fisionomico

Da quanto detto, appare evidente come il processo di identificazione in ambito giudiziario sia condotto in modo semiautomatico, prendendo in esame le caratteristiche morfometriche e utilizzando strumenti informatici sia per l'esaltazione ed estrazione dei dati, sia per la loro elaborazione.

La morfologia di un volto è espressa mediante un insieme di descrittori di base, i cosiddetti connotati (sovente non sufficienti a identificare una persona quando si consideri per esempio il colore dei capelli) che venivano [5] (Alla fine del XIX secolo il francese Alphonse Bertillon introdusse un metodo di segnalamento descrittivo per scopi identificativi, sviluppato sulla base delle annotazioni

acquisite sulle caratteristiche dei detenuti parigini) e vengono tuttora riportati nelle schede di segnalazione di soggetti. I connotati sono espressi in forma testuale su proposta di ricercatori nazionali e internazionali fra i quali vanno ricordati Falco [6], Martin & Saller [7], Iscan &Loth [8]; è molto utile che la descrizione testuale sia accompagnata da una codifica grafica che facilita la cattura dell'aspetto del parametro fisionomico e rende maggiormente uniforme e più oggettiva l'analisi condotta da operatori diversi. Testi che sintetizzano i descrittori e la loro rappresentazione grafica sono per esempio quelli sopra citati e anche i seguenti [9], [10], [11]. Nel caso in cui il connotato assuma una particolare conformazione (per esempio naso molto gibboso) diventa fortemente caratterizzante e quindi singolare, assumendo la caratteristica di connotato saliente (caratteri non comuni della forma del volto o del profilo del naso).

In particolare sul volto possono essere rilevabili caratteri inequivocabili, segni particolari che per tipologia e posizione sono ascrivibili solo a un particolare soggetto; ci si riferisce allora ai con-

Fig.8 – Esempio di rilievo di connotati.

trassegni (come nel caso di nevi, cicatrici, rughe con particolari morfologie) che posseggono un forte potere discriminatorio.

Per quanto riguarda i descrittori metrici, questi possono essere di varia natura e consistere in misure assolute (per esempio peso e altezza, larghezza e altezza del volto) oppure in rapporti fra misure di segmenti che collegano punti o zone di repere e sono indipendenti dai fattori di scalamento; si tratta cioè di indici antropometrici, come per esempio l'indice facciale definito dal rapporto tra larghezza e altezza del volto. In alternativa agli indici antropometrici ci si può riferire a linee di evoluzione dei segmenti del volto, ossia a ciò che viene indicata come impronta o mappa facciale.

Osserviamo che il punto di partenza del processo identificativo consiste generalmente nella comparazione delle immagini estratte dai sistemi di videosorveglianza con quelle acquisite all'atto dell'accertamento, oppure precedentemente inserite in un archivio. Occorre pertanto sottolineare come la natura del fotogramma (frame) ricavato dal dispositivo di videosorveglianza influisca notevolmente sul procedimento di identificazione. Se per esempio le riprese sono sufficientemente nitide, ricche di dettagli immediata-

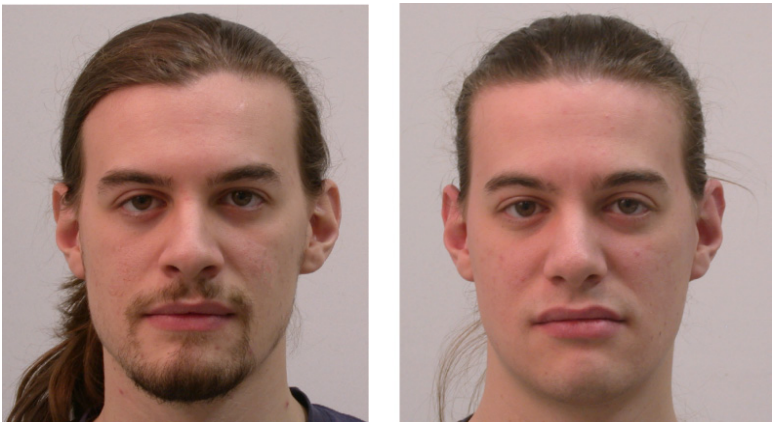

Fig.9 – Esempio di gemelli omozigoti

Fig.10 – Profilo destro della coppia di gemelli

mente deducibili, nonché raffigurino soggetti senza alcuna forma di mimetismo, saranno per lo più sufficienti confronti morfologici che evidenzino la presenza in entrambi i soggetti di un certo numero di descrittori di base. In caso contrario, è opportuno verificare anche la compatibilità strutturale metrica, al fine di introdurre nel procedimento di identificazione un'ulteriore valenza.

Sottolineiamo che quando ci si trovi a dover confrontare immagini di bassa qualità dell'evento criminoso con quelle di discreta qualità provenienti da immagini di foto-segnalamento, è utile nella valutazione di similitudine rendere omogenei dal punto di vista visivo i documenti video-fotografici, in modo che non vi sia grossa disparità e vengano catturati i particolari in eguale modo.

Il processo di identificazione si articola nei seguenti passi:

- Verifica della compatibilità dei connotati rilevabili nell'indagato e nel reo, con riferimento alle possibili prospettive (frontale e di profilo)
- La coincidenza di un certo numero di connotati di base su entrambi i soggetti in esame getta le basi per la formulazione del grado di identificazione.

In Fig.8 un esempio di definizione dei connotati presenti in un soggetto

Può capitare però che non sia sempre facile rilevare la compatibilità o la diversificazione dei connotati, specialmente nella visione

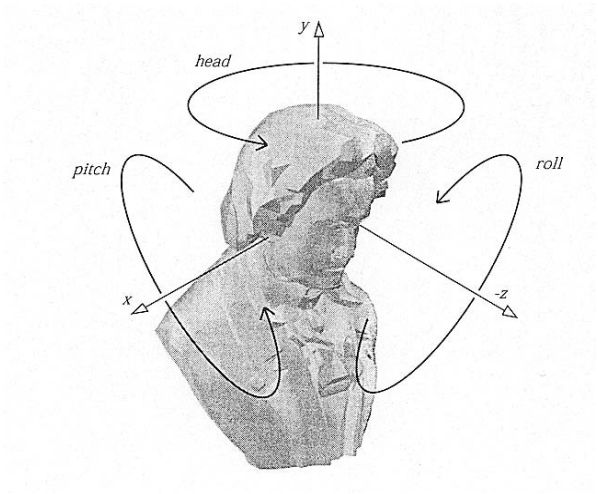

Fig.11 – Angoli di rotazione di Eulero

frontale, e formulare una identificazione. Gli autori hanno sperimentato le loro metodologie anche su gemelli monozigoti straordinariamente simili. InFig.9 si riporta un caso molto interessante; è evidente come l'apprezzamento dei connotati nella visione frontale non permette un'identificazione certa.

Poiché le informazioni morfologiche ricavabili dalla visione frontale non permettono una discriminazione, si può procedere all'analisi dei connotati del profilo. La Fig.10 evidenzia però come i due gemelli abbiano i connotati di base (del profilo destro) fortemente coincidenti e sia ardua la loro identificazione.

Ne segue che anche la valutazione dei connotati del profilo può condurre a una non identificazione. Vedremo nel seguito che in realtà l'analisi puntuale di un particolare connotato dei gemelli possiede un forte potere di discriminazione e permette di distinguerli.

3.3. **Misurazione degli indici antropometrici, triangolazione, mappe facciali.**

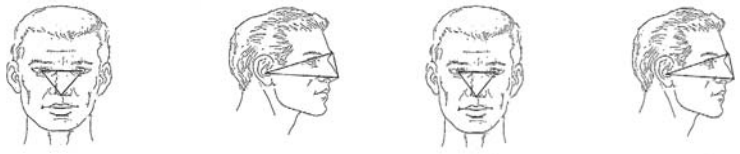

Fig.12 – Esempi di triangolazione

Occorre osservare come la valutazione degli aspetti morfologici e le misurazioni di strutture anatomiche richieda che le posture assunte dai soggetti a confronto siano tali da generare sul piano bidimensionale di acquisizione fotografica, immagini dei segmenti anatomici con aspetti e forme confrontabili. Ciò richiede generalmente che le immagini del soggetto di confronto siano acquisite ponendolo spazialmente in una postura che ricalchi il più possibile quella rilevabile nel soggetto in indagine. Le immagini di lavoro sono la rappresentazione sul piano di acquisizione della proiezione prospettica degli individui posti nello spazio 3D; l'immagine che si ricava dipende dalla postura del soggetto rispetto a un sistema di riferimento locale a lui solidale che assumiamo destrogiro Fig.11.

Rispetto a tali assi possiamo definire l'orientamento del capo mediante angoli di rotazione, detti angoli di Eulero.

Come esempi di misurazione, si possono considerare gli indici antropometrici, che sono svincolati dalle trasformazioni di scalamento e sono abbastanza robusti rispetto alla presenza di contenute differenze di orientamento, corrispondenti a piccole variazioni degli angoli di Eulero. Un altro metodo molto utile ai fini della valutazione metrica è la triangolazione in cui si considerano punti di repere tali da permettere la costruzione di triangoli. Sui triangoli si può calcolare il fattore di forma definito come

$$FF = 4\pi A / p2$$

dove p e A sono rispettivamente perimetro e area del triangolo. Tale fattore costituisce una grandezza adimensionale invariante per le trasformazioni fondamentali di rotazione sul piano, traslazione e scalamento, che permette quindi di caratterizzare i triangoli

Fig.13 – Esempio di mappa facciale corrispondente a un individuo

stessi e di conseguenza le fattezze ad essi associate. Vengono così descritti metricamente aspetti strutturali del volto (Fig.12).

In alternativa agli indici antropometrici e alla triangolazione si può costruire la mappa facciale che si ottiene come descritto nel seguito.

Un volto è costituito da regioni che rappresentano i singoli connotati; nella visione frontale questi sono costituiti per esempio dai connotati locali quali la fronte, il trichion, le arcate sopraccigliari, la bocca, il dorso nasale, il mento, nonché quello globale della forma del volto. Nella visione laterale ben si presta il profilo definito dall'evoluzione fronte, naso, bocca, mento e la forma-posizione dell'orecchio.

Si può quindi pensare di procedere alla loro segmentazione mediante tecniche di evidenziazione dei contorni basati sull'applicazione di operatori del gradiente e del laplaciano, cui segue un eventuale utilizzo di operatori di regolarizzazione atti a rendere il più possibile sottili e meno frastagliate le linee di contorno [3]. L'applicazione dei filtri di estrazione dei contorni sopra accennati dà luogo a una sorta di "gabbia strutturale" che costituisce l'"impronta facciale"; questa si presenta come un'immagine binarizzata. La mappa facciale rappresenta una struttura metrica che congloba indici antropometrici e triangolazioni in quanto collega punti di repere conservando i rapporti fra le loro misure. Dal punto di vista

Fig.14 – Esempio di sovrapposizione di gabbia strutturale con un individuo

Fig.15 – Esempio di non compatibilità metrica

pratico, viene solitamente estratta l'impronta facciale dell'indagato in quanto le immagini a disposizione sono generalmente di qualità tale da permettere l'elaborazione automatica e di conseguenza la costruzione di un'impronta facciale con buona definizione. L'impronta facciale dell'indagato viene successivamente sovrapposta all'immagine del soggetto in analisi, al fine di verificare la sovrapponibilità delle linee di definizione dei segmenti anatomici estratti con i connotati del soggetto. Nel caso in cui si verifichi una forte

Fig.16 – Compatibilità metrica tra gemelli

aderenza, allora si è di fronte a un dato metrico che integra le valutazioni fisionomiche e può quindi raffinare la formulazione di un giudizio di compatibilità fra i due soggetti.

Fig.17 – Esempio di robustezza dell'impronta facciale

La metodologia di estrazione dell'impronta facciale da noi usata si basa sui seguenti passi [12,13]:

1. **acquisizione numerica delle immagini**: i frame estratti dalle cassette di videosorveglianza e le fotografie dell'indagato vengono convertiti in forma numerica, provvedendo se necessario al loro miglioramento e/o ripristino di qualità.

2. **estrazione dell'impronta facciale**: l'immagine numerica del volto dell'indagato (una fotografia che rispecchi la postura assunta dal reo in un fotogramma di videosorveglianza) viene sottoposta a procedimento automatico di estrazione dei contorni che evidenzia le strutture caratteristiche del volto (Fig.13).

3. **sovrapposizione delle immagini e analisi**: si verifica la presenza, oppure non, della sovrapponibilità fra l'immagine di confronto del rapinatore e quella della mappa facciale dell'indagato; come già detto, il procedimento può richiedere l'applicazione di trasformazioni di scalamento omogeneo e/o di roto-traslazione sul piano Tali trasformazioni permettono "l'aggiustamento fine" della gabbia strutturale di contenimento con i corrispondenti punti di repere del reo, al fine di analizzare in quale misura questi si adattino all'impronta facciale dell'indagato. La valutazione della sovrapponibilità ottenuta permette di esprimere il grado di compatibilità metrica fra i soggetti rappresentati nelle immagini.

Nell'esempio riportato in Fig.14 la sovrapposizione è perfetta in quanto si tratta dello stesso individuo; nella realtà corrisponde al

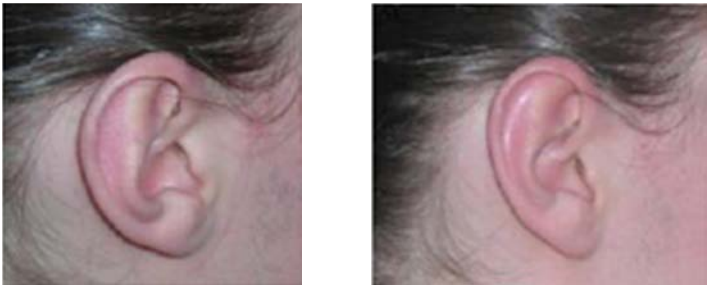

Fig.18 – Diversa morfologia dell'orecchio destro dei due gemelli

Fig.19 – Orecchio destro dei gemelli ripreso in diverse posture

Occorre però osservare che due gemelli potrebbero avere impronte facciali (frontali e/o di profilo) molto simili, per cui non è detto che l'impronta facciale sia in questo caso discriminante. La Fig.16 riporta il caso della sovrapposizione dell'impronta di un gemello e la sovrapposizione con l'altro che come è evidente presenta una forte coincidenza.

Fig.20 – Variazione tra orecchio destro e sinistro nei due gemelli

In questi casi è necessario utilizzare metodologie che analizzino in forma dettagliata la presenza di eventuali connotati salienti e di contrassegni., o altre tecniche antropometriche.

Sulla robustezza dell'impronta facciale a fronte di leggere difformità nella postura ci si può riferire a quanto illustrato in Fig.17. Si può osservare come la rotazione attorno all'asse y mantenga fondamentalmente inalterato il profilo e influisca solo sulla posizione dell'orecchio.

Si leggano le immagini di Fig.17 nel seguente modo: sinistra-alto: soggetto in postura di netto profilo destro; sinistra-mezzo: mappa facciale; sinistra basso: sovrapposizione del soggetto di cui a sinistra alto, con mappa facciale, per cui si ha perfetta aderenza; destra-alto: il soggetto ha subito una rotazione oraria attorno all'asse y di una decina di gradi; destra-medio: impronta del soggetto sinistra-alto; destra-basso: sovrapposizione del soggetto destra-alto con mappa facciale sinistra-medio in cui si nota come vi sia sostanziale aderenza del profilo del volto, mentre sia leggermente disallineato l'orecchio. Da tale analisi segue che il confronto del profilo è significativo anche quando i soggetti differiscano leggermente nella postura.

3.4. L'orecchio come connotato discriminatore

Fra le tecniche di riconoscimento in alternativa alle impronte digitali è in fase di studio con grande interesse quella che analizza morfo-metricamente l'orecchio.

Gli studi di maggior rilievo condotti sull'orecchio, datati 1989, sono di Alfred Iannarelli, capo della polizia di un campus universitario in Hayward [14]. Iannarelli analizzò nell'arco di alcuni anni oltre 10.000 morfometrie di orecchi e constatò come non ce ne fossero due identiche. L'orecchio infatti dopo il quarto mese di vita assume una morfologia che rimane praticamente immutata nel tempo e non varia con l'espressione facciale. Una leggera variazione della lunghezza del lobo può avvenire per effetto della forza di gravità (si trascurano agenti esterni come orecchini) ma si tratta comunque di variazioni di contenute dimensioni che rimangono tali

fino a età avanzata. Nei primi otto anni di vita e dopo i 70 anni la variazione in lunghezza assume valori più elevati rispetto agli altri periodi della vita. È facile notare come l'orecchio presenti maggior difficoltà descrittiva rispetto al volto. Vi sono infatti numerosi aggettivi che sono usati per descrivere le caratteristiche salienti di un volto e poche per l'orecchio. Come abitudine consolidata infatti, si pone maggior attenzione agli aspetti fisionomici del volto di una persona, per poi riconoscerli, mentre si prestano ben poche attenzioni all'orecchio.

Tenendo in considerazione che le fotografie segnaletiche ritraggono i soggetti in esame nella visione frontale e di profilo destro, l'orecchio destro è generalmente quello di riferimento. Un esempio di utilizzo dell'orecchio per la discriminazione tra soggetti [15] è riportato in Fig.18, che si riferisce agli orecchi destri (ottenuti da immagini di netto profilo) dei due gemelli per i quali è stata sopra mostrata la compatibilità fisionomica e metrica. Appare evidente come la morfologia dei due orecchi sia diversa e come pertanto possa costituire un elemento fisionomico saliente che permette una distinzione tra i due soggetti.

Occorre osservare che la valutazione dell'aspetto morfologico dell'orecchio è soggetto a variazioni di illuminazione e di postura. La Fig.19 evidenzia il diverso apprezzamento della morfologia dell'orecchio dei due gemelli a fronte di variazioni di postura. Ne consegue che anche per l'orecchio occorre che le posture dei due soggetti siano il più possibile coincidenti.

Per quanto riguarda poi la variabilità intra-personale, generalmente la forma dell'orecchio destro è diversa da quello sinistro. La Fig.20 raffigura in alto l'orecchio destro e sinistro di un gemello, in basso quello del secondo.

L'orecchio può quindi costituire elemento fisionomico con forte potere di discriminazione.

3.5. **Criteri identificativi**

Non esiste una codifica internazionale standard per l'identificazione. La Polizia Scientifica italiana e i reparti operativi dei CC utilizzano una scala comparativa che recita quanto sotto riportato, in

cui le frasi in corsivo sono commenti degli autori:

- non compatibilità: nelle immagini ritraenti gli individui a confronto è presente almeno un particolare non posticcio e non modificabile nel tempo che permette di escludere che le due figure in analisi ritraggono lo stesso individuo. *Si tratta di parametri fisionomici con forte discriminazione, come per esempio evidenti deturpazioni, espressioni facciali inusuali, segmenti anatomici con strutture particolari, cicatrici, nei in precise locazioni. In questo caso l'indagine fisionomica può condurre a esclusione, nel caso di presenza in uno solo degli individui a confronto, e a identificazione certa, quando si rilevino su entrambi i soggetti.*
- compatibilità parziale: vista la scarsa definizione e/o visibilità di almeno una delle immagini a confronto, non è possibile rilevare particolari anatomici facciali che permettano di giungere ad un giudizio positivo di comparazione, vi si riscontrano comunque alcuni particolari simili tra gli individui a confronto. *Generalmente le immagini a scarsa definizione sono quelle di videosorveglianza o di indagine ambientale, mentre le foto segnaletiche o acquisite sull'individuo sono di buona qualità. Le immagini a scarsa definizione, pur sottoposte a miglioramento di qualità non sempre permettono di cogliere in modo dettagliato aspetti fisionomici. Ne segue che a fronte di similitudine di aspetti fisionomici può essere opportuno procedere a valutazioni metriche (impronte facciali o altre misure metriche); ciò significa che un'eventuale compatibilità parzia-*

Fig.21 – posizionamento dei punti di repere sulle immagini

le basata su dati descrittivi (gli aspetti fisionomici) potrebbe evolvere, sulla base dei dati metrici, verso una compatibilità.

- compatibilità: gli elementi presenti nei due individui a confronto permettono di rilevare numerosi particolari fisionomici facciali simili in entrambi; non è possibile comunque, vista la definizione di almeno una delle immagini a confronto, evidenziare contrassegni (nei, cicatrici, rughe caratteristiche etc.) nei due individui messi a confronto, che porterebbero a un giudizio di compatibilità totale. *Occorre osservare che gli aspetti accennati costituiscono solo un parte dell'anatomia fine del volto, come per esempio la linea fronte-naso, la piramide nasale, la bocca, il mento, il prognatismo, la struttura dell'orecchio, accompagnate*

Fig.22 – Confronto fra ricostruzione e immagine originale

Fig.23 – Confronto fra l'orecchio e la sua ricostruzione

eventualmente da misure metriche. Ne segue che anche in questo caso il giudizio potrebbe ricadere in quello più forte di compatibilità totale. Si noti poi che non venga definita numericamente la quantità di elementi simili, per cui il consulente/perito deve valutare il peso associato ai parametri e agire in base all'esperienza acquisita nel tempo.

- compatibilità totale: i due individui ritratti nelle immagini a confronto, hanno tutti i particolari facciali visibili simili, comprese le relative proporzioni generali. Sono inoltre presenti particolarità anatomiche singolari, contrassegni, riscontrabili in entrambe le immagini degli individui a confronto. *Le proporzioni di cui si fa cenno, sono le misure metriche che aggiungono valenza ai rilievi dei parametri fisionomici. Anche in questo caso risulta difficile codificare quali particolarità anatomiche singolari o contrassegni assurgano ad ago della bilancia per asserire la compatibilità totale. Si ritiene che a fronte della presenza di connotati coincidenti e di misure confrontabili si possa parlare di compatibilità totale. Occorre comunque sottolineare che le indagini sono svolte su documenti fotografici e quindi manca il rapporto diretto con uno dei due individui; ciò può introdurre pertanto un minimo di aleatorietà.*

4. Ricostruzione tridimensionale di soggetti, ambienti, scene statiche

4.1. Ricostruzione 3D del volto

Come sottolineato a proposito del confronto fra immagine rilevata dalla videosorveglianza e immagine dell'indagato, può capitare che le posture dei due soggetti non siano confrontabili o comunque tali da generare difficoltà nella comparazione. Occorre allora procedere mediante l'acquisizione mirata di immagini fotografiche scattate in modo da simulare la videoripresa, oppure provvedere alla ricostruzione 3D del soggetto e poi ruotare nello spazio la ricostruzione; ciò al fine di ottenere una rappresentazione bidimensionale che sia il più possibile aderente a quella della videosorveglianza.

Esistono in commercio software per le ricostruzione tridimensionale di un volto a partire dalla definizione di un insieme di FDP (Facial Definition Point); dato un modello tridimensionale di partenza, si posizionano un certo numero di punti di interesse e il sistema sulla base delle informazioni fornite dalle fotografie 2D frontali e laterali, adatta sia la metrica del volto sia le caratteristiche fisionomiche mediante tecniche di mesh morphing.

Gli autori hanno sperimentato il pacchetto Facegen [W7] che fornisce un'interfaccia utente tale da rendere il software molto semplice da usare. Lo strumento per l'adattamento di tre foto, una frontale e due laterali è indicato come Photofit. Il processo che sta

Fig.24 – Esempi di ricostruzione di scene 3D

Fig.25 – Fotogrammi estratti dall'animazione di un'esplosione

alla base del PhotoFit si compone di diverse fasi. Viene richiesto all'utente di caricare immagini bidimensionali nitide e senza occlusioni di vario genere. In particolare è obbligatoria la vista frontale, mentre le laterali sono facoltative ma naturalmente migliorano notevolmente il processo di ricostruzione del volto tridimensionale. Sulle immagini si posizionano i punti di repere, secondo le indicazioni fornite. LaFig.21rappresenta un esempio di posizionamento dei punti su uno dei gemelli nella visione frontale, di profilo sinistro e di profilo destro.

L'elaborazione prodotta dal software, comparata con le immagini effettive del soggetto è riportata in Fig.22.

È da notare che il software Facegen non si occupa della ricostruzione dell'orecchio che, come sopra evidenziato, costituisce invece un parametro tale da assurgere a notevole discriminatore.

4.2. Ricostruzione 3D dell'orecchio

Per tenere conto di quanto sopra detto, abbiamo sviluppato un sistema che sulla base di due fotografie (una frontale e una laterale) dell'orecchio lo ricostruisce utilizzando particolari funzioni di interpolazione dette Radial Basic Function (RBF) [16]. Il procedimento è simile a quello di Facegen e si basa sui seguenti passi:

- Allineamento delle immagini per la vista frontale e laterale: questa fase prevede l'inserimento e l'allineamento di 2 diverse fotografie all'interno di un software di modellazione. In questo contesto si è pensato di adottare l'ambiente 3D Studio MAX per importare le immagini e visualizzarle;
- Inserimento dei punti di repere sulle viste: individuazione di

alcuni marker caratteristici sulle diverse parti anatomiche dell'orecchio;

- scelta della RBF per l'algoritmo di fitting.

La Fig.23 rappresenta i risultati ottenuti e mostra l'inserimento dell'orecchio nella ricostruzione tridimensionale del capo ottenuta con Facegen. Si osservi come vi sia una notevole coincidenza fra la rappresentazione reale e quella ricostruita.

La ricostruzione dell'orecchio e il suo eventuale inserimento nel modello 3D del capo permette di effettuare confronti fisionomici più accurati ed eventualmente di procedere a valutazioni metriche con indici e/o mappe dell'orecchio.

4.3. Ricostruzione di ambienti e scene statiche

In ambito forense è sovente richiesta la ricostruzione tridimensionale di ambienti e scene dove si sia consumato un evento delittuoso. Le metodologie utili allo scopo si basano generalmente sulla fotogrammetria e sulla modellazione che, supponendo inizialmente non vi sia alcuna evoluzione delle strutture fisse dell'ambiente, degli arredi e dei soggetti presenti nella scena, ne permettono la ricostruzione 3D; questa può essere così osservata da diversi punti di vista permettendone un'esplorazione più raffinata.

La fotogrammetria viene solitamente impiegata nel caso in cui non sia possibile ottenere informazioni metriche dettagliate sull'ambiente considerato, ma si posseggano immagini riprese da differenti posizioni che ritraggano soggetti fermi in un ambiente noto; è così possibile ricavare per esempio la distanza reciproca tra soggetti, oggetti e dimensione degli stessi. A titolo esemplifi-

Fig.26 – navigazione virtuale di un ambiente, diversi punti di vista della scena

cativo, la fotogrammetria può essere impiegata per la valutazione dell'altezza di soggetti all'interno di un ambiente (per esempio in una banca di cui si possegga un frame della videosorveglianza), oppure della distanza fra altri soggetti e/o arredi presenti nell'ambiente stesso (si pensi a immagini diverse di reportage in una manifestazione di piazza). La modellazione invece permette una ricostruzione tridimensionale più dettagliata di un ambiente di cui siano note le necessarie misure metriche (rilievi).

Per la ricostruzione di ambienti e scene gli autori utilizzano abitualmente 3D Studio MAX; la scelta è motivata dal fatto che tale strumento è molto potente e versatile. La Fig.24 riporta due esempi di ricostruzioni dettagliate di ambienti realizzate dagli autori.

4.4. Animazione di eventi

La possibilità offerta dai software di modellazione grafica e animazione, con diverso grado di sofisticazione, ha creato una nuova metodologia di presentazione nelle aule giudiziarie delle ipotesi formulate da parte del consulente/tecnico sull'accadimento di fatti ed eventi. Alcuni recenti processi hanno utilizzato in aula giudiziaria di animazioni con lo scopo di presentare in modo più evidente quale possa essere stata l'evoluzione dei fatti; ciò sulla base della ricostruzione ottenuta dai dati raccolti dagli inquirenti e dalle dichiarazioni dei testimoni. Le tecniche di animazione forense, rispetto al sistema verbale e scritto sono sicuramente strumenti rappresentativi che evidenziano con immediatezza, grafica e suono quanto si pensa possa essere successo nella dinamica dei fatti.

Alcuni frame dell'esempio di animazione, da noi realizzato con 3D studio MAX, per rappresentare un'esplosione al fine di capire la dimensione del fenomeno e per esempio l'accessibilità alle uscite di sicurezza, sono riportati nella Fig.25 (inizio esplosione, esplosione al suo massimo, fumi residui).

4.5. Simulazione di eventi e sistemi di realtà virtuale

La simulazione di eventi è un'area delle applicazioni dell'informatica forense che non ha ancora raggiunto livelli sofisticati in quanto

non è semplice la sua realizzazione in termini sia di ricostruzione in tempo reale dell'ambiente, sia delle leggi fisiche che regolano l'evoluzione della scena, nonché nelle azioni intraprese da personaggi e delle interazioni con gli oggetti presenti nella scena stessa.

Se poi ci si riferisce alla realtà virtuale le cose si complicano maggiormente. Occorre infatti risolvere problemi di interazione in cui l'utente non è un semplice spettatore passivo, bensì un attore; vengono infatti superate le barriere delle interfacce convenzionali legando movimento e interazione, per analogia, all'azione fisica effettiva. Potenzialmente l'utente si muove senza alcun tipo di limitazione prestabilita. Il senso di presenza fisica nel mondo simulato, cioè l'immersione, è poi condizione indispensabile per poter parlare di realtà virtuale. Il coinvolgimento dell'utente sarà alto quando verrà completamente isolato dall'ambiente reale circostante e gli sarà sostituito ogni stimolo sensoriale naturale con quelli indotti.

Attraverso un sistema grafico computerizzato, gli verranno forniti segnali di input per rappresentare il nuovo ambiente sintetico. La tecnologia ha ovviamente un ruolo primario nella determinazione del senso di immersione, ma deve essere chiaro che sono i contenuti degli ambienti di sintesi e la qualità e la ricchezza dell'interazione a determinare il coinvolgimento degli esploratori. Una nota negativa che suona quasi paradossale è che per l'immersione in un mondo virtuale senza limiti e barriere si è costretti ad indossare ingombranti protesi (occhiali, auricolari, data-glove, tute) per poter godere della completa libertà di movimento e di espressione nello spazio simulato.

È importante sottolineare come le applicazioni di realtà virtuale permettano di verificare ipotesi alternative nell'evoluzione della scena (soggetti e oggetti possono trovare diverse collocazioni e interagire fra loro). Si possono utilizzare modelli di illuminazione diversi per verificare la visibilità di componenti della scena stessa. La significatività dell'applicazione di realtà virtuale dipenderà dal grado di accuratezza con il quale si simulino le condizioni iniziali, l'evoluzione dell'ambiente nel rispetto delle leggi fisiche e delle possibili interazioni. Come per l'animazione anche in questo caso la realtà virtuale rimane uno strumento per spiegare meglio l'evolu-

zione spazio-temporale di un evento e osservare se possa fornire plausibili spiegazioni con quanto osservato nei sopralluoghi.

Un semplice esempio di simulazione da noi realizzato riguarda la visita interattiva, e con buon livello di immersione, di un ambiente ipotetico in cui sia avvenuto un fatto di tipo delittuoso. La Fig.26 riporta alcuni frame in cui si evidenzia come possa essere cambiato il punto di vista e il contenuto della scena, a seconda di come l'utente rivolge lo sguardo e interagisce con essa.

5. **Conclusioni**

Da questa breve carrellata sulle metodologie informatiche che si possono impiegare in ambito forense e da risultati ottenuti dalla nostra esperienza sul campo, appare evidente come queste siano molto variegate e non esista un'unica via, per cui la sua scelta è fortemente vincolata dal contesto in cui si opera. In particolare la videosorveglianza e sue derivazioni coinvolgono problemi legati al riconoscimento automatico o semiautomatico dei volti che non sono ancora approdati a risultati definitivi.

Restano così aperti problemi di miglioramento delle analisi sulle quali si indaga da anni e occorre sviluppare e approfondire le metodologie atte a risolvere problemi più ambiziosi legati alla computer vision, quali ad esempio la motion-capture, applicata per la ricostruzione dell'evoluzione temporale della postura di una persona, al fine di definirne il tipo di deambulazione, oppure la valutazione dell'altezza di un individuo con piccoli margini di errore.

Il cammino è ancora lungo e ogni piccolo passo richiede notevole impegno.

6. Ringraziamenti

Lo studio svolto dagli autori è stato reso possibile anche dai finanziamenti MURST e alla disponibilità dei gemelli, studenti del Corso di Studi di Informatica dell'Università degli Studi di Torino.

7. Riferimenti bibliografici e sitografici

[1] Bramble S., Compton D. Klaéen L., Forensic image analysis, 13th INTERPOL Forensic Science Symposium, Lyon, France, October 16-19 2001

[2] Graziano E., Problematiche della videosorveglianza in rapporto all'attività delle Forze di Polizia, VISIT 2008, Facoltà di Ingegneria, Modena, 22 maggio 2008.

[3] Gonzales R., Wood R., Digital Image Processing, 3rd ed., Prentice Hall, 2008.

[4] Reis G., Analisi forense con Photoshop, Apogeo, 2008

[5] Bertillon A., Identification anthropometrique: instruction signaletiques, Melun, Imprimerie Administrative, 1893.

[6] Falco G., Identità: metodo scientifico di segnalamento e identificazione, II Edizione, Roma, 1923.

[7] Martin R., Saller K., Lehrbuch der Anthropologie in systematicher Darstellung, Dd. I-II. Fischer, Stuttgard, 1956-59.

[8] Iscan M.Y., Loth S.R., Photo image identification, in Siegel J.A., Soukko J.P., Knupfer G.C., (Eds), Encyclopedia of Forensic Sciences, Academic Press, pagg 795-805, New York, 2000.

[9] Olivieri L., Antropologia e Antropometria, C.E.V. Idelson, Napoli, 1963.

[10] Bairati A., Trattato di Anatomia Umana, Volume IV, Minerva Medica, 1971.

[11] Farkas L. G., Anthropometry of the head and face, Second Edition, Raven Press, 2000.

[12] Balossino N., Siracusa S., Parametri discriminatori nel riconoscimento di volti, Polizia Moderna. N. 1, 1998.

[13] Balossino N., Siracusa S., L'identificazione basata sul volto: metodi fisionomici e metrici, Security Forum 2004, Edizioni ItasForum, Bergamo, 2004.

[14] Iannarelli A., Ear identification , Forensic identification series, Paramont Publishing Company, Fremont, California, 1989.

[15] Balossino N., Lucenteforte M., Siracusa S., Analisi biometria dell'orecchio in ambito forense, Nuove Tecnologie in Medicina, Anno 6, N.1-2, Sirse s.r.l. Editore, 2006.

[16] Furneri F., Sviluppo di metodologie per la ricostruzione 3D del padiglione auricolare mediante funzioni radiali, Tesi di Laurea, Corsi di Studi in Informatica, Università di Torino, AA 2007/2008.

[W1] http://www.mathworks.com

[W2] http://www.vips.ecs.soton.ac.uk/index.php?title=VIPS

[W3] http://eidos.di.unito.it/eidoslab.php

[W4] http://opencvlibrary.sourceforge.net/

[W5] http://www.facegen.com

Tutela della privacy e sicurezza urbana. Le "regole" della videosorveglianza e l'uso processuale dei dati acquisiti.

Dr. Marco Dall'Olio
Giudice del Tribunale di Pescara

Sempre maggiore diffusione ha avuto negli ultimi anni - in particolar modo dopo l'abbattimento delle torri gemelle in data 11 settembre 2001 - lo strumento della videosorveglianza, ovvero l'installazione di sistemi che consentano di visualizzare immagini *live* o registrate al fine di monitorare ambienti e aree per poter individuare situazioni di pericolo.

Già agli inizi degli anni '90 però la Gran Bretagna si era distinta quale paese all'avanguardia nella messa a punto di tecnologie di sorveglianza basate sulla ricognizione visuale. A Glasgow il *City Watch*, complesso sistema di telesorveglianza urbana, veniva installato nel lontano 1994. E da anni a Manchester è attivo il *Football Intelligent System* che raccoglie in un *database* le immagini degli *hooligans* sospetti. Anche in tale paese era stato un evento traumatico a favorire lo sviluppo delle nuove metodologie di telesorveglianza: il 16 febbraio 1993 il piccolo James Bulger, di anni due, era stato rapito e brutalmente assassinato da due bambini di dieci anni che si erano con lui allontanati da un supermercato, videoripresi dall'occhio elettronico del centro commerciale, ciò che ne aveva consentito la successiva identificazione.

Analoghi sviluppi si erano avuti in Italia, antesignano proprio il Comune di Modena che già nel 1995 aveva attivato uno dei primi sistemi di sorveglianza *distribuita*.

L'obiettivo dichiarato di tutti questi sistemi - installati da soggetti

pubblici o privati - è quello di contenere i fenomeni criminali, sia mediante repressione (aumentando cioè le probabilità di punizione degli autori dei reati commessi) sia mediante prevenzione *situazionale* (sotto forma di deterrenza).

Quanto a quest'ultima finalità l'antecedente scientifico è costituito dalla teoria sociologica c.d delle *opportunità criminali*, secondo cui il crimine può essere prevenuto riducendo le opportunità di delinquere, senza che ciò determini necessariamente *displacement* (ovvero spostamento dell'attività criminale verso una diversa zona – territoriale o non – sulla quale non si sia ancora intervenuti). L'approccio della *Situational Crime Prevention* propone pertanto la modifica degli *elementi situazionali,* quali la disponibilità degli obiettivi o il livello di sorveglianza, per ottenere un impatto significativo sulla riduzione delle opportunità criminali.

Studi recenti evidenziano però - nel medio lungo periodo - riduzioni non significative nel livello di criminalità violenta della zona interessata, con l'eccezione dei reati contro gli autoveicoli per i quali la contrazione risulta evidente nelle zone videosorvegliate.

Accanto ad un interesse di carattere generale che potremmo definire di *pubblica sicurezza*, ne sussiste però uno diverso e contrapposto, costituito dalla riservatezza delle persone, che si declina, come vedremo, in diverse forme (dal diritto alla privacy del cittadino, al diritto del lavoratore a non subire discriminazioni, al diritto del malato alla propria dignità personale). E ciò in quanto la videosorveglianza è per il cittadino un vincolo, una limitazione ed un condizionamento, essa contenendo una molteplicità di dati potenzialmente sensibili, ovvero di elementi idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose e filosofiche, le opinioni politiche e l'adesione ai partiti, i dati concernenti lo stato di salute, la vita e l'orientamento sessuale, le inclinazioni e le abitudini delle persone.

In Italia il bilanciamento di questi contrapposti interessi (in adesio-

ne alla Convenzione n. 108 del 1981 del Consiglio d'Europa sulla protezione delle persone per quanto attiene il trattamento automatizzato dei dati personali – e in adesione alla Direttiva Comunitaria n. 46 del 1995 sul trattamento dei dati personali e sulla loro libera circolazione), è stato raggiunto prima con la legge n. 675 del 31 dicembre 1996 sulla tutela della persone e di altri soggetti rispetto al trattamento dei dati personali, quindi con il D.Lvo n. 196 del 30 giugno 2003, detto "Codice in materia di protezione dei dati personali", che non molto ha innovato rispetto alla disciplina precedente.

La cornice normativa prevista dal Codice del 2003 è costituita da rimedi amministrativi, civili ed anche penali, oltre che dalla previsione dell'organismo denominato "Garante della Privacy", autorità operativa sin dal 1997 con i seguenti compiti:

1. redazioni di pareri – ovvero controllo della conformità dei trattamenti di dati personali a leggi e regolamenti e segnalazione ai titolari o ai responsabili dei trattamenti delle modifiche da adottare per conseguire tale conformità;
2. decisioni sui ricorsi – ovvero esame delle segnalazioni e dei reclami degli interessati, nonché dei ricorsi presentati ai sensi dell'art. 29 della legge;
3. emanazioni di autorizzazioni e di provvedimenti a carattere generale – ovvero adozione dei provvedimenti previsti dalla normativa in materia tra cui, in particolare, le autorizzazioni generali per il trattamento dei dati sensibili;
4. contestazione delle violazioni – ovvero emissione di divieti, in tutto od in parte, o di blocco del trattamento di dati personali quando per la loro natura, oppure per le modalità o gli effetti di tale trattamento, vi sia il rischio concreto di un rilevante pregiudizio per l'interessato.

Il Garante per la protezione dei dati personali è autorità indipendente, organo collegiale composto da un Presidente (allo stato Francesco Pizzetti, ordinario di diritto costituzionale all'Università di Torino), da un Vice Presidente (ora Francesco Chiaravallotti, già

procuratore generale presso la Corte di Appello di Reggio Calabria) e da due componenti, Mauro Paissan, già giornalista e deputato, e Giuseppe Fortunato, già Presidente della Associazione nazionale dei difensori civici italiani), tutti membri eletti dal Parlamento, in carica per sette anni non rinnovabili.

Nell'ambito della vasta produzione dell'Autorità Garante della Privacy, e per quanto attiene nello specifico i sistemi di videosorveglianza, assumono particolare rilevanza i due provvedimenti generali – cogenti per tutti gli interessati - emanati rispettivamente il 29 novembre 2000 (c.d. "decalogo per il trattamento dei dati personali"), ed il 29 aprile 2004. A ciò si aggiungono le relazioni annuali del Garante, ultima delle quali quella del 16 luglio 2008, laddove vengono raccolti i provvedimenti specifici presi nel corso dell'anno ed indicati gli elementi di criticità del sistema.

Secondo il Codice del 2003, così come prima secondo la legge n. 675/1996, costituisce dato personale qualsiasi informazione che consenta l'identificazione - anche in via indiretta - dei soggetti interessati, e ciò sebbene l'informazione derivi da suoni o da immagini anziché da dati alfanumerici. E' dato personale pertanto il suono o l'immagine proveniente da un sistema di videosorveglianza, anche se tali informazioni non vengano immagazzinate in un archivio elettronico e comunicate a terzi, ed anche ove le persone non possano essere identificate in maniera diretta ma possano esserlo solo attraverso il collegamento con altre fonti conoscitive quali foto segnaletiche, identikit, archivi di polizia contenenti immagini.

Il Provvedimento generale del 2004 individua in primo luogo i principi applicabili a tutti i sistemi di videosorveglianza, quindi evidenzia prescrizioni specifiche concernenti particolari tipi di trattamenti di dati (ad es. quelli effettuati da soggetti pubblici).

I quattro principi generali cui tutti devono attenersi per l'installa-

zione di sistemi di videosorveglianza sono i seguenti:

1. **il principio di liceità** – che prevede che il trattamento dei dati vada effettuato nel rispetto di tutte le prescrizioni normative, primarie o secondarie in materia.
2. **il principio di necessità** – secondo cui il trattamento del dato non deve superare il limite strettamente necessario per raggiungere lo scopo della videosorveglianza (ad es. un sistema per il solo monitoraggio del traffico non deve consentire zoomate per il riconoscimento delle targhe o peggio per l'osservazione di ciò che accade all'interno delle autovetture) e le immagini devono essere cancellate periodicamente ed automaticamente, il più rapidamente possibile (di solito entro le 24 ore, fatte salve le festività; in alcuni casi entro una settimana, come ad esempio per gli istituti di credito od i mezzi di trasporto a rischio; eccezionalmente per un periodo maggiore, secondo specifiche esigenze del caso od allorquando vi sia richiesta dell'autorità di polizia o dell'autorità giudiziaria).
3. **il principio di proporzionalità** – che prevede che la videosorveglianza debba costituire l'extrema ratio, utilizzabile laddove altri sistemi (quale ad esempio l'utilizzo di personale dipendente) risultino insufficienti o inattuabili.
4. **il principio finalistico** – secondo cui lo scopo del trattamento attuato deve essere determinato, esplicito e legittimo. Ciò che non avviene ad esempio allorquando un privato si proponga finalità di sicurezza pubblica, di prevenzione e di accertamento dei reati che invece competono solo ad organi di Polizia. Per tale ragione tutti i soggetti interessati devono essere informati - mediante apposizione di cartelli e di informative scritte - che stanno per accedere ad un'area videosorvegliata, con eventuale registrazione. E lo scopo del trattamento va adeguatamente documentato in un atto che deve essere conservato presso il responsabile del trattamento stesso al fine di verificarne la corrispondenza al reale.

- Laddove i dati vengano conservati (come detto per il minor

tempo possibile), occorrono diversi livelli di accesso al sistema, ad esempio mediante *creazione di una doppia chiave* che consenta la visione integrale delle immagini solo congiuntamente alle forze di polizia.

- Vanno poi specificamente designati i *responsabili del trattamento*, addetti all'utilizzo degli impianti per la eventuale visione delle immagini conservate.
- Devono inoltre essere adottate *misure di sicurezza* per il trattamento e la conservazione dei dati.
- L'interessato ha sempre *diritto di accesso* per il controllo e per la modifica delle modalità e delle finalità del trattamento in caso di violazione dei principi suddetti.

Le eventuali conseguenze in caso di violazione espongono alla inutilizzabilità del dato (per la finalità per cui è stato disposto), alla adozione di provvedimenti di blocco, alla comminazione di sanzioni amministrative od al limite anche penali.

Nella generalità dei casi il rispetto dei limiti connessi a detti principi consente di attivare un sistema di videosorveglianza senza autorizzazione preventiva, fatte salve le eventuali sanzioni di cui si dirà infra.

Necessita viceversa di verifica preliminare il sistema che:

1. preveda una raccolta delle immagini collegate e/o incrociate ad altri dati personali (ad es. biometrici) o con codici identificativi di carte elettroniche o con dispositivi collegati con la voce (allorquando ad esempio l'accesso in alcuni istituti di credito avvenga previo incrocio tra immagini ed impronte digitali).
2. preveda una digitalizzazione o indicizzazione delle immagini che consenta una ricerca automatizzata o nominativa.
3. consista in una videosorveglianza dinamico/preventiva, ovvero non riprenda staticamente un luogo ma rilevi percorsi o caratteristiche fisionomiche (ad es. riconoscimento facciale) o eventi

improvvisi e perciò portatori di allarme.

4. preveda la ripresa di persone malate o di detenuti (ad es. nel caso di videoriprese all'interno di un ospedale o di un istituto penitenziario).

In applicazione delle regole generali summenzionate l'Autorità Garante ha avuto modo di occuparsi di numerosi casi concreti.

Circa la videosorveglianza da parte di soggetti pubblici o a rilevanza pubblica -

- E' consentita solo ed esclusivamente per svolgere funzioni istituzionali che l'ente deve individuare ed esplicitare con esattezza. Il Garante ha qui riscontrato l'illiceità in alcuni casi, laddove enti locali hanno dichiarato di perseguire finalità di prevenzione ed accertamento dei reati che invece competono all'autorità giudiziaria ed alle forze di Polizia (viceversa i Comuni non hanno questo divieto in quanto soggetti preposti alla gestione della polizia locale).

- Vi deve essere una esigenza effettiva e proporzionata di prevenzione o repressione di pericoli concreti e specifici. Non è consentita perciò una videosorveglianza capillare di intere aree cittadine riprese integralmente e costantemente. E' inoltre privo di giustificazione l'uso di telecamere allo scopo esplicitato di controllare il rispetto del divieto di fumare, di calpestare aiuole, di affiggere o di fotografare.

- La videosorveglianza del traffico non può consentire ingrandimenti o zoom che non siano limitati all'accertamento del numero di targa del veicolo.

- Si possono installare telecamere per il controllo video su autobus e tram laddove vi sia la esplicitata necessità di prevenire atti di vandalismo e furti. In tal caso le riprese non potranno essere tanto particolareggiate da essere intrusive della riservatezza delle persone con acquisizione di particolari specifici (ad es. dati fisici, giornali letti, ecc.). Le telecamere non dovranno in alcun modo riprendere in modo stabile le postazioni di guida degli autisti, ciò che violerebbe l'art. 4 della legge 300/70 ovvero lo statuto dei la-

voratori.

- Per le stesse ragioni la videosorveglianza all'interno di un Comune non potrebbe consentire che si controllasse a distanza l'attività lavorativa né potrebbero essere installate videocamere nei bagni, negli spogliatoi, nelle docce, ecc.

- Negli ospedali e nei luoghi di cura occorre la stretta indispensabilità delle riprese ed occorre altresì che le stesse siano limitate a determinati locali e per fasce orarie. Occorre comunque che non siano ripresi malati se non in caso di assoluta necessità, in ossequio alla tutela non solo della riservatezza ma anche della loro dignità personale.

- Negli istituti scolastici è consentita la videosorveglianza nelle ore notturne ed in casi ristretti (ad es. atti vandalici ripetuti nel tempo). Mai si potrebbe perciò videoregistrare lo svolgimento delle lezioni in classe o l'ingresso e l'uscita degli studenti da scuola.

Circa la videosorveglianza da parte di soggetti privati

- Essa è ammissibile senza previa autorizzazione ma occorrerà che la dislocazione delle telecamere e l'inquadratura siano tali da limitare l'angolo visuale delle riprese alla registrazione delle sole immagini indispensabili.

- Una videocamera installata all'ingresso di una casa plurifamiliare non dovrà permettere di vedere chi entra dall'ingresso comune ed in quale alloggio si rechi.

- Se si riprende l'accesso ad un edificio dalla strada pubblica, la ripresa dovrà evitare il più possibile di inquadrare la zona prospiciente, in modo tale da non consentire ad esempio l'individuazione di coloro che transitino lungo la via.

I soggetti privati possono installare telecamere senza il consenso dei terzi interessati. Le riprese dovranno però essere limitate agli spazi interni od a quelli esterni immediatamente antistanti gli accessi. E le informazioni raccolte non dovranno essere comunicate o diffuse ad altri. Il vincolo di conservazione è però in questo caso meno stringente, ovvero può estendersi ad un periodo più ampio sempre che ciò si renda necessario (ad es. tutto il periodo delle

vacanze).

Quanto all'uso nel corso delle indagini ed in giudizio delle immagini raccolte può dirsi quanto segue:

- In primo luogo occorre distinguere tra attendibilità della prova, ammissibilità ed utilizzabilità della stessa.

Circa la prima questione basta dire che trattasi di problema tecnico e non giuridico, attenendo, ad esempio, alla esatta collocazione temporale dei dati, alla loro qualità e alla loro autenticità. Quanto alla ammissibilità ed utilizzabilità in giudizio essa è permessa ai sensi dell'art. 234 c.p.p. che consente di ricondurre la videoripresa in oggetto nella categoria della prova documentale. Ciò che occorre però è che le immagini siano effettuate in modo tale da non interferire con i luoghi di privata dimora altrui, posto che in tal caso si potrebbe ragionevolmente parlare non di prove atipiche (che sono consentite) bensì di prove illecite in quanto lesive dell'art. 14 della Costituzione che sancisce l'inviolabilità del domicilio, permesse perciò solo allorquando siano avvenute nelle forme della intercettazione ambientale, con i presupposti e secondo i limiti degli artt. 266 e segg. c.p.p.. E' questo il caso della ripresa di un impianto di videosorveglianza che, in violazione non solo della norme sulla privacy ma anche di quelle del codice di rito, abbia avuto ad oggetto l'interno di una abitazione altrui, con registrazione audio e video.

- Circa i sistemi di videosorveglianza posti in essere nell'ambito di una attività di indagine essi sono espressamenti consentiti, come detto, dall'art. 234 c.p.p. che li annovera tra le prove documentali, ciò che esclude in radice che con riferimento ad essi si possa porre un problema di violazione del diritto alla riservatezza come tutelato dal D.Lvo n. 196/2003. Laddove la videoripresa intervenga in luogo pubblico essa non costituisce intercettazione ambientale e perciò è consentita anche al di fuori dei limiti posti dalla disciplina della privacy (ad es. con riferimento alla limitazione nella attività di videoripresa e quanto alla conservazione delle immagini).

Ove invece l'attività di videoripresa sia avvenuta all'interno di un appartamento essa costituisce intercettazione ambientale e presuppone perciò una richiesta del PM ed un provvedimento ammissivo del GIP procedente.

Come già detto dalla violazione della disciplina sulla privacy di cui al D.Lvo n. 196/2003 possono discendere conseguenze anche penali.

L'art. 167 – Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione delle norme del decreto legislativo in questione è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. Nei casi più gravi, sempre laddove il fine sia di trarne per sè o per altri profitto o di recare ad altri un danno, il soggetto è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

L'art. 168 - Falsità nelle dichiarazioni e notificazioni al Garante

1. Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

L'art. 169 - Misure di sicurezza

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non ecce-

dente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

L'art. 170 - Inosservanza di provvedimenti del Garante

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante, sia quanto a quello autorizzatorio sia con riferimento a quelli conseguenti a reclamo e ricorso, è punito con la reclusione da tre mesi a due anni.

L'art. 171 - Altre fattispecie

1. La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.

L'art. 172 - Pene accessorie

1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza

---

E' chiaro che un sistema di videoripresa potrebbe essere in violazione delle norme dettate dal Codice sulla privacy e le videoriprese realizzate costituire addirittura reato, sia quelli di cui sopra sia di diverso tipo (ad es. per l'avere taluno ripreso con il sistema della videosorveglianza l'ingresso dell'abitazione e del parcheggio di estranei, in violazione dell'art. 615 bis c.p. che punisce il reato di interferenze illecite nell'altrui vita privata). Nel qual caso, evidentemente, l'uso in giudizio della ripresa è costituita dal fatto che essa

altro non è che il corpo del reato commesso.

Così come è utilizzabile l'immagine acquisita e/o conservata illecitamente allorquando essa costituisce ad esempio prova o alibi di un omicidio. L'autorità garante infatti non può bloccare l'uso in giudizio della videoripresa in quanto l'atto con cui si impedisce il trattamento dei dati personali è atto amministrativo. L'inutilizzabilità di cui all'art. 11/2° del D.Lvo non opera infatti nel processo penale, in relazione al quale vige la sola sanzione di inutilizzabilità interna alle norme processuali.

Al termine della relazione qualche notazione di carattere extragiuridico mi deve essere consentita. Nonostante i contrappesi di cui sinora si è detto l'avanzare delle tecnologie e le esigenze di tutela della sicurezza pubblica implementeranno ancora il sistema della videosorveglianza, collegando più sistemi tra loro e banche dati a questi, creando una rete via via più capillare e diffusa.

Senza qui scomodare lo Stato di Oceania in cui campeggiavano - nel celebre romanzo - cartelli con lo slogan *Big Brother is watching you* che ricordavano ai sudditi che erano continuamente controllati, non si possono non preconizzare gli sviluppi di un sistema di tal fatta.

Non ci troviamo neppure di fronte al vecchio *panopticon* descritto dal filosofo e ingegnere inglese Jeremy Bentham, né a una sua superfetazione. Nel caso del modello proposto da Bentham eravamo di fronte a un potere esercitato da un oscuro osservatore. Nel *panopticon*, quindi i pochi osservavano i molti. Ora invece ci troviamo di fronte a una situazione in cui molti scrutano e controllano pochi. Si realizza cioè un mutamento nelle forme di controllo che ha ripercussioni profonde nel tessuto sociale, dinamica di controllo sociale definita da taluno come *synopticon*.

Un tempo, la sorveglianza era un processo in cui persone in carne e ossa erano controllate da altre. Con lo sviluppo della modernità, i sistemi che iniziarono a sfruttare l'elaborazione di dati per-

sonali astratti si perfezionarono sempre più. Ciò che si dimostrava efficace in un settore di rado però ne interessava un altro. I contenitori di dati erano ermeticamente sigillati. Oggi la situazione sta mutando poiché quei contenitori sono più permeabili. Le pratiche di sorveglianza e i flussi di dati si muovono molto più liberamente da un settore all'altro. Ciò che accade in un'area interessa anche un'altra. Il cosiddetto sistema a controllo incrociato è da tempo una caratteristica dei sistemi di sorveglianza e può essere osservato in contesti molto semplici. A uno studente può non essere permesso di laurearsi, per esempio, finché non siano interamente pagate le quote relative al residence in cui lui o lei hanno soggiornato. In questo caso, un sistema i cui riferimenti sono di tipo accademico è usato da un altro, di tipo commerciale, al fine di ottenere gli adempimenti del caso.

Ma non è questo l'unico modo in cui i contenitori della sorveglianza mostrano la loro crescente permeabilità. Le società di sorveglianza esistono laddove il controllo cessa di essere una mera caratteristica di rapporti istituzionali distinti e diviene routinario e ampiamente generalizzato nei confronti delle popolazioni. I corpi che nella modernità scompaiono spariscono ancor prima con l'avvento delle tecnologie di comunicazione e informazione.

Le società sorvegliate qui ipotizzate però non hanno nulla a che vedere con un controllo totalitario (da qui la differenza essenziale con lo scenario del romanzo orwelliano), non sono tecnologicamente determinate e nemmeno frutto di semplici imposizioni calate dall'alto. Esse invece evolvono e mutano tramite mezzi e in direzioni che sono ad un tempo tecnologici, socio-culturali e politico-economici.

In Gran Bretagna, per esempio, la paura rispetto al crimine di strada costituisce uno stimolo potente nei riguardi dei politici, che sono per questo indotti a sostenere l'installazione di televisioni a circuito chiuso e sistemi di telesorveglianza. Ma gli stessi sistemi sono sostenuti anche dalle compagnie commerciali che li producono, in quanto soluzioni tecniche di rilevamento nei confronti dei conflitti sociali metropolitani. Ed eventi drammatici come l'11 settembre (per tornare all'esempio con cui ho iniziato il mio inter-

vento) non fanno che intensificare questo processo, legittimando l'espansione del mercato della sicurezza - *warfare* - a scapito di quello della protezione sociale - *welfare*.

Considerazioni queste ultime non mie, bensì opera di *David Lyion* – sociologo e professore all'università di Kingston in Canada, sede della Queen's University, nonché direttore del Sourveillance Project - contenute nel libro "*La società sorvegliata. Tecnologie di controllo della vita quotidiana*", Feltrinelli, 2002, che suggerirei a tutti coloro, come noi, che si occupano di videosorveglianza, di leggere.

Progetti di ricerca in Visione artificiale per la Video sorveglianza

Prof. Rita Cucchiara
Dipartimento di Ingegneria dell'Informazione
Università di Modena e Reggio Emilia

Tutti ora parlano di Video Sorveglianza, sui giornali, TV e Web, spesso intendendo in forma molto riduttiva solo le centinaia di telecamere installate nelle nostre città, nelle strade e negli uffici, collegate attraverso una rete (*wired o wireless*) a centri di memorizzazione, a centri di controllo remoti o distribuiti, dove le immagini dovrebbero essere osservate con continuità da occhi attenti di addetti alla sicurezza.

L'azione deterrente e l'azione di supporto a posteriori della raccolta di dati visuali in aiuto alle attività investigative e giudiziali è ben noto, e non sta a me ribadirlo, come è altrettanto noto, purtroppo, che sistemi CCTV di questo tipo difficilmente possono avere un ruolo attivo nelle prevenzione del crimine, perchè non esiste disponibilità di personale umano capace di attendere alle attività di vigilanza 24 ore su 24. Nelle agenzie private americane la presenza costante di un osservatore umano è valutato in circa 150.000$ all'anno, anche considerando che studi di psicologia della percezione concordano che dopo solo 20 minuti l'attenzione umana su monitor degrada sotto il limite di accettabilità.

Ciò malgrado le telecamere stanno diffondendosi sempre di più: quelle istallate in Italia solo dagli enti pubblici sono migliaia, centinaia a Roma e a Milano e numerose anche nelle città di provincia; si pensi ad esempio che nel 2008 il record sembra essere di Reggio Emilia, con una telecamera ogni 350 abitanti.

L'opinione pubblica e dei media è comunque altalenante anche

rapportata alla percezione di sicurezza degli individui. Mi piace riportare una notizia molto enfatizzata anche sulla stampa italiana di qualche mese fa: in una intervista al "*The Guardian*" del maggio 2008 Mick Neville, ispettore di Scotland Yard, ha bollato la Video Sorveglianza come un "utter fiasco", affermando che l'Inghilterra a fronte della enorme diffusione degli apparati (4,2 milioni di telecamere con un rapporto 1 a 14 tra telecamere ed abitanti) e dei miliardi di sterline impiegati, ha sistemi decisamente inefficaci; ha stimato solo in un 3% il miglioramento nella lotta alla criminalità grazie alle telecamere.

Il problema è quello prima richiamato: le forze dell'ordine non possono materialmente osservare in tempo reale centinaia di migliaia di video e l'efficacia di tali sistemi nel momento in cui il fatto si verifica è di praticamente nulla. L'ispettore al termine dell'intervista, però, assolve i sistemi del futuro e ipotizza come unica soluzione plausibile l'affidarsi a software di analisi di immagini per elaborare in tempo reale i video e fornire allarmi. Finalmente!

Da anni la comunità scientifica internazionale sta lavorando nella Visione Artificiale per trovare soluzioni all'interpretazione della scena in modo automatico. Le nuove generazioni di sistemi di videosorveglianza non sono e non saranno più soltanto sistemi hardware, ma trovano nel software di analisi, spesso chiamato com-

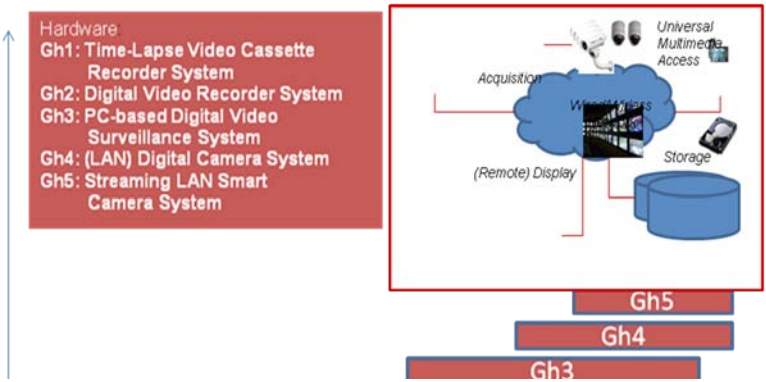

Fig.27 – generazioni dell'hardware di sistemi di videosorveglianza

mercialmente di **video analytics**, il più grande valore aggiunto.

1. Anatomia dei Sistemi di Videosorveglianza

Nei sistemi di video sorveglianza si sono susseguite diverse generazioni di tecnologie dell'hardware, i cui limiti temporali non sono formalmente definiti. Il primo sistema pubblicizzato che possiamo descrivere come di "prima generazione" totalmente analogico risale al 1969, installato al Muncipal Building del City Hall di New York: con telecamere CCTV analogiche collegate a VCR (*video cassette recorder*) e monitor. La seconda generazione ha visto l'impiego di tecnologia digitale nella registrazione: le telecamere analogiche CCTV venivano collegate a video switch e trasferite a DVR (*digital video recorder*) per salvare qualche immagine selezionata in un formato standard come ad esempio il JPEG. (Fig.27)

Mentre ormai i sistemi con videocassette stanno sparendo, i sistemi con registrazione digitale sono tuttora i sistemi a basso costo in uso in molte sedi dove non è richiesta un'interazione con il servizio di sorveglianza (ad es in alcuni uffici pubblici o banche o esercizi commerciali).

Una grande trasformazione si è verificata quando le tecnologie informatiche hanno soppiantato quelle puramente elettroniche, impiegando il calcolatore, sostituendo al multiplexer e al DVR un PC con *video capture card* capace di comprimere immagini e video su hard disk.

Tipicamente questi sistemi visualizzano poche telecamere per volta a risoluzione completa e a colori mentre registrano a risoluzione ridotta (ad es. formato CIF 320x240). La registrazione avviene a 25 o 30 frame al secondo complessivamente per tutte le telecamere. Questi sistemi sono ottimali per la visualizzazione di piccole installazioni private (negozi, uffici); spesso però sono impiegati anche in grandi centri come nei centri di polizia, ma hanno una qualità non sempre accettabile per l'analisi forense, dando a disposizione pochi frame (ad esempio 3 al secondo con 10 telecamere) e a una risoluzione così bassa che spesso rende impossibile l'identificazione degli individui o delle targhe.

I sistemi più recenti adottano telecamere digitali, collegabili an-

che alla rete LAN con tecnologia IP , spesso controllate in remoto e brandeggiate in pan, tilt o zoom (PTZ). Le telecamere sono collegate a uno *switch ethernet* che le collega a centri di controllo e di registrazione remoti. In larghe installazioni urbane, "foreste di telecamere" sono collegate in fibra ottica a centri di acquisizione con una topologia a stella da cui i dati sono trasferiti a centri di controllo. Le ultime generazioni hardware permettono di avere le cosiddette *smart cameras,* ossia telecamere equipaggiate di processori RISC per permettere una miglior compressione video anche in *streaming* (si parla di *streaming-lan cameras*) con tecnologie MPEG2, MPEG4 o H264 L'uso di IP e di streaming naturalmente implica tutti i problemi di sicurezza legati ad internet e quindi non sempre vengono installate come dovrebbero, se non in intranet o in reti sicure.

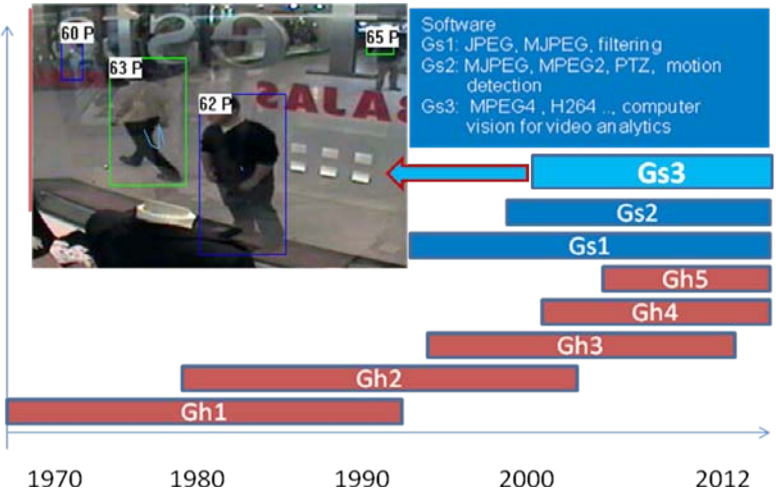

Fig.28 – generazioni del software di sistemi di videosorveglianza

Questo miglioramento tecnologico e l'uso di un calcolatore integrato nelle telecamere o centralizzato ha permesso di iniziare ad inserire nei sistemi di *videosorveglianza* anche software dedicato

sempre più sofisticato per l'elaborazione e l'analisi automatica dei video.

I primi sistemi digitali prevedevano solo l'uso di elaborazione di immagini per il miglioramento della loro qualità e per la compressione. Ad essi si sono aggiunti tool software per il controllo del movimento delle telecamere brandeggiabili PTZ. Il primo software di visione artificiale realizzato per sistemi di video sorveglianza "intelligenti" è il così chiamato *motion detector*, ovvero un tool per il riconoscimento automatico delle zone in movimento nel video, al fine di identificare oggetti di interesse (Fig.28).

Una vasta pletora di algoritmi di motion detection sono stati studiati ed implementati negli anni sia in sistemi di ricerca che in sistemi commerciali; i più semplici si basano su differenze tra frame successivi per verificare la presenza di moto (e magari abilitare solo in questo caso una registrazione selettiva), altri si basano su differenze nello spazio colore o nei livelli di grigio del frame corrente con un modello dello sfondo (*background suppression*), per estrarre pixel considerati di interesse in quanto diversi dallo sfondo stesso. Il metodo più studiato in letteratura è basato su *Mixture of Gaussians*, proposto al MIT da Stauffer e Grimson nel 2000 [9] e ora presente anche nelle librerie open-source di OpenCV, ma molti altri metodi più sofisticati e precisi sono stati studiati negli ultimi anni, capaci di gestire il problema delle ombre, e soprattutto di fare anche un inseguimento corretto nel tempo degli oggetti di interesse anche se ripresi da più telecamere.

Il mercato dei sistemi di video sorveglianza è in costante aumento, stimato del 10% all'anno nel mondo con stabilizzazione negli Stati Uniti e crescita in Europa ed in Cina [1]. Le informazioni provenienti da IMS Research (25 marzo 2009) davano una previsione di crescita dal 2004 del 65% annuo. Ora malgrado la recessione, nel 2009-2010 la crescita è del 3% e del 29% all'anno per il mercato delle telecamere analogiche e delle telecamere IP rispettivamente. A Livello EMEA (Europa, Medio Oriente e Africa) è previsto un aumento del 33% all'anno del mercato dell'hardware per la videosorveglianza [2]. Le previsioni per il software di video analyti-

cs in surveillance sono in crescita, del 10% annuo (215 Milioni di sterline nel 2009). Secondo la fonte Frost & Sullivan (Dic. 2008) [3] gli investimenti nel 2009 del British Government UK sono di 80 Milioni di sterline mentre gli investimenti nel 2009 del Department of Homeland Security (DHS) USA di 239 Milioni di Dollari.

Questi numeri sono una prova dell'immenso interesse non solo scientifico e sociale ma anche economico legato alla video sorveglianza.

2. **Progetti di ricerca e sviluppo in videosorve**-glianza

Non è difficile immaginare che nel prossimo futuro l'uomo sarà sempre più immerso in una rete di sistemi e sensori digitali capaci di percepire le attività nell'ambiente osservato, individuare situazioni di interesse, interpretare le azioni che si stanno svolgendo, riconoscere espressioni, comportamenti ed affettività ed interagire con gli esseri umani.

Nel mondo della sicurezza ciò porterà alla realizzazione di sistemi attivi e pro-attivi, non più solo in grado di registrare informazioni visuali per analisi a-posteriori, ma capaci di percepire e comprendere ciò che nella scena sta accadendo.

L'estrazione automatica di oggetti in movimento, l'analisi e il riconoscimento di traiettorie, la interazione spaziale tra cose e persone può essere applicata in molti casi concreti. I risultati ora disponibili sul mercato nascono come risposta di tanti anni di ricerca scientifica sull'argomento, in particolare nell'ambito della Visione Artificiale.

La Visione Artificiale (Computer Vision) fino a pochi anni fa era bollata come una disciplina di nicchia al più assimilata ad una sotto-disciplina dell'Intelligenza Artificiale (IA). Con l'IA, la Visione Artificiale condivide molti dei meccanismi inferenziali e strumenti per la rappresentazione della conoscenza. Banalizzando, gli stessi meccanismi di logica computazionale impiegati per la costruzione di sistemi artificiali per il gioco di scacchi possono essere usati per riconoscere l'attività di oggetti in movimento nella scena. A differenza dell'IA, però, la Visione Artificiale non può prescinde-

re dall'essenza dell'input che è fatta di sequenze di pixel, le cui informazioni visuali sono per natura parziali e corrotte da rumore sintattico (a livello di segnale) e semantico (i cosiddetti "distrattori" nella scena).

La Visione Artificiale si avvale fortemente della Pattern Recognition, la disciplina che studia tecniche, spesso statistiche, di classificazione e riconoscimento di forme a partire da dati misurati o calcolati, siano essi visuali, audio, testuali, multimediali in genere o numerici. Ora la Visione Artificiale e la Pattern Recognition sono ben affermate nel mondo dell'ICT e sono materie di studio in molti corsi di laurea di ingegneria informatica ed informatica, come a

Fig.29 – Chicago Virtual Schield [4]

Modena a Ingegneria da più di dieci anni.

I risultati degli studi di Visione Artificiale per la sorveglianza sono sotto gli occhi di tutti: alcuni già passati in sistemi commerciali per il controllo di zone ben delimitate: sappiamo bene quanto i sistemi OCR di riconoscimento automatico di targhe attraverso i varchi funzionino in modo assai preciso! È ben noto che sistemi biome-

trici di riconoscimento del volto frontale e di persone consenzienti ad esempio agli accessi delle frontiere e degli aeroporti sono molto efficaci e in forte diffusione.

Si può fare molto di più: tra i progetti in corso più imponenti al mondo bisogna citare quello che dal 2006 si sta concretizzando a Chicago: già migliaia di telecamere erano collegate in fibra anche prima dell'11 settembre. Il Comune di Chicago in collaborazione con l'IBM Watson Research Center che ha sviluppato un sistema di surveillance automatico estremamente potente (S3 - Smart Surveillance System), ha iniziato il progetto chiamato Operation Virtual Shield con circa 3000 telecamere (215 M$), molte delle quali dotate di software di lettura targhe, di riconoscimento dei vol-

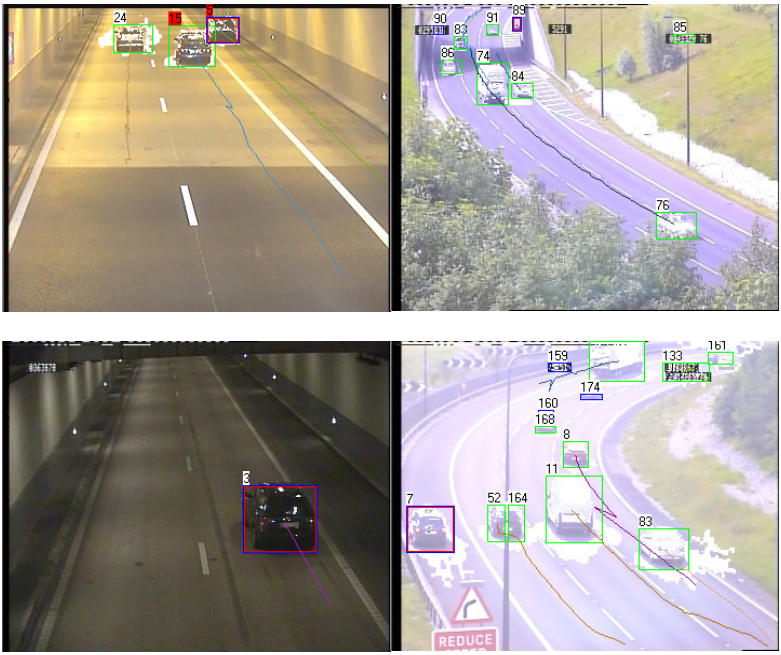

Fig.30 – Esempi di riconoscimento di auto in tunnel e corsie di emergenza ImageLab-Traficon 2005[8]

ti a gate, di riconoscimento dell'audio per rilevare possibili spari e orientare automaticamente le telecamere brandeggiabili in quella zona (Fig.29).

Questo sistema è incredibilmente imponente sia per l'ammontare del finanziamento, sia per la tecnologia utilizzata. Ciò nonostante il software di analisi è relativamente semplice per controllo targhe e volti in ambienti controllati.[4]

Un altro esempio notevole è il progetto chiamato Golden Shield nato in Cina a partire da Pechino che per i giochi olimpici ha installato 200.000 telecamere con salvataggio del volto in zone di accesso ed è stato finanziato dai maggiori partner industriali americani: IBM, Honeywell and General Electric. Questo progetto si espanderà nei prossimi due anni con il progetto Chinàs All-Seeing Eye che collegando 2 milioni di telecamere, dati provenienti da VISA Card, cell phone, Mc Donalds happy meals card ecc, creerà

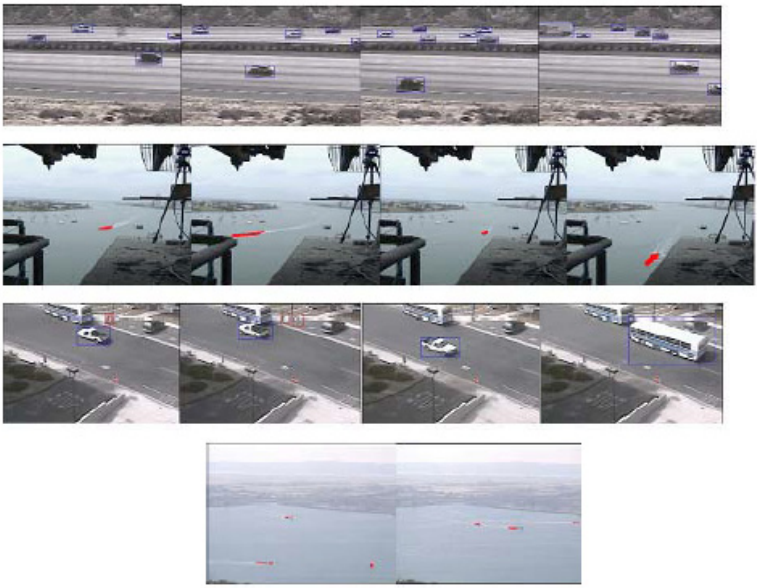

Fig.31 – Esperimenti di sorveglianza nei progetti DIVA ed ATON presso Università di San Diego [12]

la più grande rete mondiale di controllo di dati personali, ovviamente senza alcuna limitazione di vigilanza, in assenza totale di limiti legislativi e della privacy[5].

Da anni però la ricerca scientifica sta lavorando in algoritmi più sofisticati in particolare per il riconoscimento della scena. Le prime ricerche riguardavano l'ambito dei trasporti extraurbani e l'analisi dei veicoli in situazioni meno strutturate, ad esempio per riconoscere traiettorie anomale o situazioni di particolare pericolo [6]. Molti sistemi sono stati prodotti nei laboratori di ricerca americani[7] ed europei[8]. Nella Fig.30 si vede, ad esempio, il rilevamento automatico di macchine ferme in autostrada o in tunnel (frutto di una collaborazione nel 2005 di ImageLab con l'azienda belga Traficon).

Queste ricerche poi si sono rivolte all'analisi della presenza e dell'aspetto di persone per video sorveglianza, Per realizzare le prossime generazioni di sistemi di video sorveglianza attiva il lavoro di ricerca è ancora lungo ed è una delle sfide attuali più cruciali dell'ultimo decennio.

Questi studi sono nati e si sono sviluppati soprattutto in centri di ricerca statunitensi. Tra tutti si deve citare il lavoro pioneristico del progetto VSAM della Carneige Mellon University che nel 1997-2000 ha iniziato ad occuparsi di riconoscimento di persone in ambiente esterno con fondi del DARPA (Defense Advanced Research Projects Agency) [10].

VSAM è stato una pietra miliare e ha permesso di sviluppare commercialmente la video analytics per surveillance (in particolare uno spin-off della suddetta università, ObjectVideo, è ora leader nel mondo)[11] e diffondere la ricerca in visione artificiale, per il ritrovamento di oggetti in movimento, la classificazione di persone e non (ad esempio con reti neurali), il tracking nel tempo di oggetti in movimento anche con telecamere PTZ.

Molte università americane lavorano in sorveglianza intelligente, tra queste si vuole citare MIT, CMU, Berkeley, San Diego, Maryland, UCF.

Con l'Università di San Diego, ed in particolare con il gruppo di

Fig.32 – Interfaccia sviluppata dall'Università di Amsterdam in collaborazione con le forze dell'ordine di Rottherdam

ricerca di Computer Vision del prof. Trivedi, l'Università di Modena ha lavorato a lungo nel passato ed in particolare nei progetti ATON e DIVA; il primo per incidenti in strade e il secondo per array di telecamere diversificate e distribuite. Nelle immagini in Fig.31 si vedono esperimenti fatti nel porto di San Diego o attorno allo stadio del Superbowl nel 2003[12]

Un altro esempio importante è il gruppo di ricerca del prof. Mubarak Shah nell'University of Central Florida che lavora con diversi progetti di alcuni Milioni di dollari finanziati sempre dal governo americano; tra questi progetti di grande interesse sono KNIGHT, sviluppato con la polizia di Orlando, per il riconoscimento di traiettorie anomale; COCOA per la gestione di traiettorie da piattaforme aeree mobili; WhereAmI, dove anche in collaborazione con ImageLab di Modena sono stati fatti studi per il riconoscimento automatico delle proprie traiettorie confrontando immagini riprese da cellulari con quelle caricate su database di immagini riprese da sistemi di videosorveglianza e georeferenziati con GPS [13].

Studi simili sono ovviamente condotti anche in Europa da diversi anni. Un'attività interessante si sta svolgendo presso l'Università di Amsterdam in uno dei laboratori più prestigiosi al mondo per l'annotazione di dati multimediali. I ricercatori del laboratorio hanno vinto per diversi anni la competizione mondiale TRECVID [14] per il riconoscimento automatico da video e testi, come ad

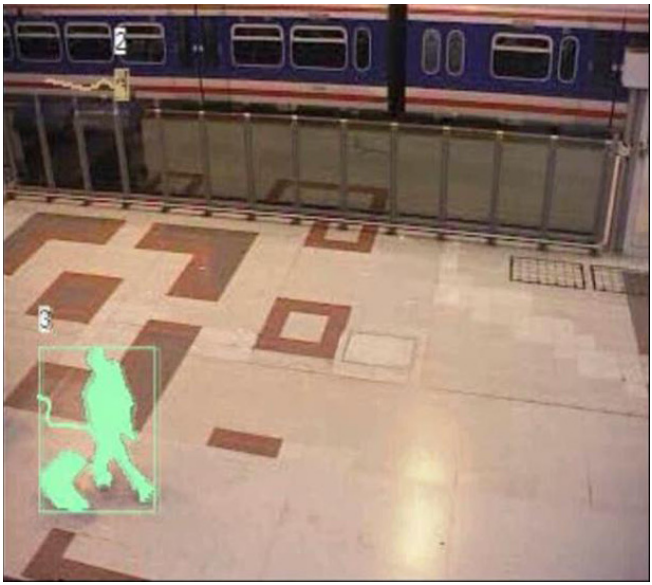

Fig.33 – video di benchmark della Victoria Station elaborato del software Sakbot di Imagelab

esempio “cerca un video con un’esplosione di una bomba”. Queste tecnologie sono applicate nell’analisi forense dove vengono integrate sorveglianza, annotazione e interfacce smart per la visualizzazione di grandi database di video. Nell’immagine di Fig.32 si vede l’interfaccia fatta in collaborazione con le forze dell’ordine di Rottherdam nell’ufficio investigativo forense. ImageLab collabora con l’Università di Amsterdam nell’ambito del progetto VISTA per l’estrazione automatica di persone e nell’ambito del progetto europeo VIDI VIDEO per l’annotazione automatica di concetti in video. Questo ha portato allo sviluppo di un portale presso ImageLab chiamato ViSOR che contiene centinaia di video di ricerca sulla videosorveglianza cone le relative annotazioni manuali per poter fare confronti su risultati ottenuti[15].

Il tema delle valutazioni delle prestazioni è assai dibattuto in ambito scientifico, commerciale e ovviamente politico; prova ne è che ora molti video di ricerca ci provengono da un ente ministeriale ed

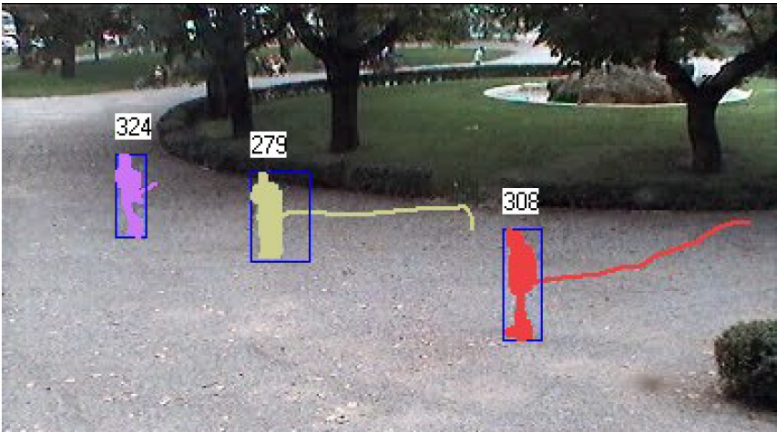

Fig.34 – LAICA: le persone sono riconosciute ed oscurate

in particolare dal database i-LIDS. Questo progetto dell' Home Office Scientific Developement Branch (il dipartimento scientifico degli interni inglesi) vuole proporre video di rifermento per confrontare le capacità di sistemi di detection automatica per il rilevamento di persone, di pacchi abbandonati etc. [16]

Un esempio di risultato è quello che è mostrato nel video di benchmark della Victoria Station a Londra riportato in Fig.33 Questo è il risultato del sistema sviluppato a Modena da ImageLab anche in collaborazione con l'University of Sidney in un progetto finanziato dall'Australian Research Council dove si vede che ogni persona viene inseguita nel tempo, calcolata la traiettoria e verificato se oggetti fermi possono essere considerati "abbandonati".

Il sistema è realizzato completamente in software e si avvale di algoritmi sofisticati di background suppression, analisi del colore, analisi statistiche della forma e lavora in tempo reale sui dati acquisiti dalle telecamere.

Effettivamente negli ultimi anni alcuni problemi sono stati affrontati e risolti per rispondere alle sfide iniziali della sorveglianza, quali il riconoscimento automatico della presenza umana nei video, il tracciamento nel tempo di persone, oggetti fissi (es. pacchi ab-

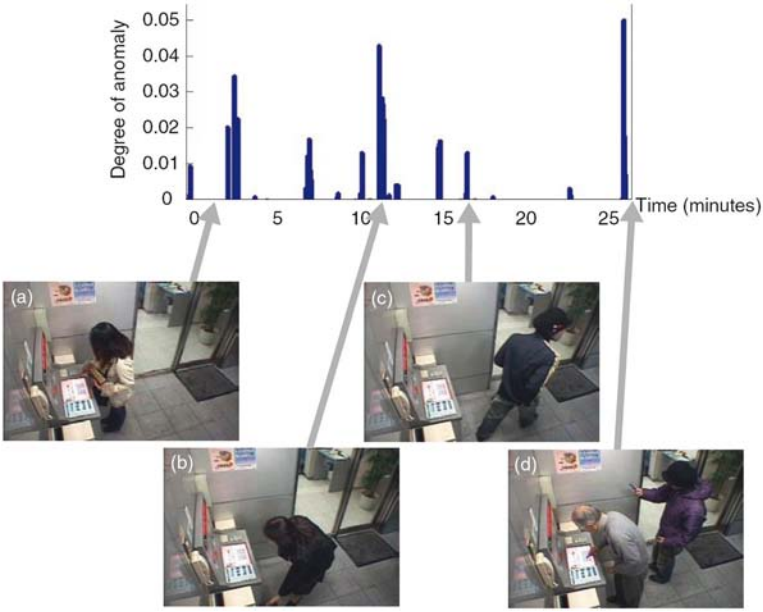

Fig.35 – Esperimenti compiuti all'NTT Cyber Space Lab in Giappone di rilevamento di attività anomale[19]

Fig.36 – esempio di rilevamento del fumo

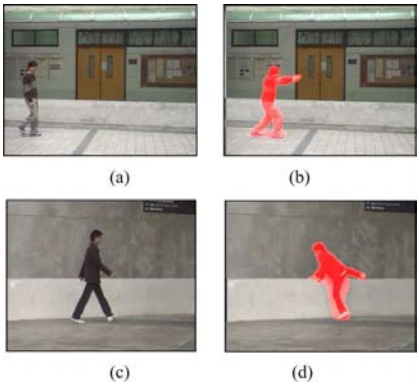

Fig.37 – Rilevamento di comportamenti anomali, Università di Taipei [19]

bandonati) e mobili (es. veicoli nel traffico urbano); sono state sviluppate tecniche biometriche per il riconoscimento del volto; sono stati risolti problemi di riconoscimento di azioni di singoli individui per interessanti applicazioni di "Human-Machine Interface" (HMI) e realtà virtuale.

Un esempio italiano è il risultato del progetto LAICA (Laborato-

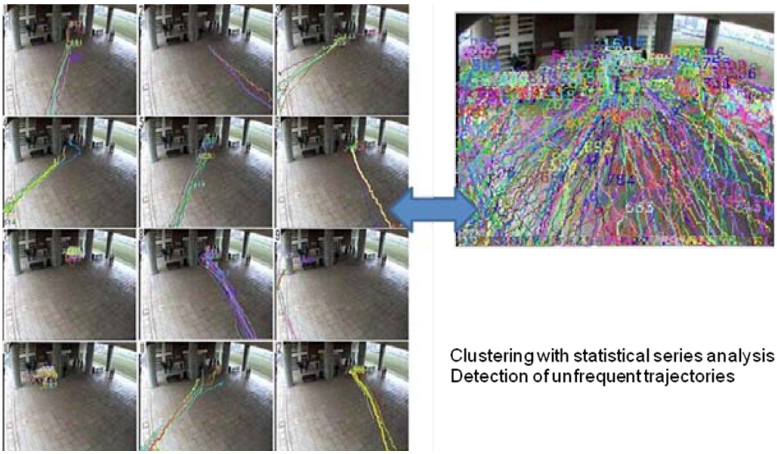

Fig.38 – Classificazione di traiettorie - Imagelab

rio di Ambient Intelligence per una Città Amica) [17] finanziato dal piano telematico Emilia Romagna in cui Modena con l'azienda Bridge129 e il Comune di Reggio Emilia ha sperimentato soluzioni di riconoscimento di persone in parchi pubblici cittadini. Come si vede dalla Fig.34le persone sono riconosciute ed oscurate. Ciò significa che da una parte per la polizia è possibile avere informazioni biometriche, e contemporaneamente ad un utente esterno, magari collegato via web, la privacy è garantita mostrando immagini senza identità. Pensate ad esempio ad una possibile applicazione per vedere lo stato e l'affollamento del parco evitando di vedere l'identità di bambini e passanti.

Ora la ricerca degli ultimi anni sta sviluppando tecniche statistiche per lo più per il riconoscimento di eventi sospetti e di azioni. In alcuni casi eventi semplici sono relativamente facili da caratterizzare, in altri sono assai più complessi.

La ricerca sull'analisi comportamentale nei video può portare a risultati concreti, in casi strutturati. Un esempio è quello di riconoscere comportamenti anomali davanti agli sportelli bancari (bancomat, ATM), dove normalmente una sola persona deve rimanere

Fig.39 – Rilevamento di persone in ore notturne in collaborazione col Comune di Modena

e per un tempo limitato davanti allo sportello controllato da telecamere.

Nelle immagini riportate in Fig.35 si vedono esperimenti compiuti all'NTT Cyber Space Lab in Giappone [18], dove con tecniche standard di statistica (MoG per rilevare oggetti in movimento, Principal Component Analysis per selezionare le feature di interesse classificate con Support Vector Machine), sono stati controllati in video la presenza di anomalie, come persone che raccolgono carta dal cestino, persone che si presentano al cospetto di altri e di nascosto si avvicinano, ecc. Le immagini sono registrate a bassa risoluzione (120 x 240) e acquisite con telecamere CCD standard a due metri di distanza.

Gli eventi e le situazioni di interesse non sono necessariamente legati alle persone. Un esempio di evento che può essere ritrovato automaticamente è la presenza di incendi e in particolare di fumo, anche in ambiente aperti dove altri sensori non possono essere usati. Nell'esempio in Fig.36 si vede che il fumo viene ritrovato.

Il sistema in realtà rileva anche la presenza di persone ma che non sono considerate interessanti mentre studiando la variazione di energia con il calcolo di trasformate Wavelet si ottiene il riconoscimento di zone di fumo. Il sistema, sviluppato in Imagelab è ora in fase di ingegnerizzazione da parte di Bridge129, che sta facendo esperimenti ormai da qualche mese sulla robustezza ai falsi positivi e negativi.

Presto si potranno anche riconoscere azioni degli individui e studiare così attività e comportamenti pericolosi, individuando traiettorie anomale o variazioni della postura e della gestualità. Le prove di Fig.37 sono fatte presso l'Università di Taipei [19], usando un ensamble di operatori visuali e metodi statistici di postura.

Analisi simili sono in corso anche presso ImageLab per distinguere traiettorie semplice o complesse e azioni semplici quali allacciarsi una scarpa, camminare o bere. In Fig.38 si vedono centinaia di traiettorie di persone estratte automaticamente dai video e raggruppate per similarità. In questo modo si possono individuare traiettorie sospette e non abituali.

Speriamo che presto questa attività, che è simile allo stato dell'arte condotto in laboratori di tutto il mondo, possa portare a risultati concreti ed utilizzabili sul campo. Ci vorranno certo alcuni anni, come è normalmente necessario anche in altri campi, per portare la ricerca ad un solido trasferimento industriale.

E nel frattempo? Nel frattempo qualche esperimento può essere iniziato, ad esempio con il Comune di Modena. Ovviamente servono finanziamenti per pagare ricercatori, oltre che per istallare hardware; la collaborazione serve anche anche per cercare finanziamenti comuni, come ad esempio della Regione o dei Ministeri Italiani.

In Fig.39 è riportato un esempio dei sistemi Imagelab applicati a telecamere di Modena; il sistema permette il riconoscimento automatico di persone, anche di notte, in zone sospette e il rilevamento di alcune informazioni visuali mediante ricostruzione 3D (ad esempio l'altezza dell'individuo).

Cosa possiamo fare di questi dati? Primo, attivare allarmi automatici se succede qualcosa statisticamente non frequente, come due persone che sostano a lungo di notte in un sottopassaggio, come supporto a guidare l'attenzione delle forze dell'ordine. Secondo, può certo servire di supporto all'analisi forense per l'analisi e il miglioramento visuale a posteriori in aiuto alle investigazioni.

Questo probabilmente è il futuro dei sistemi di videosorveglianza, quello cioè di fornire il supporto hardware e software per il controllo in tempo reale, di realizzare sistemi informativi completi capaci di gestire al meglio le enormi quantità di dati multimediali e testuali e di fornire un supporto concreto ed efficiente all'analisi forense per la sicurezza urbana e dei singoli individui.

3. Riferimenti

[1] Harris Trends in video surveillance industry, Mobotix conference 2007

[2] http://www.imsresearch.com 2009

[3] http://www.researchandmarkets.com/reports/612498 2009

[4] www.ibm.com/press/us/en/pressrelease/22385.wss 2009

[5]N. Klein Chinàs All-Seeing Eye: A Nation Under Surveillance 2009 http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye

[6]D. Koller, K. Daniilidis, H.-H. Nagel, Model-Based Object Tracking in Monocular Image Sequences of Road Traffic Scenes IJCV (1993)

[7] F. Porikli, X. Li, Traffic congestion analysis in compressed video without tracking, Proceedings of IEEE International Conference on Intelligent Vehicles, Parma, 2004

[8] R. Melli, Andrea Prati, Rita Cucchiara, Lieven de Cock: Predictive and Probabilistic Tracking to Detect Stopped Vehicles. WACV/MOTION 2005: 388-393

[9] Chris Stauffer, W. Eric L. Grimson: Learning Patterns of Activity Using Real-Time Tracking. IEEE Trans. Pattern Anal. Mach. Intell. 22(8): 747-757 (2000)

[10] Collins, Lipton, Kanade, Fujiyoshi, Duggins, Tsin, Tolliver, Enomoto, and Hasegawa, "A System for Video Surveillance and Monitoring: VSAM Final Report," Technical report CMU-RI-TR-00-12, Robotics Institute, Carnegie Mellon University, May, 2000

[11] N. Haering, P. Venetianer, and A. Lipton, "The evolution of video surveillance: an overview," Machine Vision and Applications, vol. 19, no. 5, pp. 279-290, October 2008

[12] A. Prati, I. Mikic, M.M. Trivedi, R. Cucchiara, "Detecting Moving Shadows: Algorithms and Evaluation" in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, n. 7, pp. 918-923, July, 2003

[13] A. Hakeem, R. Vezzani, M. Shah, R. Cucchiara, "Estimating Geospatial Trajectory of a Moving Camera" in Proc. of International Conference on Pattern Recognition (ICPR 2006), vol. 2, Hong Kong, pp. 82-87, Aug. 20-24, 2006[14] sito di tracvid

[15] R. Vezzani, R. Cucchiara, "ViSOR: Video Surveillance On-line Repository for Annotation Retrieval" in Proceedings of IEEE International Conference on Multimedia & Expo (IEEE ICME 2008), Hannover, 2008. http://www.openvisor.orgr

[16] H. O. S. D. Branch, "i-lids - imagery library for intelligent detection systems," Website, 2006, http://scienceandresearch.homeoffice.gov.uk/hosdb/.

[17] R. Cucchiara, A. Prati, R. Vezzani, "Ambient Intelligence for Security in Public Parks: the LAICA Project" in Proceedings of IEE International Symposium on Imaging for Crime Detection and Prevention, London, UK, pp. 139-144, June 7-8, 2005

[18] K. Sudo, T. Osawa, K. Wakabayashi, and H. Koike, "Detecting the Degree of Anomaly in Security Videos," NTT Technical Review, Vol. 5, No. 11, 2007

[19] Jun-Wei Hsieh; Yung-Tai Hsu; Liao, H.-Y.M.; Chih-Chiang Chen, "Video-Ba-

sed Human Movement Analysis and Its Application to Surveillance Systems," IEEE Transactions on Multimedia, vol.10, no.3, pp.372-384, April 2008

Analisi dei dati multimediali nelle tecniche investigative

Dr. Vittorio Rizzi
Dirigente Squadra Mobile Questura di Roma

1. Il ruolo dell'investigatore e la scena del crimine

In quanto investigatore, il mio approccio al mondo della video sorveglianza e dei dati multimediali è un approccio di ricerca ai fini di acquisire fonti di prova per la ricostruzione di eventi e di delitti che si sono consumati. Il teatro di questi eventi è la **scena del crimine**. La scena del crimine è, per un qualsiasi investigatore, il suo laboratorio; di più, è un modo di dialogare tra l'investigatore e l'autore del crimine. E' quello che Ottolenghi definiva "**il ritratto parlato**" e che l'investigatore trova nel sopralluogo alla scena del crimine. Il sopralluogo è il momento centrale di un'attività ricostruttiva di un evento delittuoso. L'investigatore è interprete delle varie scienze forensi, deve effettuare la sintesi di diverse attività che vengono svolte dalla polizia scientifica, dal biologo forense, dal medico legale, dall'antropologo forense, e così via.

L'investigatore svolge innanzitutto una funzione investigativa pura, cioè farà l'attività di interrogatorio, di acquisizione di sommarie informazioni, di pedinamenti. Ma l'investigatore, per consuetudine, svolge anche un altro tipo di attività, che si può sintetizzare con il termine di "funzioni tecniche".

In altre parole, l'investigatore effettua quello che si definisce il "sopralluogo virtuale". Otre ad esserci una scena del crimine fisica, infatti, c'è una scena del crimine virtuale, ed è questa la scena del crimine che sempre più spesso si sta rivelando determinante ai

fini dell'attività ricostruttiva di un delitto.

A differenza del sopralluogo fisico, il sopralluogo virtuale trasforma il dialogo investigatore-criminale in un dialogo multimediale, svolto non più in uno spazio fisico ma in uno spazio virtuale.

Ma che cos'è questo spazio virtuale? A cosa serve?

Innanzitutto serve a ricostruire un'investigazione su varie tipologie di casi, dai delitti più gravi (l'omicidio, lo stupro, un sequestro di persona) alle investigazione sul Web (cyber-stolking, intrusioni in sistemi informatici). In uno spazio fisico si cercano tracce, segni di un'azione delittuosa, e quindi il sopralluogo è funzionale a ricercare questi segni e queste tracce. In uno spazio virtuale, invece, si cercheranno tracce elettroniche e le immagini innanzitutto: il monitoraggio del traffico telefonico, il monitoraggio del Web, l'analisi del flusso Internet sono esempi di questi mondo virtuali che si vanno ad esplorare, mondi ricchi di dati e di informazioni.

Prendiamo ad esempio le **intercettazioni**. Prima di tutto è necessario fare una distinzione tra intercettazione e monitoraggio del traffico. Nel primo caso parliamo solamente di fonia, di contenuto audio, mentre quando si parla di monitoraggio del traffico telefonico si intende l'analisi dei numeri telefonici chiamanti e chiamati. Si tratta di una nuova scienza, che gli investigatori chiamano con un neologismo "numerologia"; richiede di orientarsi all'interno dei numeri telefonici, analizzare i tabulati per monitorare il traffico pregresso, tracciare quello futuro, localizzare nello spazio e nel tempo un'utenza telefonica. L'analisi di queste informazioni può diventare problematica quando ci muoviamo, per esempio, su investigazioni che presentano centinaia di milioni di numeri di telefono (numeri del tutto reali). La necessità di creare dei sistemi di filtraggio di questi dati e informazioni attraverso degli algoritmi è tuttora di grande interesse e studio. Recentemente, ad esempio, abbiamo cercato di tradurre il pensiero dell'investigatore in una decina di algoritmi, in modo da generare dalle ipotesi investigative dei criteri di filtraggio dell'informazione.

Anche il **monitoraggio del Web** è un altro esempio di attività che sta diventando sempre più determinante; monitoraggio del Web inteso non solo come sorveglianza, e quindi come protezione, ma anche come analisi passiva (ad esempio lo studio dei dati del passato, la ricostruzione dei log di una comunicazione intercorsa su un sistema informatico) ed analisi attiva (mediante appositi sistemi hardware e software di ricerca). Pensiamo per esempio al sistema VoIP, al sistema delle comunicazioni che avvengono attraverso il Web, al superamento della linea telefonica per comunicare. Nonostante molti sostengano la in-intercettabilità di quello che avviene nel Web, fortunatamente non è del tutto vero.

Esistono infatti tantissime tracce elettroniche che arricchiscono il sopralluogo virtuale: quest'ultimo è fatto anche delle tracce dei Bancomat, dei Telepass, delle tracce di un pagamento con un POS. Il futuro della tecnologia gioca un ruolo importantissimo proprio nella scoperta di nuove tracce elettroniche per arricchire il sopralluogo virtuale, in particolare mediante l'**audio-video sorveglianza.**

L'investigatore è innanzitutto un ricercatore, un collezionista di immagini, ovviamente per fini investigativi e processuali. Non sempre queste immagini, sia per la fase di approfondimento nei labora-

Per essere una impronta biometrica, le caratteristiche fisiologiche o comportamentali considerate devono possedere queste quattro caratteristiche:
Universalità: *ogni individuo deve avere quella caratteristica*
Unicità: *due soggetti non possono condividere la stessa caratteristica biometrica*
Permanenza: *la caratteristica biometrica deve rimanere immutata nel tempo*
Catturabilità: *deve essere possibile misurare quantitativamente la caratteristica biometrica*

tori delle università italiane, sia nel momento in cui devono essere gestite per un uso processuale, hanno quella effettiva utilità. Il lavoro nostro è di raccogliere immagini che provengono dalle più diverse sorgenti, sorgenti che sono spesso assolutamente inidonee. Abbiamo la stragrande maggioranza di fonti analogiche, dalle quali provengono immagini scarsamente utili, a scarsa risoluzione; molti sistemi sono logori e obsoleti.

Tali immagini ci aiutano spesso per quanto riguarda una ricostruzione a posteriori, ma sicuramente siamo molto indietro per quanto riguarda alcune forme di automatismo nel riconoscimento che potrebbero essere di enorme utilità. Recentemente come organo investigativo abbiamo attivato un progetto chiamato "Orme elettroniche"[], volto a ricercare tracce elettroniche in uno scenario reale (per esempio uno spazio di uno sportello bancario). Se attualmente l'impronta biometrica per eccellenza è l'impronta digitale (perché risponde a tutti quei caratteri di **universalità, unicità, permanenza e catturabilità** che deve avere un'impronta biometrica), ogni investigatore auspica a poter utilizzare allo stesso modo le impronte facciali.

Sarà possibile in futuro avere un qualcosa di analogo all'AFIS, cioè ad un automatismo del riconoscimento dell'impronta, nel riconoscimento di un volto? Sistemi funzionanti in condizioni reali sono ancora assenti; sono in fase di studio in laboratorio, mettendo una persona davanti a una telecamera e riprendendolo, fotografandolo in 2 o 3 dimensioni, ma con vincoli sulla dimensione, sul movimento, sullo sfondo. Il problema è tuttora irrisolto se ci caliamo nella realtà, con sistemi spesso obsoleti e soprattutto con immagini in movimento di persone che sono travisate o parzialmente travisate.

Attualmente stiamo sperimentando queste tecnologie in collaborazione con l'Unicredit, che ha adibito a tal fine una bussola di una loro agenzia a Milano. Il sogno investigativo è quello di poter prelevare le immagini di una rapina in una banca, darle in ingresso ad un software di ricerca automatica ed ottenere in tempi ragionevoli una serie di probabili e possibili indizi su quello che è accaduto.

Nonostante tutto, è necessario sottolineare quanto l'assenza di immagini, al di là di ogni valutazione, scientifica o politica, renda

molto più problematica l'investigazione. Certo è che le immagini devono essere individualizzanti e utili. Voglio concludere quindi con il pensiero di un grande scrittore, Arthur Conan, ovvero l'inventore di Sherlock Holmes: "la singolarità è quasi invariabilmente un indizio; quanto più un crimine è banale e comune, tanto più è difficile e incomprensibile".

Organizzatori e sponsor

Imagelab è un laboratorio di ricerca presso il Dipartimento di Ingegneria dell'Informazione dell'Università di Modena e Reggio Emilia.

La ricerca presso l'Imagelab copre diversi argomenti della pattern recognition, computer vision e Multimedia.

In particolare, le principali attività riguardano la videosorveglianza, la visione per applicazioni industriali, l'analisi di immagini mediche, tecniche e strumenti per l'accesso, l'archiviazione, l'annotazione e la trasmissione di contenuti multimediali.

Imagelab è parte di Softech, un centro dipartimentale del Dipartimento di Ingegneria dell'Informazione per lo sviluppo di tecnologie informatiche per le imprese.

Rita Cucchiara, fondatrice e responsabile di Imagelab, ricopre il ruolo di Professore Ordinario in Ingegneria Informatica presso la Facoltà di Ingegneria di Modena dal 2005. E' coordinatrice della scuola di dottorato in ICT e dal 2008 è vicepreside della Facoltà di Ingegneria di Modena.

Insieme a Rita Cucchiara, fanno parte di Imagelab Andrea Prati, Costantino Grana, Roberto Vezzani, Simone Calderara, Giovanni Gualdi, Daniele Borghesani, Paolo Piccinini e Paolo Santinelli.

Collegato ad Imagelab, lo spinoff Vision-e si occupa della ingegnerizzazione di sistemi di Visione Artificiale per sicurezza e la robotica (http://www.vision-e.it/)

Contatti

Prof. Rita Cucchiara
rita.cucchiara@unimore.it
http://imagelab.ing.unimore.it

Università di Modena e Reggio Emilia
Dipartimento di Ingegneria dell'Informazione
Via Vignolese 905, Modena (Italy)
Tel. +39 059 2056136
Fax. +39 059 2056129

CRIS, acronimo di Centro di Ricerca Interdipartimentale sulla Sicurezza è stato fondato per riunire tutte le competenze legate alla sicurezza presenti all'interno dell'Università di Modena e Reggio Emilia e nella regione. Include cinque dipartimenti di ricerca con ampie competenze. Il CRIS adotta un approccio olistico ai problemi legati alla sicurezza, con particolare attenzione alle tecnologie della comunicazione e dell'informazione, scienze della materia, esperienze biochimiche, economiche, sociali, investigative e giuridiche.

CRIS ha quattro missioni principali: Ricerca, Disseminazione, Consulenza e Formazione.

CRIS organizza corsi in sede, corsi specifici sulla sicurezza dei sistemi Informatici, Masters (es, "Information System Security" e "National and International Emergency Management").

Collabora con istituti di ricerca nazionali ed internazionali, con le forze dell'ordine, e con alcune delle società più importanti del settore. I membri del CRIS partecipano e gestiscono progetti di ricerca a livello sia nazionale che europeo.

Contatti

Prof. Michele Colajanni, direttore del CRIS
cris@unimore.it
http://cris.unimore.it

Università di Modena e Reggio Emilia
Via Vignolese 905, Modena (Italy)
Tel. +39 059 2056137
Fax. +39 059 2056129

L'Ufficio Politiche per la Sicurezza Urbana, collocato all'interno del Gabinetto del Sindaco e delle Politiche per le Sicurezze, nasce come sviluppo del progetto "Modena Città Sicura", istituito nel 1995, con il fine di dare continuità ad una attività che, col passare degli anni, ha visto sempre un'attenzione e un impegno maggiore da parte dell'Amministrazione comunale.

Gli ambiti d'intervento di questo settore hanno come finalità l'attuazione di politiche e progetti volti a sviluppare attività che garantiscano la prevenzione della criminalità e il presidio del territorio al fine di innalzare i livelli di sicurezza della città per tutelare il cittadino.

Obiettivi delle attività svolte dall'Ufficio, realizzate in collaborazione con gli altri Settori della Pubblica Amministrazione, sono principalmente: realizzare iniziative finalizzate a ridurre il degrado ambientale, sia esso di tipo sociale o urbanistico, sviluppare e creare modelli di vigilanza del territorio, favorire lo sviluppo di condizioni che limitino l'azione criminale, promuovere lezioni all'interno delle scuole in materia di educazione alla legalità, monitorare il territorio e le situazioni più critiche, intervenire sui conflitti tra cittadini attraverso lo strumento della mediazione, sviluppare azioni finalizzate ad aiutare le vittime di reato e promuovere politiche di integrazione nei confronti degli stranieri.

Contatti

Responsabile dell'Ufficio Salute e Sicurezza
Giovanna Rondinone
059/2032422
giovanna.rondinone@comune.modena.it

Collaboratori
Antonio Assirelli
059/2032431
antonio.assirelli@comune.modena.it

Annalisa Scagliarini
059/2032441
annalisa.scagliarini@comune.modena.it

La Fondazione Marco Biagi - fondazione universitaria con personalità giuridica di diritto privato che non ha fini di lucro - Adapt - Associazione per gli Studi Internazionali e Comparati sul Diritto del Lavoro e sulle Relazioni Industriali - e il Centro Studi Internazionali e Comparati Marco Biagi del Dipartimento di Economia aziendale dell'Università di Modena e Reggio Emilia, operano in regime di convenzione per promuovere i seguenti obiettivi:

- promuovere, attuare e favorire studi e ricerche scientifiche nazionali ed internazionali nel campo del diritto del lavoro e delle relazioni industriali italiane, comunitarie e comparate;
- creare un centro di eccellenza a livello europeo per lo scambio e la diffusione di best practices nell'ambito delle politiche di promozione della occupazione;
- realizzare alta formazione con specifico riferimento alle problematiche della occupabilità e del funzionamento del mercato del lavoro, anche mediante la realizzazione di master, corsi di perfezionamento, tirocini formativi e di orientamento;
- favorire il dialogo sociale a tutti i livelli – comunitario, nazionale, locale – e attività strumentali e di supporto alla didattica e alla ricerca scientifica.

Per raggiungere i loro obiettivi promuovono numerose attività formative (una laurea specialistica, alcuni master, un dottorato di ricerca) e importanti iniziative convegnistiche.

Tra le attività più caratterizzanti si evidenzia la produzione scientifica sia sulla Collana Adapt-Fondazione Marco Biagi (Giuffrè editore), istituita nel corso del 2003, su cui sono stati pubblicati dal 2003 ad oggi cinque commentari su differenti istituti introdotti o riformati dalla Legge Biagi e sulla rivista Diritto delle relazioni industriali

Contatti

Fondazione universitaria Marco Biagi
Largo Marco Biagi, 10 (già V.le Storchi, 2),
E-mail: fondazionemarcobiagi@unimore.it
Tel: 059/2056031
Fax: 059/2056068

Comune di Modena

Università degli Studi di Modena e Reggio Emilia

Presente e futuro dei sistemi di videosorveglianza per la sicurezza urbana

Per la realizzazione di questa pubblicazione si ringrazia il
Centro di Ricerca Interdipartimentale sulla Sicurezza (CRIS)