

Identità a prova di futuro

In un mondo dove la chirurgia plastica manipola i nostri lineamenti, trasforma il sorriso, incide addirittura sulle corde vocali donandoci ugole da usignoli, mentre i prodigi della contattologia ammantano di azzurro occhi in realtà nocciola, trapianti di capelli regalano nuove giovinezze, cosa di una persona rimane inalterabile, imm modificabile, non sofisticabile? Difficile dirlo e soprattutto provarlo. Identità è uno dei concetti più sfuggitivi di questa nostra epoca "allo stato liquido", come l'ha definita il sociologo Bauman. Viviamo in una realtà caotica, magmatica, sempre in movimento, dove l'effetto globalizzazione arriva ad investire la criminalità rendendola transnazionale, mobile e quanto mai di aspetto mutevole. Guerriglieri che hanno combattuto in Afghanistan, Cecenia, Algeria si spostano a fare proselitismo in altri Paesi e hanno bisogno di viaggiare rendendosi irricognoscibili. Latitanti, mafiosi che cercano di ricostruirsi una nuova vita all'estero, ladri e rapinatori pregiudicati che migrano dalle zone consuete d'azione dove sono ormai facce conosciute, trafficanti di esseri umani, droga e armi spinti oltre confine dall'avidità di procurarsi clientele ovunque nel mercato planetario. Sono molti i fantasmi nascosti dietro generalità posticce o rubate. La falsificazione e il furto d'identità sono tra i reati più frequenti e tipici del nostro tempo. Non è un caso che nel capitolo sicurezza dell'agenda dei governi, l'accertamento dei dati personali inizi a comparire tra le priorità. Biometria sembra la parola magica, ma prima di considerarla un abracadabra bisognerà percorrere molta strada sulla via della cultura democratica, alla ricerca dell'esatto baricentro tra controllo e privacy, come sulla via dell'applicabilità scientifica. Sebbene le tecnologie biometriche siano diventate sofisticatissime siamo ancora lontani dagli scenari hollywoodiani di Minority report dove libellule elettroniche sono in grado di leggere l'iride anche ai passeggeri della metropolitana addormentati, quindi con le palpebre chiuse, o di Nemico pubblico che prefigurava già nel 1998 satelliti in grado di dare il dettaglio antropometrico di volti ripresi in strada. La situazione è diversa riguardo i metodi di accesso ai luoghi di lavoro o aree riservate (per esempio militari) come illustrano bene le parole di Angelo Filippelli, direttore della 3S Team, azienda che produce software e soluzioni di sicurezza biometriche utilizzati in tutto il mondo, dal famoso Ncis (Naval criminal investigative service degli Usa) come dal parlamento svedese e dalle industrie australiane: "I sistemi ad uso civile funzionano perfettamente grazie alla collaborazione della persona che ha interesse a farsi riconoscere e sono più agevoli sia per il numero ristretto di individui a cui applicarli, sia per il confronto immediato del dato biometrico con quelli di tutti coloro che sono autorizzati all'ingresso. Viceversa per il riconoscimento di polizia sussistono ancora molti limiti. Perché un sistema d'identificazione sia valido ai fini investigativi devono sussistere tre condizioni: univocità del dato, facilità di rilievo, possibilità di confronto dei risultati, cioè anche dati interfacciabili". Se ciò che propone la ricerca biometrica faccia parte del nostro futuro prossimo o sia piuttosto fantascienza, sarà solo il tempo a decretarlo. Ma una sbirciata alle nuove proposte e allo stato dell'arte dei sistemi d'identificazione può aiutarci a immaginare il domani.

Il dito accusatore Nel 2004 un avvocato viene arrestato nell'Oregon: le sue impronte digitali coincidono con quelle scovate a Madrid su uno dei due ordigni inesplosi dell'11 marzo. L'Fbi mette in cella il legale, cittadino Usa di fede musulmana, anche se i poliziotti spagnoli non credono alla sua colpevolezza. Alla fine dimostrano che le dita sotto accusa appartengono ad un algerino. Il caso è da ricordare proprio per la sua rarità a riprova del fatto che in Italia come nel resto del mondo il rilievo dattiloscopico, ovvero delle impronte digitali, è il metodo per il momento maggiormente affidabile e utile. Affidabilità statistica, perché finora non è mai successo di scoprire due impronte uguali in individui diversi. Utilità nell'identificazione, dovuta alla presenza storica di archivi dattiloscopici delle forze dell'ordine consultabili e confrontabili in tutto il pianeta. A ciò si aggiunge un piccolo non indifferente orgoglio nazionale: il sistema di rilievo italiano è più sicuro di altri, perché certifica l'identificazione individuando almeno 16 "minuzie", ovvero punti significativi, nell'impronta a differenza per esempio di quello che succede in Venezuela ai quali dattiloscopisti bastano 11 punti per delineare un profilo valido in sede processuale. Una perizia e precisione di lettura che ha reso i nostri esperti indispensabili nel riconoscimento delle vittime dello tsunami del 2005 in Asia. Lunghi dall'essere "obsoleto", il rilievo delle impronte digitali viene perfezionato e reso più pratico dalle tecnologie digitali: scanner che registrano le linee papillari dei polpastrelli al posto di carta e inchiostro, immagini pronte a essere trasformate in algoritmi numerici e informatizzate attraverso software di archiviazione ultradefiniti; sensori wireless che permettono ai cops americani di effettuare il riconoscimento direttamente in strada, smart card che controllano l'accesso a scuola agli studenti londinesi e sistemi pay by touch che rendono veloce e più garantito (soprattutto per chi eroga il servizio) il noleggio di un'auto come l'acquisto on line di un'attrezzatura da taekwondo. Ne è convinto sostenitore il ministro dell'Interno Giuliano Amato che ai lavori del Jhai, il meeting informale dei ministri di Giustizia e degli Affari interni dell'Unione, svoltosi l'ottobre scorso a Lisbona, ha citato la "possibilità di intercettare gli

overstayer prendendo le impronte digitali alle frontiere esterne a chiunque entra, ove non ci siano già attraverso passaporti biometrici emessi dai Paesi di provenienza. Per l'Italia è importantissimo, perché l'overstayer è il grosso della clandestinità e noi spesso lo troviamo senza documenti”.

Occhio ai controlli Fra le altre misure che coniugano biometria e sicurezza prese in esame dall'Ue, il titolare del Viminale punta sul riconoscimento tramite lettura dell'iride, già attivo dal 2005 all'aeroporto londinese di Heathrow. “I tempi sono maturi – ha detto il ministro dell'Interno – per applicare anche agli scali italiani questo programma che assicurerebbe un fast track, cioè permetterebbe di avere un canale veloce di ingresso al gate e al proprio aereo ai passeggeri affidabili”. Mentre prima si leggeva la retinatura della cornea, con un effetto sgradevole d'invasività perché si doveva appoggiare il viso al dispositivo biometrico e posizionare l'occhio in corrispondenza di una fessura, oggi grazie al metodo Heathrow la lettura dell'iride può essere fatta a debita distanza rendendo il controllo più facilmente accettabile dai cittadini. Senza inficiarne il potere identificativo. I margini di errore sono bassissimi. L'iride è strutturalmente invariante già ad un anno dalla nascita e rimane tale fino alla vecchiaia, la possibilità di avere due iridi uguali è pari a 1x10 alla 78esima, in pratica nulla se si compara al numero della popolazione mondiale, 1x10 alla decima. I nuovi sistemi biometrici riescono a fornire immagini di alta qualità anche quando l'individuo inforca occhiali da sole o lenti a contatto e verificano la presenza di occhi vivi, controllando la normale e continua variazione della dimensione della pupilla, abilità non indifferente a fini investigativi. A chi vuole ingannare i controlli e cambiare identità non rimarrebbe che farsi trapiantare due occhi diversi, come ha fatto Tom Cruise in Minority report per sfuggire al riconoscimento della fantascientifica agenzia di sicurezza Pre-crime.

Circuito venoso “Buon sangue non mente”, potrebbe essere il motto della nuova soluzione biometrica che legge le vene della mano. Collaudata con successo in Giappone, ora sbarca in Europa proposta da due colossi della tecnologia in partnership Siemens e Fujitsu. “Impossibile falsificare o camuffare il circuito venoso, che è sottopelle ed unico per ogni individuo, il nostro metodo è inaggirabile – sottolinea Andrea Biasiol, Head of competence center di Siemens – Il palmo è letto da uno scanner all'infrarosso senza contatto diretto – continua Biasiol – Tale precauzione igienica è importante nel caso degli ospedali o di strumenti utilizzati di frequente come le casse automatiche o varchi pubblici, vedi quelli aeroportuali, cioè dove un singolo sensore deve essere utilizzato da molte persone. Inoltre il sistema ha il pregio di essere passivo, assolutamente innocuo per la salute, e quindi non viene percepito invasivo da chi si deve far riconoscere a differenza di altri metodi simili in circolazione, come lo scanning del circuito venoso delle dita effettuato con raggi laser”. Il vantaggio reale consiste nel fatto che è semplice da utilizzare e da predisporre; è sufficiente collegare un apparecchio di 30 centimetri ad un terminale. Sebbene sia un sistema a “distorsione zero”, l'utilità del rilievo per usi di polizia è ancora lontana. Non essendoci una banca dati pregressa per ora è improbabile usare l'albero alveolare per identificare qualcuno confrontandolo con precedenti schedature. Spingendo in questa direzione, gli esperti Siemens propongono di iniziare a inserire nei fascicoli per i permessi di soggiorno oltre le impronte digitali altre informazioni biometriche, prime fra tutte quelle del circuito venoso.

Salvare la faccia Meno proficuo a tutt'oggi il riconoscimento facciale automatico. “È vero – spiegano gli esperti di fisionomia della polizia scientifica – che da una fotografia o da un video si può discriminare la geometria del volto, attuando sulle immagini le misurazioni antropometriche, quali la distanza tra gli occhi o dall'attaccatura dei capelli alla base del naso. Ma allo stato attuale i risultati non sono soddisfacenti. Ad esempio, se il rapinatore che entra in una banca è completamente camuffato o se le immagini video che lo riprendono non sono ad alta definizione o deformate da un'angolatura stretta, o il chirurgo estetico ha ritoccato molto bene il soggetto in questione, il rilievo dei dati ne viene falsato”. Certo è una strada che non va abbandonata considerando il fatto che in tutti i cartellini segnaletici dei pregiudicati compaiono fotografie “oggettive” che permetterebbero, una volta digitalizzate, di poter creare già una base di archivio informatico per le comparazioni. Il futuro, sostengono i ricercatori biometrici, consiste però nella tridimensionalità. Per ottenere misurazioni apprezzabili bisognerebbe poter sempre rilevare il volto con una rete di tre telecamere triangolate sul soggetto. Apparato complesso non d'immediata installazione. Ma a volte basta un dettaglio a parlare di noi più di tutto il resto. L'orecchio è come un biglietto da visita con tanto d'indirizzo, la sua conformazione è così singolare che spesso ha portato a incastrare l'autore di un reato o a salvare un innocente. Come è accaduto al palermitano Antonino Di Caccamo, arrestato 22 mesi fa, per l'incredibile somiglianza ad un bandito e recentemente scagionato grazie alle sue orecchie a sventola. Anche i difetti rendono unici. Lo confermano gli etologi che nella savana identificano i leoni dalle orecchie. Ne hanno fatto la loro specializzazione due criminologi olandesi, Innarelli e Cor Van der Lugt, massime autorità mondiali in campo di padiglioni auricolari, elici, lobi, prodighi di pubblicazioni e convegni. Qualcuno l'hanno convinto: i ricercatori del National training centre for scientific support to crime investigation, nel Regno Unito, sono a lavoro per creare un database di immagini di orecchie.

In odore di legalità Ciò che neanche le fantasie cinematografiche hanno mai concepito è l'identificazione attraverso l'odore. Eppure non siamo così lontani. Almeno a dare credito a un gruppo

di ricercatori, provenienti dalla Bristol University, University of Vienna e dall'Indiana University, che ha annunciato di aver scoperto un metodo che permette di analizzare le tracce di odore che ogni persona emana e lascia alle sue spalle. La "fragranza umana" (thermal plume), facilmente individuabile dai segugi anche a chilometri di distanza, è riconducibile alla combinazione di 44 elementi chimici secreti dal corpo. Le loro proporzioni – secondo i ricercatori – consentono di identificare univocamente ogni singolo individuo come un'impronta digitale. Gli scienziati sono riusciti a sviluppare una tecnica che facilita il "prelievo" dell'odore senza contaminazioni, e la sua analisi attraverso un "naso" capace di scinderne ogni componente. Alcune fra le applicazioni potenzialmente più interessanti sono nei settori che hanno a che fare con la biometria (passaporti, documenti, sistema di sicurezza) e l'identificazione (medicina legale, indagini di polizia). Vi è già, ad esempio, un progetto europeo per il miglioramento dei sistemi di riconoscimento degli esplosivi e degli agenti chimici pericolosi negli aeroporti. Un "naso elettronico" più sofisticato rispetto a quello già utilizzato in alcuni terminal del mondo. Qualche riserva va comunque mantenuta: "L'odore ci permette di comprendere il sesso di una persona, il suo stile di vita, se fuma, cosa ha mangiato la sera precedente e se è stressata. Si può dire molto di una persona attraverso i marcatori chimici presenti nel sudore. Ma raggiungere un livello di affidabilità tale da rendere questa operazione una prova per i tribunali è ancora una vera sfida", ha dichiarato Silvia Valussi, del Forensic science service britannico.

Per voce solaVi ricordate Hal 9000, il megacomputer di 2001 Odissea nello spazio, che riconosceva dalla voce i due astronauti permettendo così l'accesso ai suoi programmi? Era solo il 1968 e Stanley Kubrick aveva già anticipato quello che oggi è realtà. "La lettura della voce ha raggiunto standard elevatissimi ma ancora vi è molta strada da fare – a parlare è Tommaso Bove primo dirigente tecnico ingegnere della Polizia di Stato – Si usano come parametri di misurazione le cosiddette frequenze formanti e la frequenza fondamentale, cioè le concentrazioni di energia del parlato che si riscontrano principalmente in corrispondenza delle vocali. Pur essendo altamente identificativa, la voce può variare con l'età sia, ad esempio, per interventi parodontologici. Nei processi penali questo tipo di accertamento può essere considerato elemento probante, cioè tendente a rendere il riconoscimento del parlatore più o meno probabile di quanto non sia senza la produzione di questa prova. Invece, per ammettere l'ingresso ad un'area ristretta è un metodo sicuro al 100% perché il parlato della persona da identificare viene confrontato con l'insieme chiuso e verificato di voci autorizzate. Comunque non sono mancate ultimamente situazioni risolte grazie alle indagini foniche. A Cagliari gli investigatori della Dia avevano bisogno di sapere se tra le voci che comparivano in un'utenza telefonica vi fosse quella di un latitante, di cui si aveva una traccia registrata durante un processo. La conferma del sospetto è arrivata dai nostri tecnici fonici e ha permesso lo sviluppo positivo delle indagini". La metodologia attualmente utilizzata dal Servizio polizia scientifica della Dac, scaturisce dai risultati dei progetti di ricerca smart1 e smart2, co-finanziati dalla Ue e rientra in un più ampio progetto europeo per la standardizzazione delle metodiche secondo tecniche oggettive. Attualmente i ricercatori del polo Tuscolano di Roma stanno lavorando al progetto smart3 (che in rispetto delle direttive del ministro dell'Interno verrà completato entro la fine del 2007) volto a creare nuove banche dati sonore in alcuni Paesi membri della Comunità europea (Italia, paese leader, Francia, Belgio, Spagna e Slovacchia), in modo da applicare confronti linguistici e individuare criminali stranieri sempre più avvezzi ad agire in territori transfrontalieri. Inoltre si stanno sviluppando delle micro banche dati vocali che riguardano i vari bacini dialettali italiani.

Hollywood biometrica*Blade Runner* (1982), di Ridley Scott: controllo dell'iride per individuare i replicanti.*Mission impossible* (1996), di Brian De Palma: prelievo impronte palmari per accesso all'ascensore nel quartier generale della Cia. *Charlie's angels* (2000), di Joseph McGinty Nichol: riconoscimento dell'iride e delle impronte digitali per l'accesso alla sala pc della RedStar.*Mission impossible 2* (2000), di John Woo: lettura del volto, scansione della retina attraverso gli occhiali e riconoscimento vocale.*Ocean's eleven* (2001), di Steven Soderbergh: accesso al caveau del casino "Bellagio" con l'impronta digitale.*007 La morte può attendere* (2002), di Lee Tamahori: i protagonisti attraversano una porta controllata da un rilevatore della geometria della mano utilizzando la mano tagliata di Mr Kill.*Minority report* (2002), di Steven Spielberg: riconoscimento dell'iride usato dalla Pre-Crime per identificare i potenziali criminali (locandina in foto).*The Bourne Identity* (2002), di Doug Liman: riconoscimento geometria della mano per accedere nella banca svizzera.*Paycheck* (2003), di John Woo: riconoscimento del palmo e dei vasi sanguigni della mano.*X-Men 2* (2003), di Bryan Singer: Mystica accede all'ufficio di Stryker ingannando il riconoscimento della geometria della mano ed entra nel pc ingannando il riconoscimento vocale.*Io robot* (2004) di Alex Proyas: accesso al laboratorio con il riconoscimento del palmo della mano e vocale per accedere alla e-mail.*Cristiano Morabito*

01/11/2007