24 Maggio 2013 – Milano, Università Cattolica, ITSTTIME
Visual biometrics, privacy e asimmetrie informative: una prospettiva socio-tecnica.

Alberto Cammozzo: cammozzo.com, TagMeNot.info

Alcuni fatti tecnologici, combinati tra loro e visti in una prospettiva sociale ci permettono di apprezzare la crescente difficoltà di un cittadino nel controllare i propri dati visuali personali in modo equilibrato. Questi fatti sono: (1) l'impiego diffusissimo di tecniche biometriche non cooperative quali il riconoscimento facciale (*face recognition*) o dell'incedere (*gait recognition*) per motivi anche molto frivoli, che possono però portare alla re-identificazione di soggetti che si pensano anonimi. (2) Il diffondersi del *wearable computing*, quale gli "occhiali" del progetto Google Glass, che portano queste tecnologie ovunque. (3) Il diffondersi di motori di ricerca facciale, pubblici, privati e probabilmente anche segreti. (4) Il progressivo diffondersi di sistemi biometrici interoperabili, che possono riconoscere soggetti che si sono registrati precedentemente in altri sistemi. (5) La conseguente costruzione di banche dati biometriche immense soggette a possibili violazioni e alla conseguente diffusione di dati che possono portare a identificazione e riconoscimento.

Questi fatti tecnici si combinano in un contesto socio-tecnico in cui: (1) I social network combattono lo pseudonimato, legando identità online univoche congruenti con quelle biologiche. (2) Il "diritto" alla sorveglianza viene riconosciuto in modo asimmetrico dalle norme sociali, più che dalla legge. Infatti la sorveglianza "per motivi di sicurezza" (reali, apparenti e anche fittizi) viene accettata ed è ormai ubiquitaria, mentre la sorveglianza dal basso (o *sousveillance* [Mann, Fung, and Lo 2006; Mann, Nolan, and Wellman 2002]) viene mal tollerata in quanto non collegata a ragioni espresse, esplicite e socialmente condivise.

Questa duplice asimmetria, tecnologica e socio-tecnica, porta alla cancellazione dei contesti in cui un soggetto può agire in modo anonimo o pseudonimo, e apre scenari inquietanti. Da una parte l'insorgere di un totalitarismo biometrico in cui ciascuno è obbligato ad essere – sempre e solo – lo stesso *se stesso* che *tutti* conoscono. Questo "obbligo a dire" è quello che per Roland Barthes è la sigla deteriore del fascismo [Barthes 1977]. Da un'altra parte è possibile immaginare che accada un qualche grave incidente o scandalo riguardante dati biometrici per cui una massa di persone reagiranno in difesa della propria sfera privata, ridimensionando come minimo l'attuale entusiasmo acritico per le ICT. Ciò è accaduto in passato per altre tecnologie, e non a caso questo scenario è stato chiamato di "Privacy Chernobyl" [Gruteser and Grunwald 2004].

Sembrano pochi gli strumenti per evitare questi scenari agendo su un piano socio-tecnico o giuridico. Tra questi si vede: 1) I motori di ricerca facciali pubblicamente accessibili possono aumentare il livello di consapevolezza individuale sui dati biometrici visuali presenti online e favorire reazioni appropriate. 2) La protezione del contesto pubblico come sfera di anonimato, presupponendo un *opt-out* dal riconoscimento automatico e dalla re-identificazione. 3) Occorre esplorare una soluzione tecnica analoga ai sistemi noti come "Single Sign-On" che preveda un disaccoppiamento tra chi detiene i dati di autenticazione/identificazione e chi tratta altri dati personali (ad es. i social network). In questo modo chi ha i dati non sa a chi appartengono, chi conosce le identità non ha accesso ai dati.