Privacy e nuove tecnologie.
I nuovi diritti del cittadino
nella cosiddetta società dell'informazione

di Ferry Byte

(conferenza a cura di Tommaso Tozzi per il progetto "Arte, Media e Comunicazione", 1997)

Gli abitanti di questo mondo sono (a cominciare da quelli piu' privilegiati) sempre piu' connessi a sistemi digitali.
Se dobbiamo impegnarci affinche' tutte/i possono trarre vantaggio dalle nuove tecnologie digitali in termini di maggiori possibilita' comunicative ed informative abbiamo anche il diritto di sapere cosa comporta in termini di svantaggi un'evoluzione sociale di questo tipo.
Alcuni svantaggi possano essere individuati in perdita' di socialita", in aumento di nocivita' e nella diminuzione della propia ed altrui * privacy * .
In particolare, la perdita della propria quota personale di riservatezza e' un problema che investira' ben presto i cittadini della nuova societa' dell'informazione per tutta una serie di ragioni:
1) l'uso delle telecamere in ambiti pubblici ha raggiunto livelli molto preoccupanti in tutta Europa.
2) si affacciano nuovi tipi di tecnologia come quella denominata PAN che offre la possibilita' di scambio info fra data base locali usando come conduttore la pelle dei due portatori umani che vengon a contatto che pongono inevitabili questioni etiche;
3) le carte di credito evolveranno presto in Smart Cards, ovvero in carte d'identita' elettronica multiuso capaci di scambiare informazioni (dati del possessore incluso una foto con un nuovo sistema di compressione) con un ricetrasmettitore capace di interloquire con la carta anche tramite onde radio e quindi magari anche all'insaputa del dententore della carta;
4) portare con se' un telefonino e' come avere una microspia addosso: le antenne della Telecom tengonosotto controllo gli spostamenti di ogni singolo apparecchio nel senso che il log della chiamata del telefonino registra anche l'antenna che riceve la chiamata del telefonino e quindi del suo proprietario; a denunciare questa situazione e' il deputato dei comunisti unitari Martino Dorigo: in una interrogazione parlamentare Dorigo sostiene che "sarebbe tecnicamente dimostrato che ogni apparecchio telefonico portatile, cosiddetto cellulare, anche quando spento ma collegato all'apposita batteria di alimentazione, possa ssere utilizzato, da appositi e sofisticati strumenti, come microfono ambientale mobile, in grado di ascoltare e trasmettere". A sfruttare questa possibilita', secondo il parlamentare comunista, sarebbero i nostri servizi segreti che non solo "sarebbero gia' dotati delle sofisticate apparecchiature" necessarie, ma "avrebbero gia' ottenuto, da parte della Telecom, l'intera lista dei numeri e dei nominativi delle migliaia (in realta' sono milioni, ndr) di cittadini italiani titolari di utenze telefoniche mobili".
Nel'interrogazione il deputato cita inoltre l'inchiesta del giudice veneziano Casson su "una struttura occulta parallela, denominata 'SuperSip',

composta dei servizi stessi". Una struttura della cui esistenza parlo' per la prima volta, messo alle strette dalla Commissione parlamentare d'inchiesta sul caso Moro, il dirigente della Sip Francesco Aragona. Chiamato a rispondere della scarsa collaborazione fornita dall'azienda agli investigatori durante i giorni del sequestro (il capo della Digos Domenico Spinella presento'anche una denuncia penale), Aragona ammise l'esistenza di una struttura riservata chiamata Pro-srcs per accedere alla quale occorreva essere in possesso del Nos, il nulla osta sicurezza. Della possibilita' di utilizzare i telefoni cellulari come microspia, anche quando spenti, si sarebbero vantati recentemente gli investigatori veneti che hanno catturato il boss Felice Maniero dopo l'evasione dal carcere di Padova. (...)"
5) Rete. La rete (internet e le atre reti telematiche) offre numerosi strumenti (cookies, activ X, caselle elettroniche, agenti intelligenti, Java, motori di ricerca ecc.) di intrusione della riservatezza.

Se si sposano queste info tecniche con la storica attitudini degli organi militari e polizieschi italiani a * monitorare * tutto e tutti e' evidente come si debano configurare al piu' presto i nuovi diritti del 2000.

NEL DOMINIO DEL POSSIBILE, BISOGNA SEMPRE ESSERE IN GRADO DI POTER ESPLETARE
LE NOSTRE ATTIVITA' - ANCHE CIVICHE - SCEGLIENDO FRA UN SISTEMA DIGITALE ED
UNO ANALOGICO.
Ad esempio dovrei sempre pter scegliere fra pagare il pedaggio autostradale con gli anonimi spiccioli oppure con il comodo telepass che pero' registra in una banca dati i miei spostamenti.

BISOGNA SEMPRE SAPERE COSA POSSIAMO FARE E COSA COMPORTA ANCHE IN TERMINI DI
SALVAGUARDIA O PERDITA DELLA PROPRIA ED ALTRUI PRIVACY.
I fornitori di servizi digitali dovrebbero avere il dovere oltre al buon gusto di informare i propri utenti sulle capacita' monitorative dei propri servizi.

SEMPRE NEL DOMINIO DEL POSSIBILE, SE SCEGLIAMO DI RAPPORTARSI CO UN SISTEMA
DIGITALE DOBBIAMO AVERE LA POSSIBILITA' DI POTERSI RAPPORTARE IN * FORMA ANONIMA *
OD UTILIZZANDO TYECNICHE DI * CRITTOGRAFIA * CHE ABBASSANO IL GRADO DI IDENTITA'
E LEGGIBILITA' DEI MESSAGGI DI CORRISPONDENZA PRIVATA.

Questo perche', malgrado la * difesa dell'anonimato * in rete (intendendo in rete il rapportarsi a tecnologie di tipo digitale) pur essendo una strategia resistenziale (la riservatezza personale e' comunque difficile da difendere) puo' essere una questione di sopravvivenza
(perseguitati politici), ppure necessaria (sieropositivi, donne violentate, tossicodipendenti, omosessuali ed altre categorie di esseri umani che per svariati motivi hanno il legittimo desiderio di rapportarsi alla Rete senza essere identificate/i) e comunque e' un'opzione che in ogni caso mette al

riparo da essere schedate/i da servizi commerciali o di controllo.

D'altra parte la legittimita' dell'anonimato in rete e' stata ribadita negli USA addirittura dai giudici federali che si sono pronunciati recentemente contro il Communication Decency Act (le parole testuali, estratte dalla sentenza, sono le seguenti: "Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape").

E' COMUNQUE AUSPICABILE UNA LEGISLAZIONE CHE SE DA UN LATO LEGITTIMA ALLA
FONTE IL DIRITTO DI POTER SCEGLIERE SE E COME RAPPORTARSI A SISTEMI DIGITALI
DALL'ALTRO ASSICURA UN USO DEI DATI RACCOLTI TRMITE TECNOLOGIE DIGITALI IL
PIU' RISPETTOSO POSSIBILE DELLA PRIVACY DEI CITTADINI MA ANCHE DEL LEGITTIMO
DESIDERIO DI CONOSCENZA DEL SAPERE E DELL'INFORMAZIONE.
Non va quindi dimenticato che se da un lato abbiamo il diritto affinche' la nostra privacy sia difesa da intrusioni esterne abbiamo anche il diritto che l'informazione di tipo pubblico sia messa a disposizione dei cittadini in forma gratuita, libera ed in maniera tale da poter essere reperita e consultata attraverso le tecnologie attualmente piu' avanzate. A questo proposito va aperta una piccola parentesi per denunciare come gli
archivi elettronici (facilmente consultabili via Internet una volta trattati con specifici programmi) della legislazione vigente e non ed in particolare delle Gazzette Ufficiali sia venduto ad istituti privati e non messo a disposizione della cittadinanza in forma elettronica e facilmente consultabile in maniera tale (una volta istituiti punti di accesso gratuiti ed assistiti negli uffici della pubblica amministrazione aperti al pubblico) da on poter veramente tollerare l'ignoranza di fronte alla legge e non essere a tutt'oggi una pretesa rispetto al cittadino che si trova spaesato rispetto ad una mole enorme di informazione senza avere gli strumenti per elaborarla in tempi rapidi ed in maniera razionale ed efficace.
Liberare l'informazione dai recinti del controllo del mercato e del controllo puo' essere una buona strategia d'attacco da affiancare a quella resistenziale della difesa della privacy...

Alla luce di quanto detto fino ad ora e' importanteprendere conoscenza della legislazione passata e presente sopratutto in quei passi dove si pongono degli strumenti di * tutela della privacy * del cittadino (la l. 300 del '70 - statuto dei lavoratori - nega la possbilita' di monitorare il lavoratore con apparecchiatuyre di varo tipo e le recenti l. 675 e 676 pongono degli strumnti di tutela come quello della richiesta del consenso della persona monitorata) ma e' ancor piu' importante che l'utenza finale della Rete sia cosciente delle intrinseche capacita' di monitoraggo della rete stessa e sia quindi in grado di rapportarsi (qualora scelga di rapportarsi) ad essa in forma anonima o crittografata al fine di poter salvaguardare la proria ed altrui privacy e non delegando a nessuno (nemmeno

a uno stato garantista ammesso che l'Italia si possa definire cosi') questa
forma di tutela personale.

Ferry di SN
Key fingerprint = A5 F9 A5 D3 35 70 BF 25 25 90 C1 18 ED B8 AC 64

,::. http://www.dada.it/stranet/town/crights