ANONIMA RISORSA

PRIVAC(I) - Gennaio 1997, Rapporto di Strano Network su
PRIVACY E NUOVE TECNOLOGIE - aspetti politici, giuridici e pratici -

---

0) ASPETTI POLITICI. 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 propria ed altrui privacy. Questo documento dibatte di questo ultimo aspetto.

1) APPROCCIARSI A TECNOLOGIE DI TIPO DIGITALE SIGNIFICA PERDERE UNA PARTE DELLA PROPRIA PRIVACY. Di seguito alcuni, significativi esempi.

a) Telecamere. L'uso delle telecamere in ambiti pubblici ha raggiunto livelli molto preoccupanti in tutta Europa. Spicca l'UK dove un regista ha pensato bene di comprare le immagini raccolte da compagnie di sicurezza private e filmate davanti all'entrate di banche assicurazioni ed all'interno dei bagni di pub e locali pubblici per montarci un film. Si apprende da L'Unita' del 27.12.95 che "Diecimila nuove videocamere entreranno in funzione nelle strade, nelle piazze, nei mercati attraverso il Regno Unito nel quadro di un allarmante aumento della sorveglianza elettronica sui cittadini. Quest'ultima fase dell'operazione Cctv" (close-circuit television) va ad aggiungersi alle decine di migliaia di videocamere gia' attive e non risparmia neppure i quartieri piu' periferici o i piccoli villaggi. Non e' piu' possibile spostarsi in una citta' inglese senza finire su un piccolo schermo in qualche sala di monitoraggio. Nuove tecniche permettono di ingrandire le facce dei passanti, le targhe delle auto, di spostare l'obiettivo in tutte le direzioni ed ascoltare anche le voci e le conversazioni. Dietro all'enorme sviluppo della sorveglianza elettronica c'e' l'incoraggiamento del governo che ha stanziato cinque milioni di sterline per oltre cento organizzazioni interessate ad installare centrali di monitoraggio sui cittadini. Il governo e' convinto che si tratti del modo migliore per ridurre il dilagare della

criminalita'. (...)" Significativamente, lo stesso giorno ma l'inserto locale de L'Unita' nella cronaca di Prato riportava "(...) telecamere istallate ai bordi della Zona a Traffico Limitato, come gia' avviene a Bologna, serviranno a leggere i numeri di targa delle automobili in transito. Chi, sprovvisto di permesso, varchera' il limite nelle ore non consentite sara' cosi' multato anche in assenza di un agente. L'occhio elettronico sara' infatti capace di leggere il numero di targa e di inviarlo, presumibilmente, ad un elaboratore della centrale del traffico. Il cervellone sara' quindi in grado di sapere in tempo reale se l'automobilista appena passato e' in regola o meno con i permessi. (...)" Alla luce di questi progetti sarebbe da valutare da un punto di vista giuridico (e giudiziario...) come e se e' legittima una multa ratificata in assenza di un agente (anche perche' certe recenti sentenze sembrano affermare il contrario) e chi e' legittimato a piazzare telecamere in ambiti pubblici che riprendono l'attivita' di privati cittadini e se queste riprese non debbano essere considerate violazione della privacy ed anche raccolta senza consenso (vietata dalla recente legislazione) di dati personali. Anche in Italia dunque e' di moda sostituire l'occhio elettronico a personale di controllo; un esempio che ha fatto abbastanza discutere e' stato quello di Ferrara dove il consiglio provinciale ha proposto di installare al posto dei bidelli telecamere a circuito chiuso e microfoni all'Itc Monti, per vigilare gli studenti. L'uso delle telecamere da parte di organi di controllo e' una pratica oramai comune: basta leggere La Nazione del 28.08.95 per apprendere che il C.S.A. Leoncavallo di Milano e' costantemente monitorato dalle forze dell'ordine anche grazie a delle telecamere piazzate nei palazzi circostanti. Stessa sorte tocchera' qualche mese piu' tardi al C.S.A. Ex-Emerson di Firenze anche se in questo caso le forze dell'ordine hanno sempre negato di aver piazzato la micro-telecamera nascosta di fronte all'ingresso del csa in occasione di un incontro nazionale "antagonista". Ha gia' qualche anno una sperimentazione effettuata dalla polizia tedesca e che merita attenzione per capire eventuali applicazioni future. In una stazione ferroviaria sono state piazzate delle telecamere digitali in maniera tale da riprendere frontalmente i viaggiatori che scendevano dal treno. I ferma-immagine di queste telecamere vengono confrontate con un archivio digitale di immagini di volti digitalizzati ripresi di fronte di latitanti. Quando il confronto fra l'immagine ripresa del passeggero e quella del latitante supera un tot di riscontro veniva allarmato il locale posto di polizia ferroviaria. Per tornare alla nostra realta' "nazionale" riportiamo la proposta del maggio 1995 del sindacato di Polizia Sap che vorrebbe obbligare i frequentatori degli stadi a portare dei tesserini magnetici i quali servirebbero a registrare l'entrata di detti tifosi negli stadi e grazie a particolari telecamere ad alta definizione individuarli piu' facilmente durante incidenti sugli spalti.

b) P.A.N. In un articolo su Virtual di gennaio '97 viene illustrata la tecnologia PAN ovvero la possibilita' di scambio info fra data base locali usando come conduttore la pelle dei due portatori umani che vengono a contatto (od un congegno che collega il portatore della base dati con una periferica presente nei paraggi). PAN come Personal Area Network da utilizzare come trasmettitore dati della propria carta di credito o di altre basi di info personali. Potremo cosi' comunicare inconsciamente con negozi, mezzi di soccorso, altre persone ecc. con cui veniamo a contatto e con cui siamo configurati a comunicare.

c) Smart Cards. Smart in inglese significa intelligente. Le smart card sono tessere dotate di un microprocessore di gran uso nel regno Unito dove sta per essere adottata una carta d'identita' elettronica multiuso capace di scambiare informazioni (dati del possessore incluso una foto con un nuovo sistema di compressione) con un ricetrasmettitore. La nuova memoria Y1, messa a punto dalla Motorola in collaborazione con il governo britannico, puo' anche essere letta a distanza con un ricetrasmettitore. Il trasmettitore interrogatore di questa smart card puo' leggere una simile carta a una distanza di 100 metri sfruttando le onde da 2.4 Ghz; le carte emettono un segnale di ritorno a 125 Khz fino a un metro di distanza.

d) Telefoni cellulari. Pochi lo sanno: portare con se' un telefonino e' come avere una microspia addosso. Le antenne della Telecom tengono sotto 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 (basta che sia acceso, non occorre che sia in corso una telefonata, n.d.r.) ... e quindi del suo proprietario ... Ogni antenna copre un territorio circolare: il raggio varia da qualche km in campagna a 3-400 metri in citta' densamente popolate ed il log e' inoltre in grado di registrare l'intensita' di ricezione del segnale e quindi la distanza presunta del telefonino dall'antenna. Se a cio' si aggiunge la facilita' con cui i telefonini cellulari (anche di personaggi importanti compresi magistrati e poliziotti) vengono clonati ad opera di personaggi di vario tipo, il dato assume significati ancor piu' inquietanti. Riportiamo un episodio per tutti (ma ce ne sarebbero tanti...). Da Il Manifesto del 25.08.95: "...e' il magistrato che coordina le indagini su un vasto giro di clonazioni di telefoni cellulari, ma anche il suo telefonino ha subito la stessa sorte; la Telecom ha infatti accertato che in partenza dal numero del cellulare in dotazione al procuratore della repubblica presso la pretura circondariale di Terni, Massimo Guerrini, risultano numerose telefonate in Nigeria e nel Senegal; in precedenza erano

stati clonati anche i cellulari dei sindaci di Terni e di Orvieto, e del vescovo diocesano; clonato anche uno dei telefonini in dotazione alla procura e utilizzato, tra gli altri, dal magistrato "anti-tangenti" Carlo Maria Zampi; i cellulari presi di mira sono quelli abilitati a chiamate internazionali..."
Di usi e abusi dei telefonini cellulari continua a parlarci Il Manifesto di ven. 10.11.95 descrivendoli come "oltre tre milioni di microspie sparpagliate che senza alcuna autorizzazione da parte della magistratura registrano qualunque conversazione sospetta o interessante; 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 essere 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". "Le intercettazioni telefoniche, permesse dalla legge solo alla polizia giudiziaria previa autorizzazione del giudice - aggiunge Dorigo - se compiute come sopra descritto da Sismi e Sisde, rappresenterebbero una gravissima violazione della legge". Ma il parlamentare comunista, oltre che per gli 007, ne ha anche per l'azienda telefonica: "Tale vocazione della Telecom alla violazione del diritto di riservatezza dei cittadini utenti - a detta di Dorigo - e' confermata anche dal fatto che il Comitato parlamentare per i servizi ha recentemente appurato che fu la stessa Telecom a fornire illegittimamente a Craxi i famosi tabulati delle telefonate di Di Pietro".
Nell'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. (...)"

e) Schedature. Di schedature (di tipo anche politico) effettuate in Italia da parte di polizie, aziende (Fiat in testa), servizi e contro-servizi ce ne sono veramente di tutti i gusti; basta rileggersi la storia passata e recente di questo paese per sbizzarrirsi... oppure anche la legislazione specializzata in materia per scoprire, p.e., come il soggiorno in un hotel (o in un qualsiasi altra struttura ricettiva) comporta al ricettore l'obbligo di notificazione in questura anche con mezzi telematici in tempo reale dei dati degli ospiti.

f) Rete.
Cookies: Un cookie e' un file di testo che viene inviato dal server di un sito internet al browser che vi si collega. Il file rimane in memoria fino a quando il browser chiude la sessione, a questo punto il file viene scritto sul disco rigido del client. Le info contenute nel cookie riguardano le attivita' svolte dal client. Come tali info vengono recuperate dal server non e' molto chiaro...
Posta elettronica: avere un indirizzo di posta elettronica abbinato alla propria identita' puo' anche essere uno svantaggio. Ci sono programmi che automaticamente fanno vedere e catalogano quello che qualcuno ha scritto nei newsgroups ed e' un opzione standard per un service provider quella di vedere ed archiviare quali utenze hanno visitato tal pagine web. Come non ricordare poi l'iniziativa dei riformatori in una delle ultime tornate elettorali durante la quale chiesero di chiamando Agora' per richiedere un certificato elettronico e votare per il partito del cuore indicando il proprio indirizzo Internet(?!).
Agenti intelligenti e Java: altri strumenti per l'utente finale della Rete (intendendo per Rete servizi telematici Internet inclusa) che stanno prendendo campo come gli Agenti Intelligenti oppure Java significano sicuramente aumento della funzionalita' della Rete che diventa piu' interattiva e soprattutto piu' rispondente alle esigenze personali ma anche perdita di una parte di privacy. Questi "strumenti" sono infatti in grado di riconoscere l'utente e presentargli la Rete in base alle sue precedenti "navigazioni" oppure in base a determinate esigenze di ricerca dichiarate o dedotte dall'attivita' dell'utente identificato tramite l'e-mail o l'IP della macchina usata.

g) Varie.
Riconoscimento individuale: negli Usa stanno studiando un nuovo sistema di identificazione personale. La geografia osseo-vascolare del volto sara' realizzata grazie a una telecamera a raggi infrarossi. Il tracciato sara' poi inserito in un computer dal quale verra' richiamato con un codice personalizzato. Il nuovo sistema di identificazione verra' installato negli uffici governativi americani.

Esperimento di telecontrollo dei lavoratori del'Olivetti Research Laboratory di Cambridge (in Italia forse non si azzardano per l'esistenza dello Statuto dei Lavoratori?): attraverso l'Active Badge, un piccolo congegno dotato di microprocessore che trasmette ogni dieci secondi un segnale infrarosso univocamente identificabile. Con l'Active Badge e' possibile sapere la posizione del lavoratore che lo porta, posizione che e' interrogabile tramite Internet (WWW e Finger) in qualsiasi momento... Nello stesso ambiente sono disseminate telecamere e microfoni che registrano e trasmettono ogni movimento... Mercato (da "Data Manager", rivista di informatica professionale): Ecco di seguito l'elenco delle aziende impegnate nel settore di mercato italiano cosiddetto "SECURICOM". Alenia - Sistema di gestione di chiavi di sicurezza per i terminali del Lotto automatizzato; Terminale telematico sicuro; Soluzione Alenia VAS per la sicurezza nei servizi a valore aggiunto. Assex - Kryptovox, per la scomposizione del messaggio vocale in partenza e per la sua ricomposizione secondo un particolare sistema di codifica. Banksiel - Gianos; Antima (Antimafia), per la gestione delle normative in materia di antiriciclaggio. Digicom - Terminale biometrico FRT 02 per il riconoscimento dell'impronta digitale. ELC - Sigilli di massima sicurezza; contenitori, buste monouso, porta-etichette, dispositivi drive, consulenza in sfragistica e perizie tecniche su avvenute o meno manipolazioni di sigilli o contenitori di ogni tipo. Hahn Biometrix Italia - Scanner Startek Eng per verifica impronte; Sistema Dermalog AFIS (solo per Forze dell'ordine e Polizia); Terminali biometrici per controllo accessi; Livescanner per utilizzo biometrico e perizie balistiche. Mega Italia - Erogatori blindati di banconote, sistemi per il trattamento delle banconote e delle monete, veicolazione di sicurezza per il denaro, sacche con sigilli di sicurezza, secur-cash, sistema di gestione antirapina, distruggidocumenti da ufficio. Nest - Licenze, procedura per rilevare l'equippagiamento software e hardware di ogni PC. Olivetti - Procedure di login-password per identificazione e autorizzazione dell'utente, accesso al sistema condizionato dalla consistenza dei profili di sicurezza utente e posto di lavoro, desktop sicuro, protezione del bootstrap, lock della stazione di lavoro non presidiata. Programatic - Securid Cards per individuare univocamente gli utenti che accedono ad un calcolatore centrale tramite una password dinamica generata ogni 60 secondi, ADM, propagatore di password RACF multi-mainframe e multi-piattaforma. Target - Rilevatori sia passivi che attivi di microspie, analizzatori telefonici, telefoni e fax protetti crittograficamente, disturbatori telefonici, apparati in genere connessi ai servizi di bonifica e protezione delle comunicazioni. Tekno Packages - RM, pacchetti software per la compressione e crittografia dei dati, SAFE, sistema di controllo e gestione degli accessi in ambiente mainframe, sia batch che on-line. Video Applicazioni Industriali - Voice Security, famiglia di prodotti

hw e sw basati sul riconoscimento biometrico delle persone attraverso l'impronta vocale, carta ottica, carta di plastica formato ISO e tecnologia WORM, con capacita' di 2,5 MB.
- Controllo Dna: gia' vari Stati negli USA prelevano il Dna a detenuti e detenute e lo archiviano. La Difesa sta progettando di prelevarlo a tutto il personale militare in servizio, in riserva o ex militare. Per il 2001 avra' quattro milioni di campioni di Dna. Il computer ne puo' archiviare diciotto milioni. Il Dna di ogni persona sara' tenuto in archivio per settantacinque anni.
Dc - Digital Cash: verifica gli acquisti realizzati via Bancomat (industria canadese) o per posta elettronica. E' in grado di individuare le preferenze d'acquisto della persona e le gira a societa' commerciali che la riempiranno di offerte speciali mirate. Non ci dimentichiamo che l'intrusione di soggetti commerciali nella nostra privacy e' ancor piu' probabile e pressante del pericolo di essere oggetti di controllo di tipo "poliziesco"...

2) 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 poter 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. Questo tipo di diritto dovrebbe essere previsto anche nella nostra legislazione ma tuttora non e' stato mai ipotizzato in maniera strutturata.

3) 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.

4) SEMPRE NEL DOMINIO DEL POSSIBILE, SE SCEGLIAMO DI RAPPORTARSI CON UN SISTEMA DIGITALE DOBBIAMO AVERE LA POSSIBILITA' (nota bene che quando parliamo di possibilita' intendiamo sia da un punto di vista di diritto politico-sociale-giuridico che in termini di sapere tecnico) DI POTERSI RAPPORTARE IN FORMA ANONIMA (p.e. le carte di credito usate per telefonare dalle "cabine" ed acquistate senza rilascio di dichiarazione d'identita') OPPURE USANDO DETERMINATE TECNICHE (p.e. i remailers anonimi ed i sistemi di crittografia a chiave pubblica come il pgp usato in rete) CHE ABBASSANO IL GRADO DI IDENTITA' E LEGGIBILITA' DEI MESSAGGI DI CORRISPONDENZA PRIVATA.
Nello specifico degli anonymous remailer e per smentire la teoria che vuole le tecnologie digitali intrensicamente dalla parte dei "criminali" e'

necessario fare almeno due considerazioni:
a) e' il caso di questi giorni che proprio grazie alla pubblicizzazione in Internet di un proprio servizio a pagamento alcuni pedofili che offrivano bambini da seviziare (almeno cosi' ha detto il TG1) sono stati scoperti da un giornalista che li ha denunciati alla Polizia dopo una rapida ricerca-accettazione della offerta di servizio in rete. Questo episodio dimostra - se mai ne fosse necessario - che chi offre qualunque servizio pubblicamente in rete si espone sicuramente ad essere facilmente monitorato e rintracciato e per cui coloro (polizie ecc.) che hanno interesse a ricercare questi soggetti non dovrebbero che essere contenti che tali soggetti si rapportano alla rete...
b) gli anonynomous remailer servono principalmente a mandare dei contributi in rete in ambiti pubblici (mailing-list ecc.) o privati (a singole caselle postali) propri contributi personali senza voler apparire ma non consentono di poter risalire al mittente in nessun modo per cui, nello specifico, gli anonymous remailers possono essere usati da soggetti "in andata" e basta e quindi per comunicazioni unidirezionali e sicuramente non per instaurare scambi bi-direzionali di comunicazione fra chicchessia (criminali compresi). Quelli che infatti consentono comunicazioni bi-direzionali in anonimato conservano comunque il "collegamento" fra identita' vera e identita' anonima (per poter girare i messaggi) e quindi la loro affidabilita' e' direttamente proporzionale al sistema di gestione e al personale di gestione del remailer stesso. Bisogna inoltre considerare che in alcuni casi particolari conservare l'anonimato in Rete puo' essere una questione di sopravvivenza (perseguitati politici), oppure necessaria (sieropositivi, donne violentate, tossicodipendenti, omosessuali ed altre categorie di esseri umani che per svariati motivi hanno il legittimo desiderio di partecipare a discussioni in 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"). PER TUTTE QUESTE RAGIONI SIAMO FAVOREVOLI ALLA PROPOSTA DI INSTALLARE UN ANONYMOUS REMAILER ALL'INTERNO DEL PROGETTO ISOLE NELLA RETE.

5) 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 TRAMITE TECNOLOGIE DIGITALI IL PIU' RISPETTOSO POSSIBILE DELLA PRIVACY DEI CITTADINI MA ANCHE DEL LEGITTIMO DESIDERIO DI CONOSCENZA DEL SAPERE E DELL'INFORMAZIONE E RACCOLTA. 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 non 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. Analizziamo ora brevemente alcuni tratti della legislazione esistente in materia con lo scopo di fornire alcune coordinate a chi ha il coraggio di avventurarsi in questo oceano di norme...

Iniziamo dalle recenti L. 675 e 676 sul trattamento dei dati personali.
"Finalmente" sono uscite le due leggi sul trattamento dei dati personali con il supplemento ordinario n. 3 alla G.U. n. 5 del 3.1.97 che dovrebbero in qualche modo recepire i principi della Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati., pubblicata sulla Gazzetta Ufficiale delle Comunita'; Europee N. L 281 del 23/11/95.
Le due leggi italiane sono
1) Legge 31 dicembre 1996, n. 675 Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali
2) Legge 31 dicembre 1996, n. 676 Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali
che obbliga il Governo ad emanare nei prossimi 18 mesi decreti legislativi integranti della legislazione in materia. Dunque due dispositivi che ci avviamo a commentare pur non essendo esperti (ed anzi ci aspettiamo sempre aggiustamenti e suggerimenti dai veri esperti in materia ;-) ma semplici utenti interessati delle sue sorti digitali. Due dispositivi non sulla privacy e nuove tecnologie ma piu' specificatamente sul trattamento dei dati personali.

Prima di andare brevemente ad analizzarli e' importante ricordare come i successivi decreti legislativi e regolamenti saranno ancor piu' importanti di questi due primi passi perche' andranno a regolamentare nello specifico, sperando che crittografia e anonimato in rete possano rimanere due libere possibilita' di difesa della propria ed altrui privacy in Rete.

L. 675

Mentre leggendo l'art. 3 si presume che le varie agendine personali di vario tipo possiamo continuare a redigerle senza grossi patemi d'animo subito l'art. 4 ci ricorda come questa legge non si applica al trattamento di dati personali effettuata da autorita' giudiziarie e poliziesche :-(
Negli articoli successivi sono comunque stabilite delle forme di tutela delle persone oggetto di raccolta dei dati come la condizione primaria di avere il consenso dell'interessato - art.11 - (non considerando forse che a volte l'interessato puo' cedere il consenso perche' intimidito: lavoratore/datore_di_lavoro ecc.). Altre forme di tutela benche' parziali sono comunque da conoscere ed impararsi a memoria come la possibilita' di sapere l'esistenza di trattamenti di dati che ci possano riguardare (Art. 13) oppure sui limiti di diffusione di questi dati (art. 20). Abbastanza ambiguo l'art. 16 sulla cessazione del trattamento dei dati con relativa possibilita' di scambio dati che sembra legittimato fra titolari con finalita' analoghe (?!) e comunque abbastanza poco chiara in generale questa legge sulla possibilita' di scambio/vendita di banche dati, pratica molto in uso fra grandi aziende (una per tutte: la Telecom). Esclusi i consueti organi giudiziari, ispettivi, servizi segreti ecc. ecc. l'art. 22 mette al riparo dalla raccolta impropria di dati sensibili (sesso, religione, politica ecc.) tramite il doppio strumento di tutela del consenso dell'interessato e del parere favorevole del Garante con la limitata eccezione per attivita' giornalistica (art. 25).
Il Garante (capo VII) ha numerosi compiti di controllo in materia (in alcuni casi anche per procedimenti amministrativi o giudiziari - art. 42) e pone quindi il rilevante problema politico di chi sara' il Garante e come si apprestera' a lavorare... Sperem in benem...

L. 676

Detta alcuni principi che il governo deve seguire nell'emanazione entro i prossimi 18 mesi di uno o piu' decreti legislativi che dovranno integrare la regolamentazione in materia. Principi dettati da varie Raccomandazioni del Consiglio d'Europa (art. 1) - che possono pero' essere interpretate ovviamente dai legislatori nostrani in vari modi - oppure esplicitati nella legge stessa come nel punto l) Art. 1 in cui si dice di prevedere norme che favoriscano lo sviluppo dell'informatica giuridica e le modalita' di collegamento, per

l'autorita' giudiziaria e per l'autorita' di pubblica sicurezza, con le banche dati della pubblica amministrazione; oppure al punto n) stesso art. in cui si dice di stabilire le modalita' applicative della legislazione in materia di protezione dei dati personali ai servizi di comunicazione e di informazione offerti per via telematica, individuando i titolari del trattamento di dati inerenti i servizi accessibili al pubblico e la corrispondenza privata, nonche' i compiti del gestore anche in rapporto alle connessioni con reti sviluppate su base internazionale;

L. 121 / 1981 "NUOVO ORDINAMENTO DELL'AMMINISTRAZIONE DELLA PUBBLICA SICUREZZA"
Sul tema delle banche dati utilizzate dalle forze di polizia, la Legge 121 del 1/4/1981 (nuovo ordinamento dell'amministrazione della pubblica sicurezza) integrata dal testo del D.P.R. 3 maggio 1982, n. 378 (Regolamento concernente le procedure di raccolta, accesso, comunicazione, correzione, cancellazione ed integrazione dei dati e delle informazioni registrati negli archivi magnetici del centro di elaborazione dati di cui all'art. 8 della legge 1 aprile 1981, n. 121) agli artt. 6-10, disciplina l'uso e la segretezza dei dati personali dei singoli cittadini in possesso delle Forze dell'Ordine. La L. 15 novembre 1988, n. 486, detta disposizioni integrative di quelle contenute nella legge 121/81. Alcune parti di questa legge sono state modificate dalla 675 e 676.

LEX E CRYPTO. La legislazione (escluso alcune norme riguardanti il personale del Ministero degli affari esteri) che regola l'uso della crittografia in Italia riguarda principalmente l'impiego nella tutela del segreto di Stato, sia in campo civile che militare. L'ente preposto all'applicazione del controllo e' l'ANS (Autorita' Nazionale per la Sicurezza). La violazione delle norme e direttive dell'ANS e' repressa secondo quanto previsto dal codice penale. L'ANS valuta gli algoritmi, logiche, filosofie, hardware, emissioni e ne controlla la produzione e la distribuzione attraverso l'AND (Agenzia Nazionale di Distribuzione). L'import-export di detto materiale chiave e' regolato dalle leggi 185/90 e 222/92. L'uso della crittografia per altri impieghi privati o governativi non riferiti alla tutela del segreto di stato non e' ne' vietato ne' controllato in ambito telematico. In tema di regolamenti e' bene ricordare l'art. 130 del Codice Postale che vieta ai radioamatori la codificazione delle trasmissioni ed impone l'uso di alcune lingue nonche' l'art. 9 della Convenzione per i ponti radio dati in concessione che all'art. 9 richiede per le trasmissioni in cifra il deposito dei codici presso l'Amministrazione postale. La Telecom Italia non pone limiti all'impiego da parte degli utenti di sistemi di cifratura sia per fonia sia per trasmissione dati. L'unica restrizione potrebbe essere individuata nel collaudo delle apparecchiature per l'omologazione che sono

tenute ad adottare sistemi di cifratura che non incidano negativamente sulla funzionalita' della rete... E' probabile che anche in Italia si arrivi ben presto a voler regolamentare la crittografia in Rete dato che i G7 hanno recentemente sollecitato i Paesi aderenti a controllare la crittografia in Rete. L'UNICA NORMA ACCETTABILE IN MATERIA E' QUELLA CHE LEGITTIMA IL LIBERO USO DI SISTEMI A CRITTOGRAFIA A CHIAVE PUBBLICA, UNO DEI POCHI MEZZI A DISPOSIZIONE DELL'UTENTE FINALE PER PROTEGGERE LA PROPRIA CORRISPONDENZA PRIVATA DIGITALE. A questo proposito ci e' sembrato importante riportare la:

Posizione del CERT-IT a proposito della bozza di legge:
``Atti e documenti in forma elettronica''
Recentemente l'AIPA ha reso nota una bozza di proposta di legge dal titolo Atti e Documenti in Forma Elettronica. Il CERT-IT, il Computer Emergency Response Team Italiano, prende atto con soddisfazione che finalmente anche i legislatori italiani abbiano sentito la necessita` di affrontare alcuni dei problemi inerenti a una societa` informatizzata o quantomeno una societa` che aspira a diventarlo. Nella bozza di legge si riconosce l'utilita` e la validita`della documentazione elettronica in sostituzione di quella cartacea. Parallelamente si affronta il problema ben piu` vasto e delicato dell'uso della crittografia nella comunicazione informatica, con particolare riferimento alla crittografia a chiave pubblica. Infatti, l'articolo 5 della bozza recita:
``Ciascun utilizzatore di sistemi di codificazione con criptazione a chiavi asimmetriche deve provvedersi, nei modi e nei termini di cui alla presente legge ed al conseguente regolamento di attuazione, di due chiavi asimmetriche di criptazione, delle quali una da rendere pubblica e l'altra da conservare segreta a proprie cure e responsabilita`''. Il CERT-IT ha valutato la bozza in questione e sulla stessa esprime il seguente parere.
L'aspetto piu` critico dell'intera legge e` quello relativo al meccanismo di key escrow o key recovery proposto (Un sistema di key escrow o key recovery e` un sistema di crittazione che permette a persone autorizzate - responsabili d'azienda, agenti di polizia ecc.- e sotto particolari condizioni di poter decifrare messaggi criptati anche senza conoscerne direttamente la chiave di crittazione). Piu` precisamente, il sistema di key escrow proposto dal nostro legislatore e` alquanto primitivo e inefficace. Vengono proposti 3 enti di certificazione: il Consiglio Superiore delle Autorita` di Certificazione, l'Autorita` Amministrativa di Certificazione (per la P.A.) e l'Autorita` Notarile di Certificazione (per i privati), dipendenti entrambe dal primo. A loro volta, l'Autorita` Amministativa di Certificazione puo` delegare delle Autorita` Intermedie di Certificazione e l'Autorita` Notarile puo` delegare delle Autorita` Private di Certificazione. Questi enti sono autorizzati a

generare e conservare le chiavi segrete degli utenti. Probabilmente la suddetta struttura potrebbe essere snellita rifacendosi a strutture gia` esistenti nel mondo degli utenti Internet, ed e` discutibile che un privato cittadino debba rivolgersi ad un notaio per avere la propria coppia di chiavi, sostenendo le spese del caso. Ci preme sottolineare in questa fase che e` del tutto inaccettabile che gli enti di certificazione conoscano le chiavi segrete di tutti gli utenti italiani di Internet, e che in nessuna parte della bozza di legge viene minimamente fatto riferimento alla riservatezza delle chiavi segrete e agli accorgimenti che si intendono adottare per garantire la privacy del cittadino rispetto ad ogni forma di comunicazione, come sancito dall'art. 15 della costituzione italiana. E` vero che la bozza di legge rimanda tutti i dettagli tecnici ad un regolamento di attuazione. Allo stato attuale, dubitiamo pero` che tale regolamento possa essere realizzato rispettando il difficile compromesso tra la salvaguardia della privacy del cittadino e la possibilita` di intervento degli organi di controllo. Infatti, meccanismi di key escrow piu` sofisticati che verifichino i suddetti presupposti, basati ad esempio su agenzie di certificazione e key escrow distribuite che conservano solo una parte della chiave segreta, sono attualmente solo in fase di studio o disponibili come prototipi. A riscontro di quanto affermato, vale forse menzionare il fatto che il 4 Febbraio 1994 il governo degli Stati Uniti d'America annunciava l'adozione di una tecnologia di key escrow nota come Escrowed Encryption Standard (EES), che a tutt'oggi e` tutto fuorche' uno standard. Il 1 Ottobre 1996 il Vice Presidente degli Stati Uniti D'America in un comunicato ammetteva in sostanza il fallimento di questo standard e invitava l'industria americana allo sviluppo e all'individuazione di nuovi ed efficaci strumenti di key recovery con l'evidente obiettivo di lasciare alla comunita` Internet stessa la scelta dello standard. Con molta perspicacia, il Vice Presidente degli Stati Uniti ha realizzato che agli utenti Internet non possono essere imposti standard ma e` in genere la comunita` che decide gli standard de facto. Ci siano inoltre consentite le seguenti ulteriori considerazioni. Gli articoli attuativi della legge evidenziano una notevole carenza del legislatore sia rispetto alla comprensione effettiva del funzionamento del meccanismo di crittografia a chiave pubblica, sia rispetto al reale impatto che l'introduzione di un calcolatore potrebbe avere come elemento altamente innovativo in una struttura burocratica. Nella bozza in esame, il calcolatore viene percepito come un surrogato di carta e penna, il cui uso viene regolato con le stesse modalita` di quella carta e penna che esso dovrebbe sostituire. Si legga in proposito l'art. 21 della bozza in questione, che tratta dell'autenticazione. E' noto a tutti gli utilizzatori di sistemi di crittografia a chiave pubblica con procedura di certificazione annessa che questi sistemi garantiscono

intrinsecamente l'integrita` del messaggio, la sua autenticazione e la sua non repudiabilita`. Il nostro legislatore sembra invece ignorare completamente questi vantaggi. Infatti la procedura di autenticazione di cui all'art. 21 e` basata sulla verifica notarile tradizionale che svilisce e vanifica i procedimenti di certificazione automatica derivanti dall'uso di sistemi di crittografia a chiave pubblica. In conclusione, apprezziamo lo sforzo che il nostro legislatore ha realizzato ma riteniamo che l'attuale bozza contenga degli elementi negativi che la rendono dal nostro punto di vista improponibile e quindi inaccettabile. Auspichiamo pertanto che tutti i mezzi di informazione e le forze politiche si impegnino a migliorare la legge in questione, che riteniamo di estrema importanza per lo sviluppo del nostro paese. Riassumiamo brevemente i principali elementi negativi che abbiamo individuato nella bozza in questione.

1) Una corretta attuazione della legge richiederebbe l'esistenza di un buon meccanismo di key escrow. Tuttavia non ci risulta esistano attualmente, se non in fase sperimentale, efficaci strumenti di key escrow. Quello proposto dal legislatore (deposito della chiave segreta presso un Notaio o un altro ente certificatore) non fornisce le necessarie garanzie di privacy del cittadino, e inoltre comporta un costo per l'utente che non e` ancora possibile quantificare.

2) La legge non sfrutta le potenzialita` riguardanti la certificazione automatica insite nel meccanismo di crittografia a chiave pubblica che si vuole introdurre.

3) Il legislatore si dimostra insensibile rispetto all'efficace e soprattutto innovativo impatto che potrebbe avere l'introduzione di un calcolatore come strumento crittografico nella intricata burocrazia italiana.

Rimaniamo a disposizione di chiunque necessiti di ulteriori approfondimenti.

Marta Ferrari
University of Milano
Department of Computer Science
Via Comelico, 39 - 20135 Milan (Italy)

INTERCETTAZIONI DI CONVERSAZIONI.

Materia disciplinata dagli artt. 266-271 c.p.p. In particolare, l'art. 266 bis tratta di intercettazioni telematiche.

L'art. 266 c.p.p. disciplina i limiti di ammissibilita' delle intercettazioni di conversazioni. "L'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione e' consentita nei procedimenti relativi ai seguenti reati:

a) delitti non colposi per i quali e' prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni tenendo conto se si tratti di

reato consumato o tentato.
b) delitti contro la pubblica amministrazione per i quali e' prevista la pena della reclusione non inferiore nel massimo a cinque anni.
c) delitti relativi a sostanze stupefacenti o psicotrope.
d) delitti concernenti le armi o gli esplosivi.
e) delitti di contrabbando.
f) reati di ingiuria, minaccia, molestia o disturbo alle persone col mezzo del telefono (..)".
Per quanto attiene al procedimento l'art. 267 c.p.p. indica i presupposti e le forme del provvedimento giudiziario. Per procedere all'intercettazione telefonica il pubblico ministero deve richiedere l'autorizzazione al giudice per le indagini preliminari che la concede con decreto motivato solo quando vi siano gravi indizi di reato e l'intercettazione sia assolutamente indispensabile ai fini della prosecuzione delle indagini. Tuttavia, in casi di assoluta urgenza, nel fondato timore che dal ritardo potrebbe derivare un grave pregiudizio per le indagini, il pubblico ministero puo' disporre l'intercettazione direttamente , con decreto motivato che deve essere comunicato immediatamente e comunque non oltre le 24 ore al giudice per le indagini preliminari che decide sulla convalida sempre con decreto motivato entro le 48 ore. Se il giudice per le indagini preliminari non convalida l'intercettazione telefonica, la stessa deve essere immediatamente interrotta ed i risultati acquisiti fino a quel momento non possono essere utilizzati. La durata delle operazioni relative alle intercettazioni non puo' superare i 15 giorni, ma puo' essere prorogata con decreto motivato dal giudice per le indagini preliminari di 15 giorni in 15 giorni. Per quanto invece attiene all'esecuzione delle operazioni l'art. 268 c.p.p. dispone che le intercettazioni telefoniche devono essere trascritte in appositi verbali che devono essere trasmessi immediatamente insieme alle registrazioni al pubblico ministero. I risultati delle intercettazioni telefoniche entrano a far parte del fascicolo per il dibattimento. Ai sensi dell'art. 270 c.p.p. i risultati delle intercettazioni telefoniche non possono essere utilizzati in altri procedimenti a meno che risultino indispensabili per l'accertamento di delitti per i quali e' obbligatorio l'arresto in flagranza. L'intercettazione abusiva delle comunicazioni telefoniche e telegrafiche e' disciplinata dall'art. 632 bis-c.p. Questo fino agli anni '70. Grazie alla legislazione d'emergenza (A QUANDO L'ABOLIZIONE DI QUESTA MOSTRUOSITA' GIURIDICA?), le intercettazioni telefoniche sono da considerarsi "liberalizzate", visto che e' possibile che siano rivolte anche a chi non e' indiziato di reato (legge 22 maggio 1978, n. 191) e che siano estese in modo particolare ai sottoposti a misure di prevenzione (legge 13 settembre 1982, n. 646).

NELLA LEGISLAZIONE ITALIANA ESISTONO ALCUNI DISPOSITIVI CHE TUTELANO L'ANONIMATO IN RAPPORTO, PER ESEMPIO, A DETERMINATE CONDIZIONI DI SALUTE. Riportiamo a titolo di esempio un dispositivo su

ANONIMATO E MALATTIE INFETTIVE E SOCIALI

A) Malattie infettive e diffusive - Norme generali

D.M. 13 ottobre 1995 (1).

Disciplina per le rilevazioni epidemiologiche e statistiche dell'infezione da HIV.

IL MINISTRO DELLA SANITA'

Decreta:

1. 1. Le rilevazioni epidemiologiche e statistiche dei dati relativi all'infezione da HIV devono essere effettuate con modalita' idonee d'impedire l'individuazione dei soggetti ai quali i dati stessi si riferiscono.

(omissis)

2. Gli studi di prevalenza possono essere effettuati anche utilizzando modalita' che rendano anonimi i campioni da analizzare dopo l'esecuzione del prelievo di sangue, con conseguente impossibilita' di pervenire alla identificazione delle persone interessate.

3. I sistemi di sorveglianza delle nuove diagnosi di infezione da HIV non devono contenere informazioni nominative. E' tuttavia ammesso l'uso di codici attribuiti con modalita' tali da garantire comunque l'anonimato.

3. 1. Le regioni e le province autonome, sulla base dei criteri previsti dagli articoli 1 e 2, disciplinano il funzionamento dei sistemi di sorveglianza dell'infezione da HIV.

2. L'Istituto superiore di sanita' verifica annualmente l'andamento dell'infezione da HIV, e definisce protocolli operativi per migliorare il funzionamento dei sistemi di sorveglianza.

3. Il presente decreto sara' trasmesso alla Corte dei conti per la registrazione e sara' pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

(omissis)

(1) Pubblicato nella Gazz. Uff. 2 maggio 1996, n. 101.

- MONITORAGGIO DELL'ATTIVITA' DEI LAVORATORI

La principale e piu' articolata fonte normativa sull'argomento e' costituita, in Italia, dalla Legge n. 300/70 lo "Statuto dei lavoratori". Il primo comma dell'art. 4 vieta "l'uso di impianti audiovisivi e di altre apparecchiature per finalita' di controllo a distanza dell'attivita' dei lavoratori", e dispone, nel comma successivo, che "gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive, ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilita' di

controllo a distanza dell'attivita' dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. Tutela completata dall'art. 6 che prevedendo la possibilita' di controlli sui lavoratori al termine del turno di lavoro purche' attuati in forme e con modalita' tali da rispettare la "riservatezza" dei medesimi. Ancora l'art. 8 proibisce al datore di lavoro di assumere informazioni, attraverso attivita' d'indagine, circa le opinioni politiche religiose o sindacali del lavoratore e circa altri fatti "non rilevanti ai fini della valutazione dell'attitudine professionale; tale divieto si estende sino ad inibire al datore di lavoro la possibilita' di "schedare" il lavoratore in "banche dati" o di controllarne il tempo effettivo di lavoro su computer attraverso l'uso di codici particolari di accesso (Pretore del Lavoro di Milano sentenza del 5 dicembre 1984). In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalita' per l'uso di tali impianti". L'art. 38 della stessa legge, infine, stabilisce che la violazione dell'art. 4 e' punita con l'ammenda o con l'arresto (cumulabili nei casi piu' gravi). In questo contesto la sopracitata sentenza del Pretore di Milano del 5 dicembre 1984 ha ritenuto illecito l'utilizzo di un programma per elaboratore elettronico che permettesse, mediante un rapporto settimanale su tabulato, il controllo analitico dell'attivita' lavorativa del personale addetto al terminale. La Legge 135/1990, all'art. 6, fa divieto al datore di lavoro di indagare lo stato di sieropositivita' dei dipendenti o di persone da assumere. Cio' non e' stato tuttavia sufficiente ad impedire che con l'art. 15 del d.l. 4 ottobre 1990, n. 276, in materia di assunzione, reclutamento ed organici delle forze di polizia, venisse prescritto, per il personale delle forze armate, di polizia e di vigili del fuoco, "l'accertamento dell'assenza di sieropositivita' all'infezione da HIV per la verifica dell'idoneita' all'espletamento dei servizi che comportano rischi per la sicurezza, l'incolumita' e la salute dei terzi". Dopo accesi dibattiti in sede di conversione, la successiva legge 30 novembre 1990, n. 359, ha riformulato il disposto normativo armonizzandolo con i principi della legge n. 135/1990: e' stato cosi' sancito che gli accertamenti possono compiersi solo con il consenso dell'interessato, vietando, nel contempo, qualsiasi provvedimento sanzionatorio a carico di chi rifiuti di sottoporsi al test e proibendo qualsiasi provvedimento sfavorevole nei confronti di chi risulti invece sieropositivo. In questi ultimi due casi pero' il soggetto potra' essere escluso da particolari servizi. Segnaliamo, infine, la direttiva CEE del 29 maggio 1990 relativa "alle prescrizioni minime in materia di sicurezza e salute per le attivita' lavorative svolte su attrezzature munite di videoterminali" che introduce il principio secondo cui "nessun dispositivo

di controllo quantitativo o qualitativo puo' essere utilizzato ad insaputa
dei lavoratori" (par. 3).

ALLEGATI) Avremmo potuto allegare a questo documento un'infinita' di documenti
tecnici e giuridici. Preferiamo indicare due indirizzi telematici
www.ecn.org/crypto
www.dada.it/stranet/town/crights
ovvero gli unici due siti Internet in cui vi e' un approfondimento ed un
aggiornamento in italiano dei temi sviluppati nel presente documento.

gruppo di lavoro sulla comunicazione sTRANOnETWORK
strano.network@vtt.dada.it