

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Internet e privacy

Poullet, Yves

Published in:

Innovazioni tecnologiche e privacy

Publication date:

2005

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Poullet, Y 2005, Internet e privacy: considerazioni initiali. in *Innovazioni tecnologiche e privacy: garante per la protezione dei dati personali*. Istituto poligrafico, Rome, pp. 147-165.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Innovazioni tecnologiche e privacy

CONTRIBUTI

SVILUPPO ECONOMICO
E PROGRESSO CIVILE

A cura di Gaetano Rasi



www.garanteprivacy.it



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Stefano Rodotà, Presidente
Giuseppe Santaniello, Vice Presidente
Gaetano Rasi, Componente
Mauro Paissan, Componente

Giovanni Buttarelli, Segretario generale

Piazza di Monte Citorio, 121
00186 Roma
www.garanteprivacy.it
www.dataprotection.org

Si ringraziano quanti nella struttura del Garante hanno, per le rispettive competenze, contribuito alla pubblicazione di questo volume

G.R.



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Innovazioni tecnologiche e privacy

**SVILUPPO ECONOMICO
E PROGRESSO CIVILE**

A cura di Gaetano Rasi



www.garanteprivacy.it

Indice

Perchè questo volume	3
-----------------------------	----------

Introduzione

Progresso tecnologico e sviluppo civile: la tutela dei dati personali	7
<i>di Gaetano Rasi</i>	

Apertura dei lavori

Laicizzare il rapporto fra innovazione e società	15
<i>di Stefano Rodotà</i>	

Sessione I - Interventi Protezione dei dati e sviluppo tecnologico

Presieduta da Giuseppe Santaniello

Tipologia delle innovazioni tecnologiche e protezione dei dati personali	23
<i>di Giuseppe Santaniello</i>	

Sicurezza e privacy nelle comunicazioni pervasive	28
<i>di Maurizio Dècina</i>	

Sicurezza informatica e privacy: fondamentalmente un problema di uomini	35
<i>di Danilo Bruschi</i>	

L'era dell'<i>ubiquitous computing</i>	46
<i>di Luigi V. Mancini</i>	

Le tecniche Rfid	55
-------------------------	-----------

Rfid technology - new challenges to privacy	75
<i>di Alexander Dix</i>	

Recenti applicazioni biometriche	84
<i>di Mario Savastano</i>	

Tecniche biometriche nelle pubbliche amministrazioni	89
<i>di Claudio Manganelli</i>	

Reti telematiche e minori: l'esperienza nella scuola	94
<i>di Alessandro Musumeci</i>	

Indice

Sessione I - Tavola Rotonda Tutela della persona ed efficienza socio-economica

Coordinata da Franco Carlini

Dibattito 119

1. Gaetano Rasi
2. Francesco Beraldi
3. Domenico Campisi
4. Stefano Quintarelli

Sessione II - Interventi Nuove tecnologie e società dell'informazione

Presieduta da Mauro Paissan

Sicurezza e transnazionalità 137 *di Mauro Paissan*

Quale privacy nella società tecnologica 140 *di Giulio Carducci*

Internet e privacy: considerazioni iniziali 147

Internet and privacy: Some initial thoughts 157 *di Yves Pouillet*

Privacy e sicurezza in ambito *wireless* 166 *di Franco Vatalaro*

Le reti wi-fi geografiche 176 *di Dario Zenobio*

Sessione II - Tavola Rotonda Le garanzie nelle comunicazioni

Coordinata da Alessandro Cecchi Paone

Dibattito 183

1. Maurizio Gasparri
2. Silvio Traversa
3. David Banisar
4. Guido Salerno

Indice

Sessione III - Interventi Innovazioni tecnologiche e nuovi diritti

Presieduta da Gaetano Rasi

Innovazione e progresso civile 205
di Gaetano Rasi

E-Government e diritti della personalità 207
di Paolo Vigevaro

**Il ruolo dell'impresa
per una innovazione sostenibile** 220
di Roberto Galimberti

Governare l'innovazione 232
di Giovanni Buttarelli

Sessione III – Tavola Rotonda Quale futuro per la privacy

Coordinata da Carlo Massarini

Dibattito 243

1. Lucio Stanca
2. Carlo Formenti
3. Francesco Chirichigno
4. Stefano Rodotà

Conclusioni

La rincorsa tra regole e tecnologia 267
di Carlo Rubbia

Perché questo volume

In questo volume sono raccolti i contributi di studiosi ed esperti intervenuti al Convegno *Innovazioni tecnologiche e privacy* che si è svolto nel giugno del 2004 a Roma, presso la sala conferenze del Garante per la protezione dei dati personali.

Il persistente, ampio dibattito sui rapporti tra il progresso scientifico/tecnologico e la tutela dei dati personali abbisognava di un momento nel quale si fosse “fatto il punto” sulla problematica, al fine di evitare l’incaglio su una contrapposizione innaturale, ma che tuttavia richiedeva preliminarmente l’esposizione di numerose – pur esistenti e spesso valide – posizioni antagoniste.

Riteniamo che il Convegno abbia raggiunto lo scopo e che le relazioni e i dibattiti costituiscano un materiale utile per il successivo svolgersi del rapporto tecnologia-privacy non più come contrasto, ma come equilibrio fra valori e bilanciamento fra interessi al fine dello sviluppo della persona umana.

Il volume è ripartito nelle tre sezioni nelle quali si è articolato il Convegno:

- I Protezione dei dati e sviluppo tecnologico. Tutela della persona ed efficienza socioeconomica;
- II Nuove tecnologie e società dell’informazione. Le garanzie nelle Telecomunicazioni;
- III Innovazioni tecnologiche e nuovi diritti. Quale futuro per la privacy.



Introduzione

**PROGRESSO TECNOLOGICO
E SVILUPPO CIVILE:
LA TUTELA DEI DATI PERSONALI**

GAETANO RASI

INTRODUZIONE

Progresso tecnologico e sviluppo civile: la tutela dei dati personali

Gaetano Rasi⁽¹⁾

Sommario: 1. Innovazione tecnologica ed aggiornamento normativo; 2. Il grado di tutela dei dati come misurazione del progresso civile; 3. La tecnologia “virtuosa”

1. Innovazione tecnologica ed aggiornamento normativo

Ho sempre ritenuto non rispondente al vero la contrapposizione della innovazione tecnologica alla tutela dei dati personali, così come è equivoca la contrapposizione fra la sicurezza dell'individuo e la protezione della sua libertà e riservatezza.

Vi può essere, infatti, un rapporto di bilanciamento fra valori ed interessi diversi nelle situazioni concrete in quanto, se è evidente che la prima esigenza dell'individuo è quella di essere ... in vita ed esserlo integro nel fisico e libero nell'esplicarsi (la sicurezza), è pure evidente che il progresso scientifico, tecnologico e produttivo, soprattutto nelle tematiche della elaborazione delle informazioni e della comunicazione dei dati (Ict), non possa prescindere dalle norme che garantiscono la libertà, l'identità e la riservatezza del singolo (la privacy).

D'altra parte gli indirizzi legislativi che si concretizzano nelle norme sulla tutela dei dati personali non nascono nel chiuso delle biblioteche universitarie, ma vengono espresse anzitutto dalle esigenze maturate dagli individui che vivono nelle società civili. La c.d. “coscienza collettiva” - che si esplica nei dibattiti sui mass media, negli approfondimenti scientifici e nelle discussioni parlamentari - non è una nebulosa astratta, bensì è il risultato concreto dell'avanzare delle consapevolezze razionali e morali degli uomini.

Le moderne società avanzate, nei cui ordinamenti giuridici è stato introdotto il principio della garanzia che l'identità virtuale elettronica corrisponda alla identità reale psicofisica, si distinguono anche per questo dalle società ancora arretrate per le quali si auspicano adeguati solleciti passi verso lo sviluppo per una migliore convivenza.

(1) Componente Garante per la protezione dei dati personali - Italia

Proprio in base a queste considerazioni, il Collegio del Garante – Stefano Rodotà, Giuseppe Santaniello, Mauro Paissan ed il sottoscritto – ha voluto organizzare un dibattito a carattere internazionale sul rapporto tra innovazione tecnologica e privacy e da ciò fare il punto della problematica, senza naturalmente aver l'intenzione di volerla esaurire.

Infatti, l'intensa dinamica delle applicazioni tecnologiche e la continua presa di coscienza individuale e collettiva dei diritti e dei doveri non consentono alcuna cristallizzazione normativa. In base a questa constatazione, il nuovo codice in materia di protezione dei dati personali (d.lg. 196/2003) entrato in vigore il 1° gennaio 2004 – oltre a raccogliere in un organico testo unico la ormai copiosa materia legislativa esistente – ha come caratteristica fondamentale quella di costituire una cornice normativa di principi e di indirizzi, lasciando la regolamentazione concreta e specifica delle novità tecnologiche e applicative ai *provvedimenti generali* dell'Autorità garante impegnata in un costante monitoraggio e in un adeguato, tempestivo aggiornamento della disciplina di settori particolari.

Del pari la nuova legislazione prevede l'emanazione dei codici deontologici di autoregolamentazione delle singole categorie professionali, imprenditoriali e degli enti pubblici – promossi dal Garante, ma elaborati dagli interessati pur con l'ausilio dello stesso Garante – al fine di affiancare alla normativa autoritativa una disciplina partecipata in materia di tutela dei dati personali.

In tal maniera il codice generale, i codici di autoregolamentazione e i provvedimenti generali costituiscono un corpus normativo articolato, organico e, soprattutto, aggiornato e puntuale.

Il progresso tecnologico si va così coniugando con l'ampliamento e l'approfondimento di una più sostanziale rappresentatività democratica.

2. Il grado di tutela dei dati come misurazione del progresso civile

Da poco più di un decennio le misurazioni dello sviluppo economico vengono integrate in un indice dello sviluppo umano (Hdi o human development index) promosso dalle Nazioni Unite.

Si tratta di un indicatore sintetico che, combinando insieme i dati del prodotto interno lordo pro-capite, il livello di istruzione e la durata della vita, si è posto l'obiettivo di spostare l'enfasi delle misure dello sviluppo da un concetto di benessere economico, basato su una mera disponibilità di beni, ad uno che comprenda anche una valutazione della vita nella sua interezza. E già ora si pensa di ampliare i contenuti del *benessere* includendovi i dati delle *qualità*, oltre che delle *quantità*, alimentari disponibili nel tempo e nello spazio, della sanità fisica e della

riduzione del dolore, del grado di accesso alle conoscenze dell'arte, della musica, del paesaggio, ed altro ancora!

Questo indirizzo si combina con il concetto di sviluppo sostenibile che fa riferimento non solo alla crescita economica che soddisfa i bisogni delle generazioni presenti, ma che non comprometta la possibilità – per le generazioni future – di vivere ad un livello non inferiore a quello precedente.

I due elementi in sostanza confluiscono nel concetto di sviluppo civile del quale è protagonista la persona umana che tende a migliorare continuamente le proprie condizioni in una valutazione che va oltre l'egoismo del presente.

Preoccuparsi del bene futuro significa assumere un atteggiamento altruistico – come singoli e come collettività – che è della stessa natura del rispetto della persona umana, della sua libertà, della sua identità, della sua vita intima.

Non è certo il caso di insistere nel constatare come si passi, nel valutare il progresso umano, dai modelli classici a quelli keynesiani, da quelli neoclassici a quelli shumpeteriani, per considerare alla fine il passaggio da una crescita quantitativa ad una esigenza di distribuzione diffusa ed equa dei beni, per giungere ad un concetto di *crescita qualitativa* in cui si sostanzia il nuovo concetto di sviluppo civile.

In questa dinamica il passaggio dalla tecnica alla tecnologia, ossia dal mero impiego manuale e meccanico degli strumenti di produzione, alle infinite combinazioni di tali strumenti con l'elettronica, rese possibili dalle conoscenze scientifiche applicate per la produzione di merci e servizi, ha consentito il passaggio, appunto, dalla sola disponibilità quantitativa dei beni al loro impiego, oltre che liberatorio dai bisogni primordiali, anche capace di potenziare la libertà e la personalità dei singoli.

La tutela dei dati personali si pone in questa fase evolutiva come esigenza consapevole dell'uomo contemporaneo immerso nella dinamica della tecnologia pervasiva e, nel medesimo tempo, come maturazione legislativa ed autoregolamentativa, ossia impositiva e partecipazionista, dei moderni ordinamenti giuridici.

3. La tecnologia “virtuosa”

Si perpetua così quel fenomeno storico per cui nella vita dei popoli e dei singoli le invenzioni scientifiche, le loro applicazioni e le innovazioni di processo e di prodotto – anche nelle organizzazioni strutturali ed infrastrutturali – se da un lato rompono gli equilibri precedenti, dall'altro ne ricompongono altri a livello superiore.

Non si vuole, naturalmente, esprimere una visione irenica del processo storico, tuttavia si può realisticamente constatare che nel medio-lungo periodo ciò che si è perduto nel mutamento lo si è riconquistato, poi, con una maggiore consapevolezza morale e razionale e con un superiore vantaggio generale nelle fasi successive.

Non è certamente banale affermare che l'uomo resta un impasto di buono e di cattivo, ma la coscienza civile sempre più diffusa, anche se non sempre ascoltata e praticata, rende tutti più avveduti di ciò che è progresso e ciò che invece può rappresentare quel ritorno alla barbarie che pur talvolta si compie.

Pertanto la progrediente consapevolezza civile, come ha insegnato a ricomporre gli equilibri della vita ad un livello superiore, così sa anche individuare ciò che dalle innovazioni tecnologiche può potenziare l'uomo e ciò che invece può comprometterne l'essenza.

Qui sta l'eterno rovello umano della continua individuazione dei diritti e dei doveri e del loro bilanciamento.

Tra le innovazioni tecnologiche che caratterizzano l'attuale fase della civiltà umana vi sono anzitutto quelle che riguardano le elaborazioni delle informazioni, le reti di comunicazione, le memorie elettroniche, i sistemi di rilevamento dei dati, del loro uso diretto ed in combinazione con le alte capacità della produzione industriale, della distribuzione commerciale, dei trasporti, delle indagini di mercato. E ancora le banche-dati delle reti che gestiscono la sicurezza, la sanità, la ricerca, l'istruzione, insomma tutti quegli aspetti dai quali si incrementa l'attuale progresso, diffuso e moltiplicativo.

L'uomo può essere menomato nella sua identità e nella sua dignità da un uso di dati che possono falsificare la sua personalità o da informazioni e sollecitazioni che compromettono la sua libertà di scelta.

In tale processo il concetto di riservatezza acquista un significato che va oltre la protezione dell'intimità psicologica e fisica per acquisire il significato più completo di tutela dell'autentico volere dei singoli nell'esprimere il proprio pensiero, le proprie preferenze, le proprie scelte. Insomma, di determinare la propria qualità della vita.

Etica ed economia confluiscono. L'uomo – in quanto protagonista nella nuova società – intende deliberatamente esprimere esigenze che vanno oltre quelle del mero consumatore di beni, perché effettua scelte che tengono presenti quegli elementi immateriali che sono l'esercizio della sua libertà e l'esplicazione della sua dignità. Perciò, nell'odierno modello interpretativo dell'agire umano, non è più sufficiente il riferimento al solo calcolo della convenienza, immediata e circoscritta, dei vecchi principi della scienza economica.

Come è noto, una misura per valutare lo sviluppo economico è quella di confrontare tra di loro, in progressione temporale, i tassi dei vari periodi di crescita del PIL. Sennonché, questa impostazione viene sempre più contestata anche da coloro che considerano misurabile esclusivamente la crescita economica.

La ragione di questa insoddisfazione valutativa sta nel fatto che il confronto dei tassi di crescita da periodo a periodo considera positive ed esaustive soltanto le variazioni in più delle *quantità* di beni e servizi prodotti. Già da tempo ciò non è più

ritenuto sufficiente. Le variazioni positive e crescenti sono monche se non tengono conto, nel confronto, della comparsa di nuovi prodotti e i perfezionamenti dei vecchi con i quali si soddisfano di più e meglio i tradizionali bisogni umani e le nuove esigenze dei singoli. È questo il portato della innovazione tecnologica immessa nelle attività produttive. Un primo passo verso una valutazione globale dello sviluppo è stato compiuto, appunto, misurando il grado di innovazione tecnologica introdotto nelle merci e servizi,

Nel caso degli Stati Uniti le stime storiche ufficiali del Pil reale – a prezzi del 2000 – per lavoratore, avevano indicato che tale PIL era aumentato di quasi 3 volte tra il 1890 ed il 2000 (da 13.700 a 65.000 dollari Usa a prezzi 2000); ma se si correggono le stime ufficiali per tener conto - sia pur con le approssimazioni del caso - del miglioramento qualitativo dei beni dovuto alle innovazioni tecnologiche, si ottiene un aumento di ben 14 volte: da 4.600 a 65.000 dollari (B.J. De-Long, 2000).

Tuttavia anche questo aspetto è ormai considerato incapace di valutare lo sviluppo umano in quanto non tiene conto delle esigenze riguardanti il progresso civile legato alle ulteriori consapevolezze maturate in aggiunta al progresso tecnologico.

In altre parole, mentre l'accento in precedenza veniva rivolto più alla *quantità* in sede produttiva, ora l'accento viene spostato alla *qualità* in sede distributiva, ossia all'appagamento dei singoli destinatari del mercato: consumatori, fruitori, utilizzatori. Si tratta del passaggio ad un maggior peso della domanda rispetto all'offerta e da ciò a quanto può essere misurato dall'indice sintetico dello sviluppo umano promosso nel 1990 dalle Nazioni Unite.

Questo ragionamento ci porta pertanto a considerare che se si ingloba nei beni prodotti anche quell'elemento di qualità che è costituito - insieme con l'avanzamento tecnologico - dal rispetto del cittadino nel trattamento dei suoi dati personali (quale per esempio quello riferito al mercato: pubblicità, promozione, vendita-acquisto, assistenza post-vendita, fidelizzazione,) appare evidente come il valore del prodotto lordo di una determinata società può assumere dimensioni, anche economicamente misurabili, molto superiori.

Oggi, il rispetto del dato personale nella società tecnologicamente progredita e più consapevole, non può essere affrontato soltanto dal punto di vista del valore intrinseco della merce prodotta. Il valore di scambio risulta superiore perché soddisfa, su un piano di maggior rispetto, il cittadino come individuo e come persona.

Il soddisfacimento personale richiesto dal cittadino-consumatore, deve trovare garanzie anzitutto nella legislazione costituzionalmente fondata, nelle determinazioni della Pubblica Autorità e in quelle derivanti dalla autodisciplina degli operatori.

In conclusione, si potrebbe dire che la tecnologia "virtuosa" è quella che, potenziandone le capacità, rispetta la personalità di ciascuno.



Apertura dei lavori

**LAICIZZARE IL RAPPORTO
FRA INNOVAZIONE E SOCIETÀ**

STEFANO RODOTÀ

Apertura dei lavori

Laicizzare il rapporto fra innovazione e società

Stefano Rodotà⁽¹⁾

Voglio ringraziare tutti gli intervenuti, e i relatori in particolare, che con grande generosità hanno accettato di dare il loro contributo a questa discussione. Questo convegno ha la sua origine in una frase di Gaetano Rasi e il suo fondamento in una sorta di riflessione che abbiamo fatto sul nostro lavoro quotidiano, che fa del Garante un osservatorio privilegiato sul modo in cui l'innovazione tecnologica penetra nella società, nelle materie e nei settori e più diversi.

Tutto questo ci consente non soltanto di misurare il grado di sensibilità sociale all'innovazione nei diversi settori, perché registriamo le reazioni di cittadini, amministrazioni, imprese. Ci permette di fare anche un'altra operazione, che chiamerei di "relativizzazione della tecnologia". La tecnologia si presenta non voglio dire con una pretesa egemonica e totalitaria, ma con tutta la forza di chi ha consapevolezza di essere la forza trainante dell'organizzazione sociale. E tuttavia, quando analizziamo le tecnologie e passiamo dal discorso generale sulla tecnologia alle diverse applicazioni tecnologiche, ci accorgiamo immediatamente della diversità con la quale le singole tecnologie devono poi essere considerate.

Considerando un caso che riguarda la vita quotidiana, la videosorveglianza, ci accorgiamo subito che essa assume significati molto diversi se viene adoperata per controllare i varchi di ingresso a una zona a traffico automobilistico limitato, se ha finalità di ordine pubblico, se avviene in relazione ad attività commerciali. È dunque necessario contestualizzare, e quindi relativizzare, il discorso sulla tecnologia. Non si può semplicemente dire sì o no alla videosorveglianza: questo sarebbe un discorso astratto e pericoloso. Si debbono analizzare i diversi contesti all'interno dei quali la stessa tecnologia adempia a funzioni diverse e quindi esige regolamentazioni differenziate.

Lo sguardo totale del Garante aiuta, poi, a meglio comprendere le situazioni specifiche. Il Garante talvolta è stato descritto come avversario delle tecnologie, la parola "Talebani" è persino comparsa in qualche titolo giornalistico. Senza voler fare difese d'ufficio, vorrei sottolineare il fatto che il Garante ha accompagnato con gran-

(1) Presidente Garante per la protezione dei dati personali

de attenzione, e anche con una funzione di legittimazione davanti all'opinione pubblica, l'ingresso progressivo e legittimo delle tecnologie nella società. Al tempo stesso ha messo in evidenza, come nell'ultima relazione al Parlamento, anche i rischi di derive tecnologiche.

Che cosa vogliamo dire adoperando questa formula? In primo luogo vogliamo segnalare l'inopportunità di deleghe acritiche alla tecnologia: risposta tecnologica è accettabile solo se associata a una consapevolezza dei suoi effetti sociali. In secondo luogo un'attitudine acritica, o addirittura apologetica, ha due conseguenze negative: sottovalutare le debolezze tecnologiche e non apprezzare le vere opportunità offerte dalla tecnologia nella nostra dimensione. Quando, ad esempio, si parla di biometria, terreno oggi straordinariamente fertile anche per improvvisazioni ed esagerazioni, il tema delicato e fondamentale dei falsi positivi e dei falsi negativi nell'identificazione e autenticazione dei soggetti non viene abitualmente preso in considerazione. Il fatto che gli stessi tecnologi, anche in Italia, mettano in evidenza i problemi legati alla possibilità di falsificare l'impronte digitali impone estrema cautela. Di conseguenza, un riferimento acritico rischia di mettere in crisi la credibilità stessa delle tecnologie, come dimostra la casistica di esperimenti in materia biometrica interrotti, sospesi o ridimensionati per evitare il rischio dei falsi negativi che l'avevano screditati di fronte alla collettività.

Bisogna aggiungere che una attenzione critica tende a valorizzare le opportunità che possono scaturire dall'interno stesso delle tecnologie. Non voglio evocare il mito della spada che guarisce le ferite che ha inferto. Ma è certo che le cosiddette *privacy enhancing technologies*, cioè i contenuti tecnologici che consentono di proteggere i dati personali insieme o al di là di quelle che sono le regole giuriche, riducendo quindi grandemente i rischi dell'innovazione tecnologica, individuano una dimensione da considerare con la massima attenzione.

Il nuovo Codice, entrato in vigore il primo gennaio di quest'anno, contiene una importante innovazione all'articolo 3, introducendo il principio di necessità: “*i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e dei dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettono di identificare l'interessato solo in caso di necessità*”. La rilevanza di questo principio è evidente, come è evidente l'importanza che esso assume anche per quanto riguarda l'uso economico delle tecnologie, essendo ben noti e numerosi i casi in cui sono stati trattati dati personali senza che ciò fosse effettivamente necessario per la realizzazione delle finalità perseguite. E ciò corrisponde anche alla crescente importanza del principio di precauzione, al quale fa riferimento l'articolo 174 del Trattato dell'Unione europea e di cui si propone, proprio in queste settimane, l'introduzione nella Costi-

tuzione francese per impulso del Presidente della Repubblica Chirac. A questo proposito, si è detto che, costituzionalizzando principi come questo, si laicizza la scienza, perché questa deve fare più profondamente, autocriticamente, i conti con le conseguenze che possono essere determinate dai risultati delle sue ricerche. Potrei aggiungere che il principio di necessità contribuisce a laicizzare il rapporto tra l'innovazione scientifica e la società.

È, dunque, un passo importante e che ci aiuta anche a superare alcune improprie contrapposizioni, che il Garante ha sempre mostrato essere fuorvianti: privacy contro sicurezza, privacy contro efficienza, e così via. Credo che il lavoro condotto nei sette anni che abbiamo alle spalle sia una smentita concreta dell'insuperabilità di queste contrapposizioni che, presentate come dicotomia, farebbero sì che il bisogno di sicurezza o quello di efficienza imporrebbero di azzerare la privacy. Con provvedimenti concreti abbiamo mostrato non solo come siano possibili forme di bilanciamento tra gli interessi in campo, ma pure come sia necessario trovare nuove e più adeguate forme di garanzia quando si introducono misure per altri versi restrittive della protezione dei dati. E abbiamo messo in evidenza come la privacy possa essere una risorsa per l'impresa o per l'amministrazione.

Con questo convegno vogliamo andare un po' oltre, mostrando come la penetrazione tra protezione dei dati e altri tipi di attività sia la condizione per il successo medesimo delle attività che si vogliono svolgere. Faccio un solo esempio, riprendendo un tema che ha creato qualche equivoco sulle nostre posizioni e che voglio chiarire immediatamente. C'è uno sforzo importante in Italia, e non solo, per rivitalizzare o creare in forme nuove il rapporto fra il cittadino e l'amministrazione locale, vista come luogo dove meglio si può sperimentare una forma di e-government o addirittura di e-democracy. Sono tentativi importanti, che possono tuttavia incontrare gravi difficoltà se l'accesso del cittadino ai servizi comunali, in genere a servizi pubblici, se l'attività diretta di controllo su procedimenti amministrativi e la possibilità di seguire le pratiche che ci riguardano, diventano occasioni per "schedeature" dei cittadini che si servono delle nuove possibilità di accesso, magari tracciando profili non dei cittadini più attivi, ma di quelli più "fastidiosi". Se quell'importante innovazione fosse accompagnata da questo timore, quali sarebbero le reazioni? Caduta della partecipazione, inefficienza del sistema di e-government che viene costruito. Ecco che allora non c'è contrapposizione, tra innovazione tecnologica e tutela rigorosa della privacy.

Guardando più avanti, e considerando le novità legate alla Rfid o al cosiddetto *ubiquitous computing*, dobbiamo indagare una nuova condizione dell'individuo in questo millennio, e cioè la possibilità di una sua localizzazione permanente, anche attraverso servizi personalizzati *location based*, che cambiano la natura dei rapporti personali e lo stesso rapporto tra la persona e la tecnologia non più mediata

dalle tradizionali interfacce. Su questo terreno si giocherà una partita estremamente importante, che mette in discussione valori fondativi, a partire dal ruolo e dalla portata del consenso fino al rispetto di valori fondamentali per l'autonomia della persona, la dignità e l'eguaglianza in primo luogo.

Non dimentichiamo che la Carta dei diritti fondamentali dell'Unione europea si apre proprio con l'affermazione solenne dell'inviolabilità della dignità umana. E il legislatore italiano del '96, con grande lungimiranza, aveva inserito nell'articolo uno della vecchia legge 675 (ora articolo due del Codice) il riferimento esplicito alla dignità. I valori della persona non possono mai essere trascurati, perché appartengono alla storia della nostra civiltà. E rappresentano lo strumento più forte per respingere una lettura pessimistica, heideggeriana, della potenza della tecnica che, essendo produzione incessante di fini, non sarebbe più controllabile. Se accettassimo questa interpretazione, rischieremmo anche rifiuti irrazionali della tecnologia, la cui accettazione sociale, invece, dipende anche dalla rassicurazione che proviene proprio dalle tecniche forti di tutela. Voglio ricordare che, agli inizi degli anni 70, quando la protezione dei dati e l'innovazione tecnologica erano soltanto agli inizi, Ibm registrò una caduta delle vendite di computer in Svezia. Fece un'analisi di mercato e scoprì che quella società aveva una forte tradizione di rispetto per i dati personali che, in mancanza di garanzie adeguate alla nuova situazione, stava producendo un rifiuto sociale di quella tecnologia con effetti negativi per le strategie di vendita. A questo punto Ibm scelse una strategia intelligente e divenne un gruppo di pressione perché la Svezia si dotasse di una legge sulla protezione dei dati che, a livello nazionale, è stata la prima del mondo, nel 1970.

Si ebbe la tutela dei dati personali e ripartì la vendita dei computer. La tecnologia, dunque, non può far riferimento a fini misurati soltanto sulle sue esigenze. Per ragioni di principio deve misurarsi con i valori costituzionali, quindi proporzionare il suo agire ai valori socialmente riconosciuti e così potrà trovare anche strade propizie alla realizzazione del proprio interesse. Il Garante si trova su questo crinale difficile, ha lavorato molto e spera da questo convegno di avere indicazioni di lavoro preziose.



Interventi

SESSIONE I
PROTEZIONE DEI DATI
E SVILUPPO TECNOLOGICO

PRESIEDUTA DA GIUSEPPE SANTANIELLO

Sessione I – Protezione dei dati e sviluppo tecnologico

Tipologia delle innovazioni tecnologiche e protezione dei dati personali

Giuseppe Santaniello⁽¹⁾

Sommario: 1. Note introduttive; 2. Le innovazioni tecnologiche nella scala dei valori socio-economici; 3. I tre grandi settori della dinamica innovativa; 4. Il campo delle comunicazioni elettroniche; 5. Il secondo settore e le linee guida; 6. Le tecnologie emergenti; 7. La nuova frontiera

1. Note introduttive

L'elaborazione di un quadro di principi e di regole rivolto a segnare il raccordo fra le dinamiche tecnologiche e la tutela dei diritti fondamentali della persona costituisce il fattore basilare per ogni ciclo di sviluppo economico-sociale.

Da tante fonti emerge la rilevanza di tale fattore, ma tra esse la più autorevole si rinviene nella Carta di Nizza (settembre 2000), nel cui preambolo si legge che, al fine di promuovere uno sviluppo equilibrato e sostenibile, è necessario “rafforzare la tutela dei diritti fondamentali alla luce della evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici.”

E in un recente volume *Il mondo che cambia* Antony Giddens (uno dei più influenti sociologi del nostro tempo, direttore della London School of Economics) scrive che la scienza e la tecnologia, forze motrici di un'economia mondializzante, stanno ristrutturando il nostro modo di vivere e di operare, sicché hanno bisogno di linee di guida per una innovazione sostenibile.

2. Le innovazioni tecnologiche nella scala dei valori socio-economici

Sulla base di tali fattori sorge l'esigenza di accertare come le innovazioni tecnologiche si collochino nella scala dei valori socio-economici.

Esse si pongono come indicatori di progresso, come potenti leve di miglioramento della qualità della vita, di aumento dei livelli di conoscenza e del sapere, come strumenti di ausilio alle attività di produzione e di scambio e come mezzi pro-

(1) Vicepresidente Garante per la protezione dei dati personali

tettivi della sicurezza informatica. Ma accanto a tanti fattori benefici possono venire in rilievo elementi non positivi, qualora un loro uso improprio vada a incidere su diritti inviolabili.

È opportuno chiarire che le acquisizioni tecnologiche e scientifiche non possono essere considerate come un Giano bifronte: con una faccia rivolta verso il bene e l'altra rivolta verso il male. Tale concezione manichea è fuori dalla realtà. Ogni innovazione tecnologica non può non essere considerata positiva nella sua sostanzialità. Ciò che invece richiede una formulazione di criteri e di regole va riferito alle modalità di applicazione, di uso delle nuove acquisizioni, che, se effettuate in maniera impropria da parte di taluni soggetti, producono effetti distorsivi (la c.d. *deriva tecnologica*).

E allora di fronte all'uso deformante bisogna riconoscere che (come è stato rilevato nella Relazione annuale del Garante al Parlamento) non tutto ciò che è tecnologicamente possibile è anche socialmente desiderabile ed eticamente accettabile.

L'incessante, tumultuoso ritmo di sviluppo delle nuove tecnologie, nel loro poliformismo di tipologie sempre più avanzate, determina un'affannosa rincorsa fra l'intervento dei soggetti pubblici istituzionalmente regolatori (ai vari livelli, sia di diritto interno, sia di diritto sopranazionale) e i soggetti, sempre più numerosi, creatori di diffusori delle innovazioni tecnologiche.

3. I tre grandi settori della dinamica innovativa

Poiché uno dei compiti preminenti del nostro convegno è di indicare quali interventi regolatori vadano attuati al fine di governare lo sviluppo sostenibile delle dinamiche tecnologiche, ritengo che ciò presupponga una ricognizione dei vari settori in cui esse sono articolate.

Il campo è sterminato, poiché accanto a moduli abbastanza consolidati, affiorano con ritmo crescente forme del tutto inconsuete e decollano prototipi mai immaginati, e inseriti in una forte spinta autopropulsiva.

Ritengo che si possano individuare, nella fase attuale, tre grandi settori (o categorie):

- 1) il settore delle innovazioni tecnologiche che sono già ricomprese in un quadro di regole di valore legislativo che le governano;
- 2) il settore delle innovazioni tecnologiche inquadrabili finora in linee guida derivanti dal potere prescrittivo di carattere amministrativo (ad es. autorizzazioni generali, decaloghi di comportamento, etc.) oppure derivanti da codici deontologici e di buona condotta formati con l'intervento dell'Autorità garante;
- 3) il settore delle innovazioni tecnologiche, che in relazione al loro decollo molto recente, non sono tuttora sorrette da regole specifiche, né di valore legislativo né di un efficiente potere ordinatorio amministrativo.

4. Il campo delle comunicazioni elettroniche

Nella prima delle categorie indicate rientra il vasto campo delle comunicazioni elettroniche.

In riferimento alle quali la direttiva europea del 2002 ha inteso promuovere regole neutrali rispetto alla tecnologia, segnando l'obiettivo di garantire a consumatori e utenti lo stesso elevato livello di tutela indipendentemente dalla tecnologia con la quale viene fornito un determinato servizio.

Assume particolare rilevanza il Codice delle comunicazioni elettroniche, approvato con d.lg. n. 259/2003, che nel garantire, in via di principio, i diritti inderogabili delle persone nell'uso dei mezzi di comunicazione elettronica, stabilisce che "Sono fatte salve le limitazioni derivanti da esigenze, ... e della riservatezza e protezione dei dati personali". E soggiunge che, in caso di conflitto fra il diritto di iniziativa economica nel campo delle comunicazioni elettroniche e le normative e protezione della vita privata e dei dati personali, prevalgono queste ultime.

In tal modo si viene a stabilire una interazione fra due codici, l'uno delle comunicazioni e l'altro della protezione dei dati personali, dando vita a un baricentro normativo nel quale confluiscono la tutela di due valori fondamentali, inerenti sia alla libertà di comunicazione e sia alla protezione della riservatezza nei servizi *on line*.

5. Il secondo settore e le linee guida

Il secondo settore racchiude una numerosa serie di acquisizioni tecnologiche di notevole impatto sociale, quali ad esempio la videosorveglianza, le tecniche biometriche, il trattamento dei dati genetici etc..

Pur mancando nella fase attuale un *corpus* legislativo inerente a tali tipi di trattamenti, l'Autorità garante ha potuto supplire a siffatta carenza, emanando linee di guida connesse all'uso del potere dispositivo di valore amministrativo (quali le autorizzazioni generali, i decaloghi di comportamento, la elaborazione di parametri per la legittimità e la correttezza dei trattamenti). Tali interventi hanno trovato ampio consenso e ottemperanza da parte di tutti i soggetti interessati e hanno seguito un sapiente bilanciamento fra i vari interessi coinvolti, delineando soluzioni congrue dei molteplici problemi.

Inoltre nella vasta area di tale settore occupano un posto rilevante i codici deontologici, i quali rappresentano il punto di confluenza fra i poteri propulsivi e di indirizzo dell'Autorità garante e la proposizione delle regole da parte dei soggetti rappresentativi di determinate categorie.

Tali codici hanno particolare attitudine a seguire le dinamiche della tecnologia.

6. Le tecnologie emergenti

Il terzo settore ricomprende innovazioni della tecnologia e della scienza, che stanno emergendo in una fase recentissima, si trovano ancora in una situazione di sperimentazione, ma presentano una particolare rilevanza, poiché alcune di esse da un lato incorporano i fattori di sviluppo del futuro e dall'altro, pur offrendo agli utenti grandi opportunità, possono creare nuove vulnerabilità individuali e sociali.

Il documento strategico elaborato recentemente dal Gruppo di lavoro dei garanti europei pone particolare attenzione a tali innovazioni emergenti, quali le Rfid, i servizi di geolocalizzazione, le acquisizioni della genetica e della biometria.

Un particolare impegno di vigilanza va rivolto alla tecnologia delle radiofrequenze, la quale ha portato alla creazione di etichette intelligenti, che, sostituendo i codici a barre, permetteranno di seguire i prodotti nei loro spostamenti, creando però anche la possibilità di controllare coloro che hanno acquistato o usano tali prodotti.

È da rilevare che l'esigenza di intervenire in tale delicato settore, è avvertita non solo in Italia, ma anche in altri Paesi e particolarmente negli Stati Uniti, dove è stato avviato un ampio dibattito in merito alle opportunità offerte dall'introduzione della Rfid e alle cautele da porre in essere, per evitare la violazione delle libertà civili e del diritto alla privacy.

Bisogna evitare un utilizzo incontrollato, e a tal fine viene proposto un modello normativo che tuteli il diritto del consumatore di conoscere quali prodotti sono caratterizzati, il diritto alla rimozione della *tag* al momento dell'acquisto del prodotto, l'applicazione della tecnologia ai servizi al consumatore solo in virtù del consenso informato, libero, e specifico degli interessati.

Anche i servizi di geolocalizzazione devono essere inquadrati in un nucleo di regole basilari. È stato già rilevato che le tecnologie elettroniche, dopo aver contribuito all'annullamento della distanza, stanno ora facendo riscoprire la *prossimità*, la localizzazione delle persone. Ed anche tale fattore va coordinato con i diritti di libertà della persona.

Sulla base di tali profili, possiamo affermare che per tutto il terzo settore è urgente la elaborazione di regole che valgano a rendere sostenibile il processo innovativo della scienza e della tecnologia.

Ma l'evoluzione normativa della materia non può affidarsi a una fonte legislativa monocentrica, bensì a un policentrismo di fonti collocate in una coordinata sequenza a vari livelli (una cornice legislativa concertata tra tutti i Paesi interessati alla soluzione del problema e, in aderenza ad essa, la specificazione di regole mediante leggi nazionali, a seconda delle varie aree geografiche, e inoltre l'adozione di codici-modello di formazione autodisciplinare). Si realizza in tal modo quel moderno processo regolatore, frutto della convergenza di molteplici fonti normative, che si definisce come *coregulation*.

7. La nuova frontiera

Siamo consapevoli che il raccordo fra innovazione tecnologica e protezione dei dati personali presenta una particolare complessità, poiché sono in atto due forti dinamiche. Da un lato emerge l'accelerazione delle acquisizioni tecnologiche, che sempre più accentuano i loro caratteri della multidimensionalità e della globalità. Dall'altro lato viene in rilievo l'accelerazione della metamorfosi della riservatezza, che da guscio protettivo della persona va evolvendo a patrimonio informativo circolante, come denominatore comune di tutte le realtà industriali, commerciali, culturali, pubbliche e private e come riferimento costante in tutti i campi di attività. Ma il nostro impegno istituzionale è rivolto a superare le intrinseche difficoltà, individuando il punto di saldatura fra le due dinamiche e realizzando la sinergia fra le due forze motrici di un grande ciclo evolutivo.

Come ha rilevato in un suo recente scritto il prof. Gaetano Rasi “l'accelerazione nell'introduzione di innovazioni è il centro del processo evolutivo del sistema economico contemporaneo e, a livello macroeconomico, del comportamento dei singoli operatori. Sicché è necessario che si crei un equilibrio virtuoso tra l'espansione economica e le garanzie per i soggetti destinatari degli impulsi che spingono le innovazioni, le quali, a loro volta, determinano l'espansione economica”.

Governare l'innovazione tecnologica: è questa oggi per tutti noi la frontiera più avanzata.

Su tale terreno si misura la capacità innovativa dei sistemi giuridici a tutela di valori fondamentali degli individui e della collettività.

Maurizio Dècina⁽¹⁾

Ringrazio il presidente Santaniello e il presidente Rodotà per il gradito invito a partecipare. Sono un rappresentante della tecnologia e voglio assicurare il Garante che credo anch'io che la tecnologia sia una sorta di Giano bifronte. La tecnologia, di volta in volta, da un lato presenta delle grandi opportunità, mentre dall'altro presenta delle grandi minacce.

Sta proprio agli scienziati e agli ingegneri il compito di ascoltare le raccomandazioni della società civile per armonizzare l'introduzione delle nuove tecnologie.

- La sicurezza e la privacy delle informazioni sono oggi minacciate dai pirati informatici che navigano nel ciberspazio realizzato dalla rete Internet e dalle sue innumerevoli applicazioni. Questo scenario è destinato ad evolvere rapidamente, verso orizzonti ancora più minacciosi. La rete si amplia vertiginosamente, sia con la diffusione degli accessi ad Internet tramite i sistemi mobili, sia con la diffusione dei sistemi di calcolo pervasivo: gli oggetti intelligenti.

Nel mondo degli oggetti intelligenti, del calcolo pervasivo e ubiquo, le minacce alle informazioni del mondo "virtuale" creato da Internet si arricchiscono di nuove minacce, forse più devastanti, connesse al mondo "reale", degli oggetti, degli indumenti e degli ambienti che ci circondano, fino ad arrivare agli oggetti "immersi" nel corpo delle persone.

La tecnologia moderna indirizza il problema della sicurezza informatica nei due mondi, quello virtuale d'oggi (Internet) e quello reale del futuro (Internet pervasiva).

Mentre nel mondo virtuale, nel ciberspazio, non ci sono più luoghi fisici e distanze; in quello reale, popolato di "sensori wireless" immersi nell'ambiente che ci circonda, localizzazione e distanza diventano di nuovo importanti. Tutti i problemi socio-economici relativi alla raccolta d'informazioni sugli utenti nel ciberspazio diventeranno attuali anche nel mondo reale.

- Ci sono tre facce della sicurezza dell'informazione, tre diversi aspetti della sicurezza, strettamente collegati tra loro dal punto di vista delle tecnologie informatiche usate e dei problemi socio-economici che stimolano. Queste sono: la sicurezza vera e propria, intesa come la segretezza, la confidenzialità o la riservatezza delle informazioni che si scambiano in rete gli interlocutori.

La privatezza delle informazioni è la seconda faccia. Qui si tratta sostanzialmente del problema della "riservatezza dei dati personali", ma non solo, direi che è in gioco il "diritto all'anonimità", o meglio il diritto alla "inosservabilità", sem-

(1) Politecnico di Milano/CEFRIEL

plici e basilari diritti che le persone hanno (avevano) nel mondo della pre-tecnologia-dell'informazione.

La terza faccia è quella della proprietà intellettuale. La gestione dei diritti digitali per il godimento on-line di brani musicali, brani video, e-book, è un tema molto importante che si affida a soluzioni tecnologiche per controllare l'accesso degli utenti alla fruizione dei prodotti elettronici. Sono fornite ai clienti, che hanno acquistato i diritti d'autore, delle chiavi crittografiche personalizzate che consentono la visione e l'ascolto dei prodotti scaricati on-line.



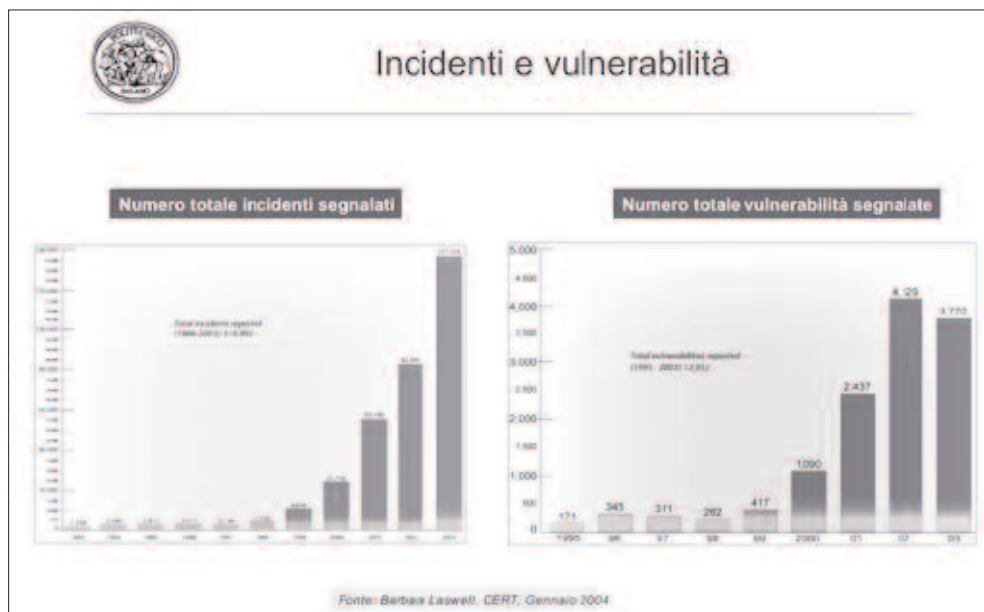
Le tecnologie della crittografia per provvedere alla segretezza, alla privacy e alla gestione dei diritti digitali sono comuni alle tre facce e sono largamente basate su algoritmi matematici relativi alla teoria dei numeri primi.



Privacy, security e accountability, sono tre temi di cui oggi stiamo dibattendo. La sicurezza la conosciamo: l'integrità dei messaggi, la confidenzialità, l'identificazione delle persone, la disponibilità dei sistemi, sono tutti aspetti noti. La privacy è più complessa e richiede una terza proprietà per permettere il commercio elettronico "etico" (dal punto della vista della sicurezza e della privacy): l'accountability, la garanzia di responsabilità, legata alla "reputazione" degli individui dal punto di vista del commercio elettronico. Che cosa vuol dire anonimità? Non voglio che qualcuno sappia che la tal sera sono andato al cinema con la famiglia a vedere un certo film: perché è un mio diritto elementare di agire senza essere continuamente osservato. C'è quindi la pseudo-anonimità per consentire l'uso di pseudonimi plurimi e cangianti nel tempo, esiste anche il principio del "non ripudio", cioè della responsabilità dell'individuo. Se faccio una transazione commerciale su Internet, la transazione è sicura ed è andata a buon fine: ho usato uno pseudonimo (per motivi di privacy), ma non posso negare di aver effettuato quella transizione e ne assumo la responsabilità economica. Sempre in relazione al tema dell'anonimità si parla di principi di "intracciabilità" e "inosservabilità" delle persone, sia nel ciberspazio (la passeggiata virtuale su Internet), sia nello spazio fisico e reale (nella geo-localizzazione delle persone con i telefonini e i Gps, eccetera).

- Nel 2003 sono stati rivelati dal Cert Coordination Center (il celebre ente statunitense per la sicurezza telematica, che ha appena compiuto 15 anni di vita) circa 140.000 attacchi informatici (incidenti) segnalati, contro 80.000 del 2002.

Nel 2004, il numero degli incidenti segnalati continua inesorabilmente ad aumentare, con tassi di crescita del 60-80% l'anno. L'unico miglioramento segnalato dal Cert/cc è la diminuzione delle vulnerabilità riscontrate a fronte degli attacchi rivelati: questo significa che in qualche modo la consapevolezza delle aziende e dei consumatori nei riguardi della sicurezza informatica è aumentata.

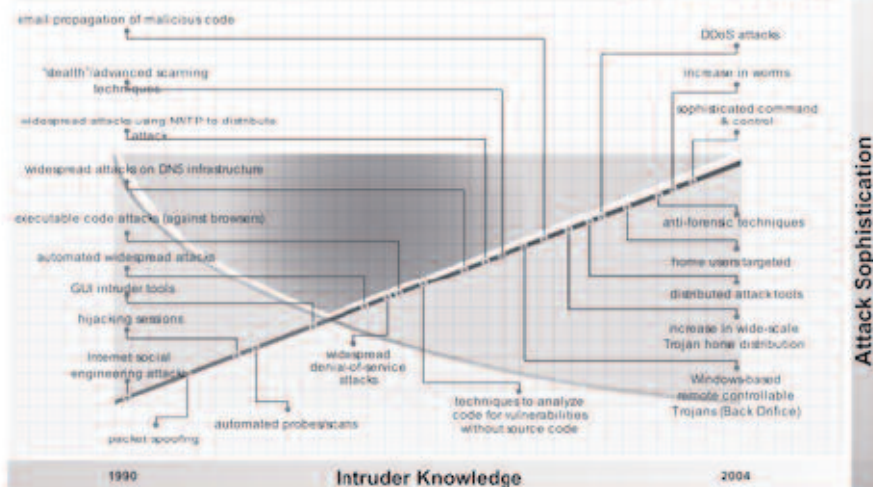


Un celebre grafico pubblicato dal Cert/cc mostra che dal 1990 al 2004 le tecniche d'attacco sono diventate sempre più sofisticate, grazie alla disponibilità sulla stessa Internet di siti web pirata che forniscono strumenti informatici, tools, che permettono di eseguire attacchi a persone che non sono esperte, ma semplici esecutori.



Evoluzione delle tecniche di attacco

Fonte: CERT/CC 2004



• Dai virus ai worm, dai trojan allo spyware, per finire con lo spam e il phishing. L'universo zoologico degli strumenti di pirateria informatica si è andato popolando di nuove devastanti specie. Oggi quello che importa è appunto il cosiddetto “ciclo delle vulnerabilità”, in altre parole, con riferimento ai virus, il periodo di tempo che intercorre tra l'immissione in rete del virus e l'applicazione dell'antivirus sui computer esposti in rete. Questo periodo comprende la rivelazione della vulnerabilità attaccata dal virus, la creazione del “fix”, dell'antivirus, ed inoltre la distribuzione del fix in rete. Oggi il ciclo dura da poche settimane a qualche giorno, nell'assunzione che gli utenti dei computer applicano poi effettivamente il fix alle loro macchine. L'evoluzione degli attacchi tende a generare virus che si autoreplicano e si diffondono sempre più rapidamente: in un prossimo futuro il ciclo di vulnerabilità potrà arrivare a poche decine di minuti. Una vertiginosa competizione globale “guardie e ladri” contro il tempo!

Va rilevato che spesso le aziende e gli utenti in generale sono “pigri” nell'eseguire gli aggiornamenti antivirus necessari, così come gli aggiornamenti delle loro password. Nel caso del worm Sasser, la Microsoft aveva rilasciato il fix della vulnerabilità il 13 aprile del 2004, gli attacchi effettuati nei mesi seguenti hanno colpito numerosi grandi enti e grandi aziende che non avevano eseguito per tempo l'aggiornamento dei loro server.

Si tratta di mancanza di “cultura della sicurezza”. La sicurezza dei sistemi infor-

matici in rete non si protegge soltanto utilizzando strumenti tecnologici di difesa: un adeguato grado di sicurezza si ottiene anche attraverso l'impiego di processi organizzativi e risorse umane

- Ci sono una serie di grandi innovazioni nelle tecnologie della sicurezza. Possiamo fare riferimento a quattro grandi famiglie di tecnologiche. La prima è la tecnologia della crittografia, gli algoritmi matematici che oggi ci consentono di cifrare i messaggi e autenticare le persone. Lo standard Des ha lasciato posto al nuovo standard Aes, molto più potente contro gli attacchi dei malintenzionati. Anche qui si tratta di una gara contro il tempo tra coloro che inventano nuovi algoritmi crittografici e coloro che invece studiano algoritmi per la decifrazione di testi segreti.

La seconda famiglia tecnologica è quella della trasmissione a distanza d'informazioni, "sicura al 100%". È il settore della crittografia quantica, che permette di trasmettere informazioni sulle fibre ottiche con la garanzia di non-intercettazione: incominciano ad apparire sul mercato i primi costosissimi dispositivi commerciali (vedi la società Quantique di Ginevra).

Il terzo settore è quello dell'identificazione biometrica (impronta digitale, configurazione del volto, dell'iride, impronta vocale, ecc.). Un settore molto decantato dai media, che però deve fare i conti con le probabilità di falso riconoscimento associate a queste tecniche: solo l'uso del Dna minimizza tali probabilità.

L'ultima gran famiglia è quella che fa riferimento allo sviluppo del calcolo pervasivo e ubiquo e degli smart objects, gli oggetti intelligenti. La più grande sfida posta all'ingegno umano per consentire l'armonioso sviluppo a queste nuove tecnologie informatiche consiste proprio nel progettare adeguati livelli di sicurezza in un mondo popolato da oggetti intelligenti.

- Le cosiddette "etichette intelligenti", smart tag o Rfid, Radio Frequency Identification, sono dei tag flessibili che sostituiscono i codici a barre con cui si classificano e si movimentano tutti i prodotti industriali. Gli Rfid sono alimentati direttamente dalla radiazione elettromagnetica del fascio di lettura in radio frequenza. Oggi il costo di un Rfid è dell'ordine di 5/10 centesimi di dollaro Usa, per grandi quantità. La distanza a cui possono essere letti o scritti questi "flexible tag" può arrivare, in determinate applicazioni, anche ad alcune decine di metri. Il mondo della logistica e della grande distribuzione sarà molto presto invaso da applicazioni basate sugli Rfid, con grandi benefici di efficienza ed efficacia.

Nel caso delle etichette intelligenti le tecnologie della sicurezza e della privacy permettono un vasto ventaglio d'opportunità e di soluzioni che possono adattarsi alle specifiche esigenze sociali che verranno a determinarsi. Il metodo più attraente è basato sulla crittografia ed è gestito direttamente dal cliente finale del prodotto dotato di Rfid. Sarà proprio il cliente a decidere quale informazione residente nelle etichette potrà essere rivelata al pubblico e quale dovrà rimanere segreta.

- Le etichette intelligenti sono soltanto un esempio dei prodotti del calcolo pervasivo e ubiquo che si diffonderanno nella nostra vita quotidiana. In generale gli oggetti intelligenti saranno dotati di sensori capaci di comunicazione via radio, wireless, in rete con altri sensori, al fine di realizzare nuovi servizi e applicazioni. Si pensi ad esempio all'uso di micro-sensori wireless per il controllo della inquinazione ambientale o del traffico urbano, oppure per il controllo del riciclaggio di tutti i prodotti industriali.

Nel ciberspazio e nel mondo reale c'è una virtuosa e dinamica frontiera d'equilibrio, tra necessità di garantire la sicurezza, fisica e virtuale, degli individui e necessità di garantire la libertà degli individui stessi e in particolare la loro privacy.

Le tecnologie informatiche della sicurezza e della privacy vanno di pari passo nello sviluppo della scienza e dell'ingegneria dei grandi sistemi telematici. La progettazione e la gestione dei sistemi informativi devono aderire a criteri di diffusione basati sul consenso sociale e civile ai sacrifici delle libertà personali in favore di un equo ed elevato livello di sicurezza sociale.

- Le grandi minacce del mondo digitale sono compensate dalle grandi opportunità offerte dalla tecnologia digitale. Ad esempio, di recente ho avuto modo di illustrare attraenti applicazioni civili e virtuose delle reti di sensori intelligenti, con riferimento ai sensori cosiddetti "smart dust", polvere intelligente. Ho descritto uno scenario (non molto distante nel tempo) in cui la polvere intelligente dotata di sensori d'esplosivi, come quelli che si usano negli aeroporti, è messa a sorveglianza degli snodi di traffico, quali le stazioni delle metropolitane, per la prevenzione d'attacchi terroristi, come quello recente e devastante di Madrid.

Danilo Bruschi⁽¹⁾

Nell'ambito di questo intervento analizzeremo il problema della sicurezza dei sistemi Ict, e quello ad esso correlato della privacy delle informazioni, analizzando la problematica da un punto di vista macroscopico, considerando quindi la sicurezza Ict come un problema a livello di sistema paese e più in generale di cyberspazio. Non ci soffermeremo quindi sui problemi che questo fenomeno induce sulle singole realtà ma ci concentreremo sui suoi effetti a livello di sistema. In particolare analizzeremo le strategie che sono state adottate per affrontare e contenere il fenomeno nel mondo occidentale, cercando di individuare i limiti di queste strategie e proponendo strategie alternative, a nostro avviso, più consone ed efficaci.

L'intervento seguirà la seguente traccia. Dopo una breve introduzione del fenomeno sicurezza informatica e privacy, descriveremo le politiche introdotte per far fronte al fenomeno, analizzeremo le principali criticità di questo approccio ed indicheremo delle strategie alternative mirate a superarne i limiti.

La sicurezza informatica nasce in ambito militare intorno alla fine degli anni '70 con lo scopo di studiare e progettare meccanismi per proteggere le informazioni memorizzate e custodite su sistemi informatici. La disciplina rimane essenzialmente in tale ambito sino al 1988, quando un attacco informatico noto come Internet Worm, effettuato da uno studente della Cornell University⁽²⁾ riesce a mettere fuori uso, nel giro di poche ore, circa 6000 calcolatori collegati alla rete Internet. L'evento fa il giro del mondo, ed il problema dell'insicurezza dei sistemi informatici diventa di pubblico dominio.

Dal 1988 si assiste ad una escalation formidabile del fenomeno, testimoniata da un crescente numero di attacchi informatici (per avere dati quantitativi legati alla realtà italiana si consulti il sito <http://cert-it.dico.unimi.it>, mentre quelli relativi alla realtà statunitense sono consultabili presso il sito <http://www.cert.org>). Per darvi comunque una indicazione approssimativa del fenomeno si tenga presente che nel 2003 gli incidenti informatici registrati in Italia sono stati circa un migliaio contro i circa 150000 degli Usa.

Gli attacchi informatici di questo ultimo periodo sono, rispetto a quelli di prima generazione, sempre meno orientati verso i server di grosse organizzazioni ed enti, e concentrati verso i sistemi dei singoli utenti. Le ragioni di questo cambio di

(1) Università degli Studi di Milano - Dipartimento di Informatica e Comunicazione

(2) E. Spafford, "The Internet Worm Program: An analysis", Computer Communications Review 19(1), pp. 17-57, Gennaio 1989.

prospettiva sono diverse: questi sistemi sono mediamente molto meno protetti di quelli di un'azienda e quindi più facili da attaccare con successo, anche i sistemi di utenti finali contengono informazioni particolarmente utili (non a caso in tutto il mondo si sta assistendo ad un crescente aumento di casi di furto di identità digitale per maggiori dettagli si veda <http://www.idtheftcenter.org>, con la diffusione della banda larga anche un singolo Pc può essere particolarmente interessante come macchina di appoggio per l'effettuazione di attacchi.

Non è nemmeno molto difficile prevedere gli sviluppi di questa situazione, tenuto conto della pervasività delle tecnologie informatiche in tutte le sfere dell'attività umana, è facile prevedere che l'obiettivo degli attacchi informatici sarà sempre più costituito dai singoli utenti, in particolare l'attenzione di chi opera nel mondo dell'hacking sarà rivolta a tutti quei dispositivi in cui si stanno introducendo, solo di recente, tecnologie informatiche quali: telefonini, palmari, elettrodomestici, televisione digitale e sistemi Rfid.

Quindi, a partire dal 1988 le dimensioni del problema sicurezza informatica sono costantemente cresciute, e sicuramente questo trend sarà confermato in un futuro prossimo. Dato alquanto preoccupante, il fenomeno cresce in maniera assolutamente indipendente dalle varie contromisure proposte per il suo contenimento. Anche se molti tra gli addetti ai lavori, insistono nel vedere nella tecnologia la componente preminente della soluzione al problema, sono della convinzione che la soluzione più naturale del problema, sia da ricercarsi a livello politico. Su questo aspetto vorrei incentrare il resto dell'intervento.

Di fronte al dilagare del fenomeno attacchi informatici, la reazione di gran parte dei paesi occidentali, è stata quella di privilegiare una politica di prevenzione basata quasi esclusivamente sulla deterrenza. Il fenomeno sicurezza informatica è infatti stato trattato come un qualunque fenomeno di delinquenza, e dal '90 in poi tutti i paesi occidentali si sono dotati di una legge sulla criminalità informatica, che penalizza le varie tipologie di crimine informatico, sfociate recentemente nella convenzione internazionale sul cybercrime. In alcuni paesi a queste leggi si sono aggiunte leggi che imponevano agli utenti finali l'adozione di una serie di misure per proteggere i propri sistemi, vedi ad esempio la legge italiana sulla privacy⁽³⁾

Oggi, nessuno può negare che l'adozione di questa politica non ha prodotto i risultati attesi. Nonostante l'emanazione di leggi sulla criminalità informatica gli attacchi ai sistemi e la diffusione di virus continuano a ritmi vertiginosi, ed in proporzione sono davvero pochi i responsabili di queste azioni che devono fare i conti con la giustizia. Ad oggi non credo esista nel nostro paese, una sola persona che sia stata condannata in base alla legge 547/93 sul crimine informatico, eppure in dieci anni di at-

(3) In questo scenario una eccezione è costituita dagli Usa, che accanto a misure di questo tipo hanno anche introdotto, seppure in misura minima, misure di educazione, responsabilizzazione e supporto dell'utenza finale.

tacchi informatici ne sono avvenuti parecchi. La stessa legge sulla privacy fa fatica a trovare dei seri “interlocutori”. Quali sono le motivazioni di questa situazione?

Sicuramente uno dei fattori che ha maggiormente influito su questo insuccesso, è un errore di valutazione basato sulla grossolana approssimazione che bit ed atomi siano la stessa cosa. Dove, riprendendo una metafora introdotta da Negroponte⁽⁴⁾, il bit rappresenta tutto quanto concerne il mondo dei calcolatori e delle reti e l'informazione in formato digitale, e l'atomo tutto quanto concerne il mondo che ruota intorno all'informazione stampata.

Ma il Bit non è l'atomo. I bit sono molto più facili da copiare e manipolare. I bit sono molto più facili da inviare. Nel mondo del bit non esistono copie ed originali tutto è un originale o tutto è una copia. Nel mondo del bit è facile nascondere la propria identità o avere mille identità virtuali e nessuna reale. Nel mondo del bit siamo tutti fortemente connessi e una nostra azione può avere ripercussioni e migliaia di chilometri contrariamente a quanto accade nel mondo dell'atomo dove la sfera di influenza di ciascuno di noi è, in genere, geograficamente limitata.

In questo quadro di riferimento non è difficile capacitarsi del perché misure di tipo deterrente/repressivo non possono avere molta presa. Affinchè lo strumento deterrente funzioni è necessario che la repressione sia efficace, ma per reprimere è necessario possedere gli strumenti che consentano di poter individuare con certezza i colpevoli, e nella rete è molto facile nascondere le proprie tracce.

Per contro l'imposizione di scelte o soluzioni tecnologiche può essere facilmente vanificata, se chi le deve implementare non ne capisce l'utilità o l'importanza, e quindi non le installa correttamente, oppure non provvede alla loro regolare manutenzione e aggiornamento.

È cruciale, nel momento in cui ci si riferisce al mondo del bit, conoscerne i meccanismi e le dinamiche, senza questo tipo di conoscenza si rischia di intraprendere iniziative che nel migliore dei casi non portano alcun risultato.

In questo quadro di riferimento le strategie di imposizione e deterrenza, anche se ingrediente irrinunciabile ed insostituibile di ogni strategia di prevenzione, assumono molta meno enfasi, e diventano più efficaci nuovi paradigmi di riferimento che vedano maggiormente coinvolto l'utente finale e quindi la rete. Questi paradigmi si chiamano: sensibilizzazione, formazione, educazione e supporto.

Se si vogliono diminuire i crimini informatici, non è sufficiente penalizzarli, è necessario invece promuovere azioni che spieghino all'uomo della strada il corretto uso delle tecnologie ed i rischi che il loro uso comporta. È inoltre necessario coinvolgere l'utenza finale nel processo di rilevazione e reporting degli incidenti, fornendole un adeguato servizio di supporto. Se si vogliono “imporre” una serie di comportamenti agli utenti della rete, è necessario spiegarne la loro funzione e farne cogliere l'importan-

(4) N. Negroponte, “*Being Digital*”, Vintage Books, 1985.

tanza, l'atteggiamento impositivo non può avere successo, perché comunque è molto difficile individuare chi non si adegua. Le nuove tecnologie impongono nuovi modi per affrontare e risolvere i problemi, siano essi nuovi (cioè generati dalle nuove tecnologie) o vecchi, la storia ci insegna che le vecchie politiche difficilmente funzionano con le nuove tecnologie. Al fine di chiarire meglio questo concetto estremamente importante per la comprensione del resto dell'intervento voglio proporre due esempi su come le nuove tecnologie potrebbero essere usate in modo "innovativo" per ridurre il problema della violazione della privacy, ed il numero di attacchi informatici.

Il principio ispiratore delle politiche per la protezione dei dati personali è l'incentivazione di tecnologie e metodologie mirate a limitare e controllare l'uso di dati personali e sensibili da parte di chiunque possieda una banca dati ad essi relativa. Il problema dal mio punto di vista è un pò diverso. Chiunque conosca i principi di base della sicurezza informatica sa benissimo che una volta che i dati sono stati raccolti e memorizzati su un hard-disk, non sono più controllabili. L'esperienza di questi anni ci ha dimostrato che non esistono sistemi informatici che possono garantire in modo assoluto la riservatezza dei dati in essi memorizzati. Se davvero vogliamo limitare il problema della violazione della privacy, dobbiamo risolvere il problema a monte, e quindi limitare la raccolta di questi dati. La ricerca da diversi anni ha dimostrato che è possibile svolgere gran parte delle attività che si svolgono in rete garantendo l'anonimato di chi le compie e al contempo la correttezza della transazione. Stiamo parlando ad esempio di moneta digitale, di credenziali anonime ecc.⁽⁵⁾. Il ricorso a questi strumenti consentirebbe di ridurre drasticamente la raccolta "impropria" di dati personali e di conseguenza le dimensioni del problema violazione della privacy.

Nell'ambito del mondo della sicurezza informatica invece, il paradigma di riferimento è la protezione di un dato sistema dagli agenti maligni che operano sulla rete. Se osserviamo però attentamente quanto sta accadendo sulla rete in questi ultimi anni, scopriamo che la maggior parte degli attacchi attuali è realizzata sfruttando computer di utenti completamente sprovvisti che lasciano il loro sistema, in genere assolutamente sproteetto, collegato 24 ore su 24 su internet. Un modo quindi per ridurre il numero di incidenti sulla rete sarebbe quello di rendere innocui questi computer. Ecco che quindi l'altra faccia del problema sicurezza informatica, sinora poco esplorata, diventa proteggere gli altri da se stessi, e non solo il viceversa. Se potessimo fare in modo di rendere inutilizzabili tutti i Pc al fine di attaccare altri sistemi, ridurremmo drasticamente il numero di incidenti informatici sulla rete con particolare riferimento alla diffusione di virus e spam. Anche questa è una strada perseguibile, nata ed esplorata nel nostro laboratorio di Sicurezza e Reti (Laser) presso il Dipartimento di Informatica e Comunicazione dell'Università degli

(5) 4 Cfr. D. Chaum, "Security without identification: transaction systems to make big brother obsolete", Communications of the ACM 28(10), pp. 1030-1044, Ottobre 1985.

Studi di Milano, nel quale abbiamo realizzato un prodotto software che installato su un sistema Linux /Windows lo disarma completamente, cioè non gli consente di attaccare altri sistemi⁽⁶⁾, senza intaccare in alcun modo nessun'altra funzionalità.

Questi esempi ci dimostrano che esistono quindi strumenti e metodologie che consentirebbero di ridurre significativamente i problemi di sicurezza dei sistemi e di violazione alla privacy dei cittadini, ma sono semplicemente ignorate. Per contro non è difficile realizzare che queste soluzioni richiedono originalità e padronanza delle tecnologie e quindi difficilmente concepibili da chiunque sia nato e formato nel mondo dell'atomo, che riapplica il suo vecchio atteggiamento al nuovo senza però rendersi conto che la natura delle cose sta cambiando.

Questo discorso è vero in generale per quanto concerne le tecnologie dell'informazione e della comunicazione ma assume la sua drammatica veridicità quando si parla di sicurezza informatica e privacy. Non è possibile pensare e implementare adeguate strategie di sicurezza Ict senza un solido bagaglio di conoscenze tecnologiche, o meglio senza avere capito come funziona la tecnologia della informazione e della comunicazione. È oramai inconcepibile definire una qualunque strategia a livello paese ma anche a livello di qualunque organizzazione, che possa prescindere dall'uso e sviluppo delle tecnologie informatiche, e spesso dall'uso sicuro delle stesse. È quindi fondamentale che nella definizione di queste strategie siano coinvolti sin dall'inizio esperti di tecnologie che sappiano indirizzare correttamente le scelte iniziali e possano valutarne gli impatti. Un aspetto spesso trascurato della rivoluzione informatica è che oramai sono davvero poche le attività che possono essere svolte senza il coinvolgimento di esperti in tecnologie, ed il postulato è ancor più vero in quelle attività in cui entra in gioco la sicurezza.

In conclusione, credo che il problema principale della sicurezza informatica oggi sia essenzialmente un problema di persone. La transizione dalla società dell'atomo alla società del bit, in corso a livello di società civile è ancora in uno stadio primordiale a livello dirigenziale, di fatto gran parte della classe dirigente attuale è stata formata ed è cresciuta nella società dell'atomo di cui dimostra tutte le prerogative. Se tutto ciò è accettabile per quelle sfere in cui la tecnologia Ict gioca ancora un ruolo secondario non lo può essere in quegli ambiti come la sicurezza informatica in cui la tecnologia Ict è soggetto principale. Mai come in questa fase storica la risposta ai problemi di sicurezza coincide con la risposta ai problemi di ammodernamento del paese e dell'intero scenario internazionale e si chiama semplicemente *Bit-Generation*.

(6) D. Bruschi, E. Rosti, "Disarming offense to facilitate defense", Proc. New security Paradigm Workshop 2000, pp. 69-75, Settembre 2000; D. Bruschi, L. Cavallaro, E. Rosti, "Less harm, less worry or how to improve network security by bounding system offensiveness", Proc. 16th Annual Computer Security Application Conference, pp. 188-195, Dicembre 2000.

I futuri scenari della sicurezza informatica

Danilo Bruschi
Dip. Informatica e Comunicazione
Università degli Studi di Milano

Sommario



- Breve rassegna dei principali attacchi in rete
- Scenari futuri
- Breve rassegna sulle strategie introdotte per far fronte al problema
- Analisi delle strategie
- Nuove proposte
- Conclusioni



Passato

- Attacchi a siti istituzionali e grandi aziende (Internet worm, Citibank, DoD, CIA ecc.)
- Hacker i protagonisti della scena
- Molti attacchi distruttivi
- Virus relativamente lenti a diffondersi e particolarmente distruttivi



Presente

- Relativo abbandono degli attacchi in stile "hacker"
- Molti virus
 - Molti veloci ma poco distruttivi
 - Alcuni lenti ma molto distruttivi
- Graduale abbandono della email come meccanismo di infezione
- Crescente numero di sistemi utenti obiettivo di intrusione
- Diffusione di spyware
- Digital Identity theft

FUTURO



- Il virus perfetto: molto veloce e distruttivo, che possa distruggere la rete prima che sia individuato il suo antivirus
- I nuovi obiettivi degli attacchi informatici:
 - Singoli ed i loro dati personali
 - Singoli ed i loro sistemi
 - Le nuove tecnologie: PDA, cellulari, Wi-Fi, elettrodomestici

Strategie - Passato



- Molta enfasi sulla repressione:
 - Leggi e convenzioni sul cybercrime
 - Leggi e convenzioni sui diritti d'autore in rete
- Molta enfasi sull'imposizione:
 - Legge sulla privacy
 - Invio bilanci on-line
- Abbastanza enfasi sulla risposta:
 - CERT

...ma il bit non è l'atomo (I)



- La repressione non è efficace:
 - Nascondere le proprie tracce in rete non è difficile
 - Avere false identità in rete non è difficile
- L'imposizione è diseducativa
 - Rallenta il processo di apprendimento
 - Allontana l'utente dalle tecnologie

...ma il bit non è l'atomo (II)



- La rivoluzione informatica ha sconvolto i paradigmi di riferimento e se nell'era dell'atomo repressione e imposizione potevano essere efficaci
- Nell'era del bit Prevenzione, Sensibilizzazione e Formazione assumono un ruolo preponderante

Prevenzione (privacy)



- Il problema non è solo proteggere i dati raccolti, ma evitare che si raccolgano
- Tutti i servizi informatici hanno bisogno di una identificazione?
 - Sulla rete è possibile fare acquisti in maniera assolutamente anonima (digital cash)
 - Esistono sistemi per accedere a servizi a pagamento in modo anonimo (Anonymous credential)
 - Esistono sistemi per accedere in modo autorizzato e anonimo a qualunque servizio di rete

Prevenzione (security)



- Ogni PC (specialmente se connesso in banda larga) è oggi una potenziale "arma"
- Sulla base di questa considerazione abbiamo sviluppato un sistema per disarmare i computer
 - Il sistema rende innocuo un qualunque PC
 - Basato sul principio "proteggi gli altri da te stesso" invece che "proteggiti dalla rete"
 - Ha ricevuto molta attenzione dalla comunità scientifica internazionale

Il problema è la governance



- Viviamo in una fase storica in cui ad un mutamento della società verso una società del bit, non è ancora corrisposto un mutamento della classe dirigente (gran parte) verso la BIT GENERATION
- Il risultato:
 - Difficoltà nello sfruttamento delle potenzialità delle nuove tecnologie
 - Difficoltà nel predisporre progetti innovativi
 - Uso poco appropriato delle tecnologie
 - Arretratezza della società civile

Conclusioni



"Technological progress is like an axe in the hands of a pathological criminal"

Albert Einstein

Luigi V. Mancini⁽¹⁾

Sommario: 1. Principi dell'ubiquitous computing; 2. Le applicazioni di interesse; 3. Tecnologie abilitanti per l'ubiquitous computing; 4. Problemi di privacy nell'ubiquitous computing; 5. Conclusioni.

Ringrazio gli organizzatori del convegno in particolare il prof. Rodotà e il presidente Santaniello per avermi dato l'opportunità di presentare il mio pensiero sull'erosione della privacy causata dai nuovi sviluppi tecnologici dei sistemi e delle reti informatiche. Oltre che presso il mio dipartimento, questo tema viene affrontato anche dal laboratorio del Consorzio Interuniversitario Nazionale di Informatica (Cini) che ha sede presso l'Università "La Sapienza", ma che ha una valenza nazionale e comprende oltre 20 università italiane. In particolare, il Cini coordina il progetto triennale Firb "Web Minds" (<http://web-minds.consortio-cini.it>) che affronta anche le tematiche dell'*ubiquitous computing*.

Le reti senza cavi o *Wireless* costituiscono una realtà tangibile e pervasiva; si considerino ad esempio la tecnologia *Wireless Fidelity* (Wi-Fi oppure Ieee 802.11x), ma anche i cellulari. In caso di reti wireless l'intercettazione dei dati è particolarmente semplice: questo di per sé solleva un problema di privacy e di security dell'utente. Non voglio approfondire in questa breve presentazione il modo con cui la privacy viene concepita e realizzata negli standard utilizzati oggi per realizzare le infrastrutture di comunicazione wireless, perché questo argomento verrà trattato anche da altri oratori, successivamente, illustrando in dettaglio le soluzioni e gli attacchi più diffusi. Qui voglio in particolare analizzare i più recenti sviluppi delle tecnologie elettroniche ed in particolare i cosiddetti Mems, i Micro Electro Mechanics Systems, per cogliere indicazioni sulle nuove attività di ricerca da intraprendere nel settore della privacy per reti wireless ubique. Esiste oggi una tendenza alla miniaturizzazione e alla pervasività degli apparati wireless. In particolare, l'*ubiquitous computing* rappresenta una nuova era dell'informatica nella quale i computer divengono così piccoli grazie all'uso di nanotecnologia e così poco costosi che essi possono essere immersi, integrati, in quasi tutti gli oggetti nel nostro mondo fisico. I possibili apparati miniaturizzati, impiegabili in una vasta gamma di applicazioni, li chiamerò nel seguito genericamente sensori o reti di sensori. In particolare, con il termine sensore mi riferisco a un'ampia classe di dispositivi ed applicazioni presenti e futuri che si basano sulla miniaturizzazione di

(1) Università di Roma "La Sapienza" - Dipartimento di Informatica

dispositivi wireless che hanno capacità di computazione e comunicazione. Esempi di tali sistemi vanno da dispositivi indossabili miniaturizzabili, pensate a cellulari miniaturizzati, a sensori di controllo di accesso in un edificio, a sistemi di rilevamento e identificazione. La mia tesi è che le soluzioni tecnologiche sviluppate oggi non si applichino direttamente alla rete ubiquitous di domani, ma che è necessario rivisitare gli odierni algoritmi, architetture e protocolli di rete, in modo da poter supportare le applicazioni del domani preservando il diritto alla privacy degli utenti. Inoltre ritengo che alcune delle soluzioni che sembrano adatte per i dispositivi miniaturizzati possono essere direttamente utilizzate con profitto per preservare il diritto alla privacy degli apparati tradizionali di oggi. Cercherò di semplificare questa tesi con vari esempi.

1. Principi dell'*ubiquitous computing*

Gli aspetti che caratterizzano l'*ubiquitous computing* includono:

- la *pervasività funzionale* del computer nelle attività quotidiane. Il permettere agli utenti di espletare il maggior numero di attività quotidiane della sfera personale e professionale utilizzando piccoli dispositivi wireless;
- la *pervasività spaziale*, il poter interagire con il computer ovunque nella dimensione spaziale. In questo paradigma, ogni oggetto del mondo fisico viene dotato di una capacità di calcolo e di comunicazione che gli permette di interagire con l'utente. In questo modo l'utente può accedere alle informazioni che lo interessano da ogni posizione geografica;
- la *trasparenza*, ovvero l'inavvertibilità della presenza di questa tecnologia. La tecnologia dell'*ubiquitous computing* è così immersa nel mondo fisico che diviene invisibile all'utente attraverso un'elevata semplificazione dell'uso del computer. Le operazioni più complesse sono portate avanti semplicemente grazie all'intelligenza immersa nel mondo che ci circonda. Al limite si potrebbe pensare ad un'interazione anche vocale fra l'utente e il mondo reale circostante. Ad esempio, a casa si potrebbe interagire con comandi vocali con il frigorifero per saper cosa contiene la dispensa. Un altro esempio di semplicità di utilizzo a cui sto pensando, meno astratto e più vicino in termini di futuro, è il seguente: sto partendo per un viaggio negli Stati Uniti e dimentico in Italia il mio palmare con la mia agenda elettronica. Ad oggi, sarebbe un problema insormontabile, a meno di non farmi spedire con corriere l'agenda, ma nel mondo dell'*ubiquitous computing*, all'arrivo a destinazione, affitto un palmare, mi autentico alla rete ubiquitous, e accedo in modo trasparente, semplice, ai miei dati personali, alla mia agenda con gli appuntamenti che ho lasciato in Italia e possibilmente anche ai file memorizzati sul mio computer

che si trova nel mio ufficio a Roma. Questa ubiquità, questa trasparenza rispetto all'accesso alle risorse (in questo caso la mia agenda elettronica), questa capacità di eseguire operazioni complesse in modo semplice, è uno degli aspetti fondanti dell'*ubiquitous computing*.

- la *Web presence*. La Web Presence può essere definita come il trasportare su web i servizi che un oggetto fisico offre e viceversa. In altre parole, si tratta di integrare il mondo virtuale web con il mondo fisico reale. Ad esempio, in un modello che adotta web presence, il mio palmare potrebbe interagire con i sensori associati agli oggetti che mi circondano e con i palmari delle persone che mi circondano e mostrarmi le informazioni e i servizi disponibili relativi a specifici oggetti o persone che rientrano nel mio raggio di comunicazione (nel mio vicinato fisico). Il mio palmare si comporta come un portale, si configura dinamicamente e automaticamente in base al mio vicinato fisico e mi mostra le informazioni che esistono nel mondo virtuale Internet relativamente agli oggetti e le persone fisiche che mi stanno circondando. Quindi c'è un raccordo fra il mondo reale e quello virtuale. È questo quello che si intende come concetto di web presence.

Ad oggi i sistemi di elaborazione non ci supportano a sufficienza, ma il livello di supporto si innalzerà drasticamente. I nuovi sistemi dovrebbero svolgere le funzioni di un domestico, un badante efficiente, invisibile, silenzioso: questo è lo scopo dell'*ubiquitous computing*. In altre parole, lo scopo è quello di realizzare una realtà arricchita da nuove funzioni, il che è diverso dalla creazione di una realtà virtuale. Riprendendo l'esempio di prima sull'uso della dispensa in cucina, quello che ci si prefigge è di poter interagire vocalmente con la dispensa e il frigo per rintracciare i vari alimenti e gli oggetti necessari per preparare la cena arricchendo la realtà di una nuova interattività con l'utente.

2. Le applicazioni di interesse

Nel campo del civile, possiamo pensare all'automazione domestica, ad esempio mantenere temperature differenziate nei diversi ambienti in cui viene installato un impianto di climatizzazione. Inoltre, il controllo flessibile per l'accesso ad edifici di enti e aziende: potremmo avere sensori wireless distribuiti nell'edificio che controllano gli accessi. Un'altra applicazione, già più vicina a noi, sarà quella di poter effettuare micro-pagamenti, ad esempio tramite un piccolo dispositivo wireless personale; si pensi al pagamento del biglietto dell'autobus tramite il proprio palmare o il proprio portatile o il proprio cellulare, automaticamente, mentre si sale sull'autobus e si transita davanti alla macchinetta senza dover comprare il biglietto. Inoltre un'altra delle possibili applicazioni civili è quella di identificare, individuare e seguire gli

spostamenti di valori immobili, di merci, anche al fine di migliorare la sorveglianza delle frontiere terrestri e marittime, quindi la geolocalizzazione di beni e persone.

Altre applicazioni includono: i sistemi di rilevamento, prevenzione, allarme per garantire l'affidabilità delle infrastrutture critiche, ad esempio pensiamo ai trasporti o piuttosto alle infrastrutture dell'energia elettrica, dell'acqua ecc. Si può anche pensare alla predisposizione di sistemi di prevenzione e allarme in caso di malfunzionamenti.

Un'altra applicazione di interesse è nel campo della medicina. La miniaturizzazione permette nuovi sviluppi nella scienza e nella medicina. Pensate all'uso di micro-sensori per monitorare le evoluzioni delle malattie, ma anche a nano-sensori che, una volta iniettati nel corpo umano, vanno alla ricerca di cellule malate per neutralizzarle. Si pensi alle cellule tumorali; i sensori potrebbero rilasciare micro-dosi di farmaco direttamente sulla cellula malata per poterla curare. Questi sensori sono wireless ed interagiscono all'esterno con un sistema di controllo supervisionato dal medico che ha in cura il paziente.

Considerando che intercettare le comunicazioni wireless è semplice ed è quasi non rilevabile, lascio agli esperti la valutazione della normativa per preservare il diritto alla privacy del paziente in una simile applicazione. In particolare, per quanto riguarda le informazioni che fluiscono tra il computer del medico che ha in cura il paziente ed i sensori che sono nel corpo del paziente. Un'altra area di interesse riguarda la sicurezza del cittadino. Ad esempio, l'Unione Europea ha annunciato il finanziamento di grandi progetti di ricerca per realizzare un'Europa sicura. Nel prebando di marzo 2004, si enfatizza l'uso di sensori e micro-sensori per creare dei sistemi di identificazione e rilevamento per la lotta al terrorismo ed il controllo alle frontiere. Il budget che si annuncia è di 1 miliardo di euro all'anno dal 2006 in poi.

Quindi si potrebbe pensare a soluzioni tecnologiche basate sul modello di *ubiquitous computing* per identificare soggetti pericolosi, per prevenire la minaccia bioterroristica, per scoprire i crimini in esecuzione. Ad esempio, si pensi che la maggior parte degli esplosivi rilasciano delle particelle di nitrato di azoto nell'aria. Dei sensori che rilevino questo tipo di composto chimico possono essere utilizzati per prevenire attentati, monitorando bersagli sensibili agli attacchi terroristici, quali stazioni, ferrovie, treni, aeroporti ecc.. Inoltre, queste reti di sensori e di micro-sensori possono essere utilizzate per migliorare la gestione della crisi post-attentato, comprese le operazioni di ricerca e di salvataggio delle possibili vittime.

Ancora, si potrebbe pensare di realizzare un sistema di guida sicura. L'installazione nelle auto di un sistema di guida che riduca il numero di violazioni del codice della strada. Ad esempio, il sistema potrebbe segnalare l'avvenuta infrazione automaticamente all'Autorità della Pubblica Sicurezza, ma al limite si potrebbe anche creare un sistema per cui le regole della strada non possono essere violate: l'auto potrebbe rifiutarsi di superare i limiti di velocità oppure rifiutarsi di parcheggiare in se-

conda fila. Di nuovo lascio agli esperti come preservare giuridicamente il diritto alla privacy dell'utente in simili applicazioni.

Un esempio di applicazione dell'*ubiquitous computing* in ambito militare è l'utilizzo di smart dust. Gli smart dust sono micro-sensori che vengono sparsi sul terreno con elicotteri o aerei, ai fini di fornire una rete di comunicazioni tra le truppe in ambienti ostili e anche per raccogliere dati sul terreno circa la presenza di gas tossici, batteri, presenza di radioattività ed altro.

3. Tecnologie abilitanti per l'*ubiquitous computing*

Una delle tecnologie abilitanti per l'*ubiquitous computing* è quella che ho chiamato rete di sensori wireless, che può essere vista come una rete composta da decine di migliaia, possibilmente milioni, di sensori che non hanno una struttura di comunicazione fissa, ma la cui struttura di comunicazione si configura dinamicamente. Pensate a sensori che vengono distribuiti da un elicottero; la struttura si crea nel momento in cui i sensori toccano il suolo. Questa rete di sensori, possibilmente mobili, può essere formata dinamicamente, può essere unita dinamicamente ad un'altra rete, o partizionata dinamicamente mentre funziona. Qual è il punto di forza di questo paradigma? È un paradigma distribuito, quindi non ha singoli punti di fallimento. Inoltre, sono dispositivi che possono essere palmari o anche miniaturizzati al livello di grano di polvere e comunque possono essere trasportati dall'uomo facilmente, anche indossati.

Il modello di interazione fra i dispositivi è peer-to-peer. Questo modello di interazione è abbastanza diffuso su internet, si pensi a Napster, o comunque ai vari sistemi di file sharing utilizzati su Internet. Questo modello viene introdotto anche nell'*ubiquitous computing*. Ogni nodo della rete è sia un cliente sia un server. Infatti, riceve le richieste, fornisce i dati, se li ha, oppure propaga le richieste ai nodi vicini. Un utente, per accedere ai servizi, deve condividere le risorse disponibili sul proprio computer con altri utenti perdendone il controllo. Quando un utente U effettua una richiesta di un servizio, quest'ultima viene ricevuta anche dai dispositivi di altri utenti vicini che possono automaticamente propagare la richiesta ma allo stesso tempo, se ne hanno la possibilità, rispondono direttamente ad U. Quindi il dispositivo di un utente può essere contemporaneamente sia un cliente sia un server del sistema: il dispositivo dell'utente costituisce un nodo della rete ubiquitous che contribuisce, assieme agli altri suoi pari, a fornire un servizio. Vale la pena di notare che per accedere ai servizi in questo modello, l'utente deve entrare nell'idea di condividere le risorse disponibili sul suo dispositivo con altri utenti, indebolendone il controllo degli accessi. Se si vuole accedere alla rete ubiquitous, se si vuole beneficiare dei servizi disponibili bisogna accettare il modello peer-to-peer: l'utente

deve accettare di rinunciare al controllo completo su una parte delle risorse che ha in termini di memoria, di potenza di calcolo, di capacità di comunicazione, altrimenti non si riesce a beneficiare dei servizi. Questo modello peer-to-peer è alla base delle reti ubique, difatti stiamo parlando di reti di dispositivi che hanno una limitata capacità di calcolo e di comunicazione, quindi devono necessariamente cooperare tra loro per offrire i servizi.

4. Problemi di privacy nell'*ubiquitous computing*

Emergono vari aspetti critici che rendono difficile preservare il diritto alla privacy dell'utente nell'*ubiquitous computing*. Infatti, l'informatica combinata con l'uso di nano-tecnologie diventa invasiva della privacy. In particolare, un tale sistema è progettato dalla sua base per essere invisibile all'utente e per essere ubiqou. Dati questi criteri di progettazione, l'utente interagisce con il sistema ubiquitous automaticamente e può essere tracciato anche a sua insaputa. Oltre agli aspetti legati all'invisibilità ed alla ubiquità del sistema, ci sono due altri punti che rendono la garanzia al diritto della privacy ancora più complessa da realizzare ed estendono le capacità di controllo sui cittadini. Le analizziamo brevemente. I due aspetti sono legati all'utilizzo del paradigma peer-to-peer e del Data Mining.

Si è detto che secondo il paradigma peer-to-peer, per accedere ai servizi bisogna condividere le risorse personali con altri utenti, indebolendo il controllo sui contenuti trattati. Ora, perché si dovrebbe accettare una cosa del genere? La risposta è perché siamo molto interessati ad usufruire del servizio. Difatti, è un'azione che compiamo supinamente già adesso quando navighiamo su Internet. Noi accettiamo che sul nostro computer venga memorizzato automaticamente un cookie per poter accedere ad un certo servizio, perché altrimenti il servizio non verrà fornito. Il cookie rappresenta un esempio di condivisione di risorse personali di memoria senza avere il controllo completo sui contenuti. Nel peer-to-peer questo fenomeno è la norma su cui si fonda l'interazione fra i vari nodi della rete. Ad esempio, si consideri un sistema peer-to-peer per la segnalazione di eventi di congestione del traffico. Si è verificato un grave incidente. I sensori che sono sulle automobili coinvolte, oppure anche non coinvolte nell'incidente, ma che transitano nelle vicinanze, catturano l'evento "Grave incidente automobilistico" e lo diffondono in tutte le direzioni alle altre macchine che transitano fino a che la notizia non arriva in una stazione radio che la inoltra in broadcast e pianifica eventi per risolvere la congestione del traffico. Si potrebbe dirottare il traffico su altri itinerari, ecc.. Chiaramente, l'evento dell'incidente potrebbe anche essere immediatamente segnalato ai palmari dei guidatori che sono nelle automobili che sopraggiungono per evitare complicazioni ulteriori.

Il paradigma peer-to-peer è potentissimo proprio perché permette questo tipo di

applicazioni di grande utilità sociale. Dall'altro lato, però, è necessario che chi usufruisce di questi servizi rinunci al controllo completo sui propri sistemi; in questo caso del proprio cellulare, che autonomamente propagherà la segnalazione dell'incidente.

Il data mining estende ulteriormente la capacità di controllo. L'*ubiquitous computing* permette di raccogliere grandi quantità di informazioni, ed in particolare incrementa la capacità di raccogliere informazioni sugli utenti. Questo sviluppo si affianca ad una più affinata capacità di analizzare efficientemente i dati raccolti. Grazie alle tecniche di data mining, allo sviluppo dei motori di ricerca, e alle base dei dati, il trovare correlazioni ed inferire conoscenze dai dati raccolti è diventato estremamente efficiente. Queste tecniche estendono maggiormente la capacità di controllo dei cittadini da parte di aziende ed enti governativi, difatti permettono di inferire conoscenze che non sono presenti nei dati, ma che possono essere ricostruite correlando i dati raccolti. La semplice analisi degli acquisti dei cittadini in un supermercato, oggi rappresenta una minaccia molto limitata alla privacy se rapportata alle informazioni che saranno analizzabili efficientemente in un prossimo futuro.

5. Conclusioni

Garantire la sicurezza e la privacy degli utenti in un ambiente di *ubiquitous computing* presenta grandi sfide: attività che normalmente non lasciano traccia, grazie alle nuove tecnologie potranno essere analizzate e correlate. Come garantire la privacy? Un primo passo è l'attuazione del *principio di necessità* espresso dal prof. Rodotà in apertura e anche richiamato dal prof. Bruschi: non utilizzare i dati personali dell'utente se non quelli strettamente necessari per portare a compimento il servizio richiesto e con il consenso dell'utente. Vorrei proporre però un ulteriore passo per garantire i cittadini. Si potrebbe progettare e realizzare l'anonimato degli identificatori dei dispositivi ai livelli più bassi di rete e non solo a livello di servizi di rete. In altre parole, non sto parlando di un servizio di denaro elettronico anonimo, ma sto parlando di utilizzare identificatori anonimi come concetto fondante dell'infrastrutture di rete. Questi identificatori anonimi sono ridondanti, quindi ogni utente reale può avere più identificatori anonimi associati a lui. L'associazione fra utente reale e i suoi identificatori anonimi è mantenuta da un'Autorità indipendente ed è utilizzabile soltanto per i fini previsti da un'apposita Norma. È fondamentale che la possibilità di costruire questa associazione non sia nella disponibilità del gestore della rete. In altre parole, sfruttando l'analogia con il numero di cellulare, oggi noi abbiamo un numero di cellulare che è associato a un utente reale. Con gli identificatori anonimi, avremmo tanti altri numeri per ciascun utente che non sono associabili al proprietario. In particolare, il gestore della rete non li può associare all'utente reale, chi può risolvere l'associazione identificatori anonimi-utente è solo l'Autorità indipendente. Questo sistema ci per-

mette di potere avere una serie di interazioni con il mondo che ci circonda, in modo anonimo. Ad esempio per effettuare i micro-pagamenti. Se un cittadino desidera prendere un'autobus urbano e pagare il biglietto dell'autobus con il suo cellulare non e' necessario che lui riveli la propria identità al gestore della rete oppure al gestore del servizio di trasporto. In questo caso il cittadino potrebbe programmare il suo dispositivo in modo da utilizzare un identificatore anonimo.

Come secondo esempio, si ipotizzi una rete di *ubiquitous computing* installata in Via del Corso. Il cellulare di un cittadino, durante una sua passeggiata in Via del Corso, interagisce in modo invisibile con migliaia di sensori e dispositivi wireless delle varie attività commerciali lungo il tragitto. Queste non necessariamente devono conoscere l'identità del cittadino, e nemmeno il suo identificatore a livello di rete, in particolare se non viene effettuato nessun acquisto.

Quindi per i micro-pagamenti è sufficiente autenticarsi con un identificatore anonimo non riconducibile all'utente reale. Per le transazioni commerciali rilevanti, ad esempio il trasferimento di grosse somme fra conti correnti bancari, l'utente deve necessariamente identificarsi rivelando la sua identità reale, ma si noti al solo fornitore del servizio. Va notato che l'utente deve poter rivelare la sua identità al fornitore del servizio e non al gestore della rete. Il gestore della rete comunque non ha la necessità di conoscere l'identità dell'utente in una transazione bancaria rilevante, l'importante è che la banca dall'altra parte della rete possa accertare l'identità reale dell'utente. A livello di principio, quindi, non è necessario che il gestore della rete conosca l'identità dell'utente reale che effettua la transazione.

Riassumendo, ho mostrato alcuni esempi di nuove problematiche; per preservare il diritto alla privacy degli utenti nell'era dell'*ubiquitous computing* si richiedono nuove soluzioni e nuove attività di ricerca che permettano di garantire il diritto alla privacy. È doveroso evitare che l'incubo Orwelliano del romanzo 1984, diventi realtà nel prossimo futuro. Dunque, nuove norme devono garantire un uso etico della tecnologia che preservi dei valori importanti e fondanti della nostra società. Se dovessimo fallire, credo che Orwell sia stato un ottimista in questa citazione:

“Nella veglia o nel sonno, al lavoro o a tavola, in casa o fuori, a letto o in bagno, non c'era scampo. Nulla vi apparteneva, se non quei pochi centimetri cubi che avevate dentro il cranio.” George Orwell, 1984.

Quindi, concludendo, bisogna governare il processo di innovazione tecnologica seguendo il concetto espresso in apertura dal prof. Rodotà della *relativizzazione* della tecnologia. Bisogna cioè analizzare i diversi contesti applicativi per ritagliare su misura la tecnologia e la normativa alle esigenze di quella particolare applicazione.

Alexander Dix⁽¹⁾

Sommario: 1. Osservazioni generali; 2. Applicazioni possibili; 3. Effetti in termini di privacy; 4. Progettazione finalizzata al potenziamento della privacy; 5. Misure legislative; 6. Conclusioni

Gli oratori che mi hanno preceduto vi hanno già fornito molte informazioni sulle tecnologie Rfid, pertanto cercherò di essere breve. Dopo avere illustrato alcuni elementi fondamentali di questa nuova tecnologia, passerò ad esaminare il quesito “se queste nuove etichette Rfid comportino un trattamento di dati personali”, che è un punto cruciale nell’analisi delle questioni attinenti alla privacy. In considerazione dell’impatto potenzialmente considerevole sulla privacy, esaminerò alcune misure di natura tecnica che non sono state menzionate negli interventi sinora succedutisi. In Europa e negli Usa sono attualmente in discussione interessanti disposizioni normative. Terminerò la mia presentazione ponendo alcuni quesiti fondamentali: non conosco le risposte, ma vorrei quantomeno formulare le domande.

1. Osservazioni generali

Gli aspetti fondamentali sono già stati descritti, almeno in parte. Società private e specialisti in tecnologie affermano talora che le etichette Rfid sono destinate a sostituire i codici a barre. Si tratta di un’applicazione indubbiamente importante. Dov’è il problema, allora? I codici a barre fanno parte della nostra vita ormai da tempo. Perché dovremmo preoccuparci delle etichette Rfid? La ragione è che le etichette Rfid sono decisamente più potenti dei codici a barre. Attualmente sono provviste di una memoria che può arrivare a 124 bit; possono contenere microchip con minuscoli microprocessori ed un sistema operativo. L’emittente (il lettore Rfid) e l’antenna presenti nell’etichetta comunicano per prossimità (senza contatto fisico), e ciò significa che, a differenza dei codici a barre, non occorre effettuare alcuna lettura visiva.

D’altro canto, un’altra differenza sostanziale fra etichette Rfid e codici a barre consiste nel fatto che le prime forniscono un identificatore numerico univoco e leggibile a distanza per ogni singolo oggetto. I codici a barre identificano soltanto categorie di oggetti, ad esempio lamette da barba Gillette, ossia un certo tipo di lametta; viceversa, le etichette Rfid permettono di identificare ogni singola confezione.

(1) Incaricato per la protezione dei dati e l’accesso ai documenti, Land Brandeburgo, Germania.

ne di lamette da barba, ed in futuro forse anche ogni singola lametta.

Una grande catena di supermercati americana, WalMart, ha iniziato un progetto-pilota lo scorso aprile a livello di imballaggi e palette di carico. Si tratta di un'iniziativa ancora di carattere molto generale; l'identificazione si ferma a imballaggi e palette, ma proseguirà giungendo all'identificazione di singoli articoli presenti in magazzino o nella catena distributiva. WalMart ha chiesto ai fornitori di dotare i rispettivi prodotti di etichette Rfid entro il mese di gennaio 2005. Dunque, come si vede, vi sono notevoli pressioni economiche che porteranno all'introduzione della tecnologia in oggetto. Un portavoce di WalMart avrebbe dichiarato che "È così (introducendo la tecnologia Rfid) che riusciremo davvero ad abbassare i costi della gestione del magazzino".

I costi legati all'impiego di questa tecnologia si riducono in misura considerevole. Inizialmente si aggiravano sui 16-20 centesimi di dollaro, oggi sono già diminuiti ed arriveranno a molto meno di 1 centesimo di dollaro nel prossimo futuro. Anche i costi dei lettori Rfid diminuiscono rapidamente. I lettori potrebbero leggere qualsiasi etichetta situata in prossimità fino ad una distanza di 10 metri, e potrebbero essere in grado di leggere simultaneamente 200 etichette al secondo ad una velocità pari anche a 300 km/ora. Sono evidenti, dunque, le grandi potenzialità di questa tecnologia per quanto concerne la raccolta di dati, personali e non (affronterò questo punto fra breve), mentre i risparmi potenzialmente conseguibili dal settore della vendita e distribuzione sono stimati intorno al 20% dei costi legati agli aspetti logistici. Può sembrare poco, ma in termini reali equivale a diversi miliardi di dollari.

Bisogna considerare, inoltre, che i transponder attivi sono in grado di trattare dati, mentre quelli passivi non lo sono in quanto sono privi di un'autonoma fonte di energia. Per esempio, i transponder attivi potrebbero effettuare la cifratura dei dati, il che è un elemento importante – ne parlerò più in dettaglio affrontando il tema delle misure di natura tecnologica. Occorre distinguere fra etichette attive e passive; esistono chip con microprocessori ed etichette prive di microchip. Queste ultime sono ovviamente molto meno costose, ma le altre sono assai più potenti e possono garantire molte più funzioni. Bisogna, inoltre, distinguere fra etichette dotate di microprocessori di sola lettura o di lettura/scrittura; di nuovo, vi sono differenze in termini di costi ed applicazioni. Ad esempio, un'etichetta senza microchip oppure un'etichetta di sola lettura sarebbe sufficiente ed economicamente sostenibile per una società che se ne volesse servire al proprio interno, oppure in un esercizio commerciale di piccole dimensioni o all'interno di un'officina.

2. Applicazioni possibili

Quali sono alcune delle applicazioni possibili? Gestione del magazzino – ne abbiamo già parlato. Monitorare i movimenti di bagagli e container diverrà chiara-

mente più facile utilizzando etichette Rfid. Inoltre, dopo l'11 settembre vari Governi hanno iniziato a prospettare ed attuare programmi finalizzati all'applicazione della tecnologia Rfid ai documenti di viaggio, quali passaporti e visti; probabilmente entro la fine del prossimo anno, o forse entro il 2006, tali documenti comprenderanno dispositivi Rfid.

Vorrei citare le affermazioni compiute di recente da un rappresentante del Governo cinese, a proposito dei progetti governativi relativi all'introduzione di carte di identità recanti etichette Rfid. Questo signore ha affermato che la Cina intendeva rilasciare oltre un miliardo di carte di identità, una per ciascun cittadino. Prevedeva che il fabbisogno annuale di carte del genere sarebbe stato compreso fra 50 e 100 milioni di unità, necessarie per sostituire esemplari danneggiati o per il rilascio di nuove carte di identità ai neonati. Inoltre, ha indicato che sarebbero stati prodotti 3 milioni di lettori Rfid portatili, uno per ciascun funzionario di polizia in Cina. Quando gli è stato chiesto se non vi fossero problemi di privacy, ha affermato senza alcuna incertezza che il Governo non è tenuto a farsi carico di tali problemi, e che in Cina il Governo fa ciò che vuole senza preoccuparsi delle opinioni dei cittadini.

Le affermazioni sopra riportate – come sottolineato dall'articolista – militano chiaramente a sfavore dell'impiego di dispositivi Rfid nelle carte di identità rilasciate dai singoli Governi, salva la previsione di limiti molto rigidi – peraltro assai difficili da monitorare. Carte d'identità di questo tipo non sono ammissibili nei Paesi democratici.⁽²⁾ È un punto di vista che, ritengo, merita di essere preso sul serio.

Un'altra possibile applicazione riguarda le carte di credito o di fidelizzazione, e le banconote. Si è già fatto riferimento alla Banca Centrale Europea ed al progetto di inserire dispositivi Rfid nelle banconote in Euro. Negli Usa è possibile chiedere l'impianto di chip sottocutanei al fine di effettuare pagamenti senza necessità di utilizzare carte di alcun tipo – semplicemente passando per l'area casse; si tratta del progetto noto come "Veripay", anch'esso basato su una tecnologia molto simile. A Monaco di Baviera, i rappresentanti dei Verdi nel consiglio comunale hanno proposto l'introduzione di un sistema di pedaggi per il traffico nel centro urbano fondato sull'impiego della tecnologia Rfid. Un'altra possibile applicazione è connessa alla gestione del parco-macchine.

Altre applicazioni sono state già ricordate da uno degli oratori che mi hanno preceduto per quanto riguarda il settore sanitario. Un ospedale di Singapore, al culmine dell'epidemia di Sars nel 2003, ha assegnato etichette Rfid a tutto il personale ed ai pazienti in modo da individuare, al manifestarsi di un nuovo caso di Sars, i soggetti con i quali la persona infettata aveva avuto contatti così da reagire tempestivamente ed isolare tali soggetti; in casi del genere, le tecnologie Rfid possono risultare di grande utilità. Un'altra applicazione pratica è legata al tracciamento dei

(2) <http://radio.weblogs.com/0121943/2004/04/21.html>

capi di bestiame in relazione al morbo cosiddetto della “mucca pazza”; in questo caso nasce un problema di privacy nel momento in cui si inizia a tenere traccia anche degli allevatori. Lo stesso dicasi per il tracciamento degli animali da compagnia – in Germania esistono norme sui cani potenzialmente pericolosi, le quali prevedono l’impianto di dispositivi Rfid a fini di identificazione e tracciamento.

Anche per le sostanze velenose è possibile ricorrere al tracciamento; ad esempio, il riciclaggio dei personal computer (Pc) costituisce attualmente un problema di grande rilevanza. Con il rapido progredire delle tecnologie sono sempre più numerosi i Pc obsoleti o inutilizzati da riciclare, oppure da sottoporre a revisione; in questi casi, dispositivi Rfid (se già integrati nel Pc in fase di produzione) potrebbero permettere di stabilire se un Pc contenga sostanze velenose in modo da sottoporlo a specifici trattamenti. Si tratta di un’altra delle applicazioni utili e ragionevoli della tecnologia in oggetto.

La miniaturizzazione dei dispositivi Rfid permette di creare la cosiddetta “polvere intelligente” (smart dust): si tratta di microprocessori di dimensioni inferiori ad un granello di sabbia.

Abbiamo già ricordato il caso Benetton. È possibile inserire etichette Rfid su capi di abbigliamento e tessuti, e si tratta di etichette “indossabili” e lavabili. In effetti, è possibile metterle in lavatrice senza causarne il danneggiamento o la distruzione. Mentre chiunque può opporsi all’impianto di chip sottocutanei, che richiede comunque un intervento chirurgico, è molto probabile che non ci si accorga di indossare un microprocessore a contatto della propria epidermide. Così potrebbe capitare – e mi rivolgo ai signori fra il pubblico – che entrando in un negozio d’abbigliamento la commessa vi apostrofi come segue: “Bello il completo di Brioni che indossa, ma perché non indossa anche la biancheria intima coordinata?”. La presenza della biancheria intima è stata individuata grazie alla presenza di dispositivi Rfid – è un esempio che ci mostra quale potrebbe essere la direzione degli sviluppi futuri.⁽³⁾

In questo ambito, i termini che ricorrono continuamente sono informatizzazione pervasiva, e dispositivi “indossabili”.

Dunque, si può ritenere che la tecnologia in questione tratti dati personali? Pongo la domanda perché alcuni amministratori di grandi catene di supermercati contestano tale possibilità, affermando che il tracciamento riguarda soltanto oggetti e prodotti e non le singole persone. È un’affermazione piuttosto miope, perché la tecnologia consente allo stesso momento di tenere traccia anche dei vettori, ossia di coloro che possiedono gli oggetti in questione, ed è qui che entra in gioco la tutela della privacy. Si può avere trattamento di dati personali da parte di dispositivi Rfid anche se questi ultimi sono utilizzati al fine di dimostrare l’autenticità di un prodot-

(3) L'esempio è tratto da Gesellschaft für Informatik, Hintergrundinformationen zur Rfid, <http://www.giev.de/download/Rfid-GI040608.pdf>

to; qui, però, il punto è capire se sia effettivamente necessario trattare dati personali per questo tipo di finalità. Lo stesso dicasi rispetto alla prevenzione della pirateria ed all'etichettatura Rfid di banconote. È possibile prevenire la contraffazione senza trattare alcun dato personale. Già oggi le banconote disponibili presentano numerose caratteristiche finalizzate ad impedirne la contraffazione senza necessità di trattare dati personali. I dispositivi Rfid potrebbero servire agli stessi scopi senza raccogliere necessariamente dati personali.

Si possono immaginare interazioni con vari strumenti di pagamento. Si potrebbero associare etichette Rfid e carte di credito per consentire pagamenti senza necessità di contatto fisico; questa è una delle visioni ottimistiche dei sostenitori della tecnologia, ma in realtà esistono limiti legati alla circostanza che un lettore non è in grado di "leggere" un'etichetta Rfid sepolta sotto una pila di lattine poiché il metallo blocca le onde radio. Dunque, l'idea di pagamenti senza bisogno di contatto fisico incontra limiti di natura tecnica.

Un'altra possibilità consiste nell'interazione fra dispositivi Rfid ed i grandi database per la gestione della clientela ormai costituiti da tutte le maggiori società di vendita al dettaglio. Alcune di queste società giungono ad affermare di avere bisogno dei dispositivi Rfid per adempiere agli obblighi loro imposti dalla legislazione sulla responsabilità per danno da prodotto, oppure al fine di garantire protezione senza soluzioni di continuità – se il consumatore acquista un articolo e lascia il negozio con l'etichetta Rfid ancora attivata, è in grado di ritornare successivamente presso l'esercizio commerciale e sporgere un reclamo per la qualità del prodotto fornito. Attraverso l'etichetta Rfid potrebbe infatti dimostrare di avere acquistato il prodotto presso quello specifico negozio. Pertanto, alcuni rivenditori affermano che è inopportuno disattivare le etichette Rfid una volta che il cliente sia uscito dall'esercizio commerciale. Personalmente non ritengo che sia un approccio corretto, perché esistono numerose possibilità per esercitare i diritti riconosciuti ai consumatori senza essere sottoposti ad un tracciamento permanente attraverso questi dispositivi.

3. Effetti in termini di privacy

Quali sono gli effetti in termini di privacy? È chiaro che l'implementazione delle tecnologie Rfid – una volta risolti vari problemi di natura tecnica, soprattutto in materia di standardizzazione – comporterà la memorizzazione massiva di dati potenzialmente personali. Le etichette Rfid diverranno un componente-chiave di quella che viene definita "informazione d'ambiente". Si potrebbe effettuare la profilazione dei consumatori su scala sinora mai contemplata, potenzialmente giungendo a condizionare i comportamenti del singolo consumatore.

Le tecnologie sinora descritte sono invisibili e trasparenti, dunque tendono a

suscitare diffidenza in quanto cittadini e consumatori non sono in grado di sapere né di seguire con precisione quanto stia avvenendo rispetto ad un determinato prodotto; spesso non si rendono neppure conto che l'articolo da loro acquistato reca un'etichetta, a meno che quest'ultima sia segnalata in modo ben visibile.

È possibile tenere traccia degli spostamenti di singoli oggetti esattamente come degli spostamenti di coloro che ne sono in possesso. E che dire, allora, dei diritti riconosciuti agli interessati? Come faranno le persone i cui dati sono oggetto di trattamento attraverso questi dispositivi ad esercitare realmente il diritto di sapere quali siano i dati in questione? Come farò a stabilire se i dati sono corretti, e potrò rettificarli o cancellarli se necessario? Sono quesiti fondamentali in termini di privacy, ed in ultima analisi si può affermare – con tutte le dovute cautele – che l'avvento della tecnologia Rfid rende sempre più probabile e possibile la creazione di un'infrastruttura della sorveglianza.

4. Progettazione finalizzata al potenziamento della privacy

Cosa si può fare per impedire la graduale definizione di un'infrastruttura del genere descritto? In primo luogo, progettare le tecnologie in modo da potenziare la tutela della privacy. Quali sono le misure di natura tecnica utili al fine di ottenere un potenziamento della privacy? Una misura immediata potrebbe consistere nel garantire la visibilità dei dispositivi Rfid attraverso ausili tecnici, cosa che normalmente non avviene. In realtà, sono proprio le dimensioni contenute e la crescente miniaturizzazione di tali dispositivi ad impedirne l'evidenziazione. Lo stesso vale per il lettore e per l'intero procedimento di scansione/lettura. Anche quest'ultimo è invisibile, visto che utilizza le frequenze radio. Un modo per raggiungere questo importante obiettivo, ossia dare visibilità a questa categoria di trattamenti, potrebbe consistere nella definizione di standard internazionali. Tuttavia, sinora non mi constano tentativi da parte di organismi di normazione (nazionali o internazionali) finalizzati ad affrontare questo o altri problemi connessi alla progettazione dei dispositivi Rfid secondo modalità tali da potenziare la tutela della privacy.

Potenziare l'usabilità e la leggibilità delle etichette Rfid, magari dando all'interessato anche la possibilità di correggere o cancellare i dati, risolverebbe una parte dei problemi evidenziati per quanto riguarda la necessità di garantire agli interessati l'esercizio dei loro diritti. In terzo luogo, un punto critico attualmente all'esame della comunità scientifica è il seguente: davvero è sufficiente definire una procedura che consenta l'annientamento o la disattivazione delle etichette nel punto-vendita, per esempio attraverso dispositivi di blocco o altri approcci? Non c'è forse un problema di privacy se il cliente/consumatore viene monitorato e seguito anche all'interno del negozio, prima che l'etichetta sia disattivata? E chi ha la responsabilità di innescare e

controllare la procedura di disattivazione? Davvero il consumatore deve fidarsi del negoziante/esercente che affermi di disattivare etichette invisibili presenti sugli articoli in vendita al momento del passaggio alle casse, utilizzando una “scatola nera”?

Infine, è possibile annullare gli effetti della procedura di disattivazione? Si possono riattivare etichette, come dire, “dormienti”? Se così fosse, le si potrebbe riattivare in un momento successivo, o magari qualcun altro potrebbe farlo (ad esempio, il Governo) per sfruttarne il potenziale di tracciamento a fini ignoti.

5. Misure legislative

Pari importanza rivestono le misure di natura legislativa. Nel mio Paese, la Germania, è in corso un dibattito su alcune tematiche; la Legge federale sulla protezione dei dati⁽⁴⁾ contiene, infatti, una disposizione concernente le smart card (“supporti mobili di memorizzazione”). Ci si è chiesti se tale disposizione sia sufficiente a gestire le problematiche appena descritte in rapporto ai dispositivi Rfid, i quali sono anch’essi, in fondo, supporti mobili di memorizzazione. Personalmente non credo che la legislazione attuale sia sufficiente; inoltre, essa appare troppo limitata, in quanto prevede soltanto obblighi di trasparenza ed informazione – che però non sono sufficienti, come cercherò di dimostrare fra breve.

È in gioco, inoltre, la riservatezza delle telecomunicazioni. La comunicazione che avviene fra etichetta e lettore è una telecomunicazione; pertanto, si applica il principio di riservatezza delle telecomunicazioni, che deve essere tutelato. Una soluzione immediata a tale problema potrebbe consistere nella cifratura dei dati. Come affermato dal senatore americano Patrick Leahy in un suo intervento a Washington, D.C., “Forse siamo pronti ad accettare che il Pentagono possa gestire le forniture utilizzando etichette Rfid, ma di sicuro non vogliamo che un membro di Al-Qaeda entri in possesso di informazioni sulle nostre dotazioni utilizzando un semplice lettore Rfid in un contesto bellico”.⁽⁵⁾ Anche qualche pirata informatico potrebbe attaccare, leggere e manipolare le etichette utilizzate in un esercizio commerciale per modificare i prezzi e poi andarsene sfruttando i meccanismi di pagamento automatico.

Si tratta di un problema cruciale in termini di sicurezza dei dati: come tutelare in modo efficace le comunicazioni fra etichette e lettori Rfid. La cifratura costituisce la soluzione più immediata, tuttavia essa richiede l’impiego di etichette più sofisticate e costose che possono essere accettabili in un contesto militare, ma difficilmente saranno utilizzate per le confezioni di formaggini in una drogheria.⁽⁶⁾

(4) Art. 6(c) del Bundesdatenschutzgesetz, 23 maggio 2001.

(5) <http://www.rfidjournal.com/article/view/843>

(6) Rfid Tags Become Hacker Target, [Le etichette Rfid diventano bersagli per gli hacker] http://news.com.com/2102-1029_3-5287912.html?tag/

Tuttavia, quanto affermato dal Prof. Rodotà e da altri oratori ha veramente un'importanza fondamentale. Prima di introdurre una tecnologia che raccoglie dati in modo automatico, dobbiamo chiederci quale ne sia l'utilità; altrimenti abbiamo un problema sostanziale. Pertanto, è necessario insistere sul principio di necessità dei dati, o di parsimonia nell'uso dei dati, ovvero, in primo luogo, sull'esigenza di evitare l'utilizzazione di dati personali – per non essere costretti, poi, ad affrontare il problema della gestione della mole di informazioni personali che, in alcune circostanze specifiche, risulta necessario raccogliere. Ma è essenziale porre il quesito dell'effettiva necessità di utilizzare dati personali. Ed in moltissimi casi tale necessità non sussiste, come ad esempio per quanto riguarda l'organizzazione logistica o l'inventariazione. Parsimonia nell'uso dei dati e rispetto del principio di necessità dovrebbero far parte, pertanto, del contesto giuridico di riferimento così come avviene attualmente in Italia ed in Germania.

Infine, bisogna considerare la possibilità di bandire per legge l'utilizzazione di etichette Rfid, almeno in alcuni casi specifici o per specifiche finalità. Se, ad esempio, si ricorresse a dispositivi Rfid per seguire gli spostamenti di singole persone oppure per eliminare l'anonimato, a quel punto dovremmo senz'altro erigere una barriera giuridica atta a contrastare prassi del genere.

Per esempio, la Banca Centrale Europea sta pensando di introdurre etichette Rfid nelle banconote in Euro. È un proposito perfettamente legittimo se è finalizzato a prevenire le falsificazioni, ma non dovrebbe eliminare la possibilità di pagare fatture e spendere denaro in forma anonima nel mondo reale, perché qualunque banconota recante dispositivi Rfid potrebbe monitorare e identificare le modalità del suo utilizzo. E qui si andrebbe a travalicare un confine cruciale e decisivo.

In questo ambito, anche gli interventi normativi talora possono risultare controproducenti. Un esempio recente è dato dalla proposta di Direttiva della Commissione europea sulle misure finalizzate a dare attuazione ai diritti di proprietà intellettuale. In base al testo iniziale della proposta, sarebbe stato configurato come reato penale ogni intervento finalizzato a sottrarsi agli effetti di dispositivi tecnici atti a tutelare diritti di proprietà intellettuale o marchi di fabbrica – compresi i dispositivi Rfid. Tale disposizione avrebbe comportato la trasformazione in reato di qualsiasi tentativo di bloccare il funzionamento di etichette Rfid lesive della privacy individuale. Per fortuna la proposta è stata emendata all'interno del Consiglio grazie alla forte opposizione manifestata dalle Autorità europee per la protezione dei dati personali, e la disposizione in oggetto è stata eliminata.⁽⁷⁾ La precedente Direttiva sull'armonizzazione del diritto d'autore nella società dell'informazione⁽⁸⁾ conteneva una disposizione analoga, ma di più ampio respiro, che

(7) Direttiva 2004/48/CE..

(8) Direttiva 2001/29/CE, Art. 6(1).

vietava interventi atti a sottrarsi agli effetti di dispositivi tecnici di protezione.

Una misura legislativa che merita di essere presa in considerazione per quanto riguarda la tecnologia Rfid è il diritto dell'acquirente di far eliminare o distruggere l'etichetta; in ogni caso, è necessario garantire il diritto di accedere ai dati contenuti nel sistema nel suo complesso (etichette e lettori). Sono misure di natura giuridica che è opportuno adottare. Ho trovato molto interessante quanto detto dal Prof. Decina stamani rispetto alla proposta giapponese di inserire una sorta di "lucchetto" personale sulle etichette Rfid – avevo formulato un'idea identica in chiave giuridica, ossia il principio per cui l'interessato, in ultima analisi, dovrebbe avere il diritto di innescare e monitorare la comunicazione fra etichette e lettori. Anche questo diritto deve essere garantito per legge.

Negli Stati Uniti, cinque Stati hanno già discusso ed adottato, almeno in parte, provvedimenti-quadro relativi all'utilizzazione di tecnologie Rfid. Progetti di legge presentati nel Maryland, nel Missouri e nello Utah hanno sollecitato l'impiego di etichette Rfid chiaramente visibili per consentire a consumatori ed interessati di prenderne conoscenza.⁽⁹⁾ Tali proposte riprendono un'idea formulata originariamente da Simson Garfinkel, che aveva auspicato una Carta dei Diritti per l'Rfid.⁽¹⁰⁾ Lo stato della Virginia sta valutando una riconsiderazione generale delle prassi legate all'impiego di tecnologie Rfid nell'ottica della privacy. Il disegno di legge presentato dalla Senatrice Bowen della California⁽¹¹⁾ è più ambizioso, in quanto prevede che sia lecito utilizzare le etichette Rfid solo in alcune specifiche circostanze – all'interno di esercizi commerciali e biblioteche, e sulla base di rigidi criteri di finalità. Questo approccio presenta, in realtà, alcuni problemi, in particolare la definizione dell'arco temporale di liceità; citando il disegno di legge, "È vietato l'impiego di etichette Rfid prima che il cliente dia effettivo inizio ad una operazione/transazione, ovvero prima che un soggetto chieda effettivamente in prestito un elemento del posseduto di una biblioteca, nonché successivamente al completamento dell'operazione/della transazione. Nelle circostanze descritte, l'impiego di etichette Rfid dovrebbe essere vietato". È chiaro, però, che non è facile definire in un'ottica giuridica quando un cliente dia effettivamente inizio ad un'operazione/transazione.

(9) V., per ulteriori particolari, la Dichiarazione resa da EPIC dinanzi alla Sottocommissione per il commercio, gli scambi e la tutela dei consumatori della Commissione del Congresso per l'energia ed il commercio, 14 luglio 2004, <http://www.epic.org/privacy/rfid>.

(10) http://www.simson.net/clips/2002.TR.10.Rfid_Bill_Of_Rights.pdf; v. anche CASPIAN, The Rfid Right to Know Act of 2003, all'indirizzo <http://www.nocards.org/rfid/rfidbills.html>

(11) http://info.sen.ca.gov/pub/bill/sen/sb_1801-1850/sb_1834_bill_20040401_amended_sen.pdf

6. Conclusioni

Avviandomi a concludere, vorrei porre due domande fondamentali. La prima è la seguente: il legislatore deve attendere che una tecnologia sia “matura” (qualsiasi cosa ciò significhi), oppure giocare d’anticipo? Personalmente, per rispondere a questa domanda, sono fermamente convinto che sia necessario giocare d’anticipo, essere “proattivi”; anzi, il termine “provvedere” esprime alla lettera questo concetto. Ciascun legislatore deve adottare alcune precauzioni per essere in grado di gestire gli sviluppi tecnologici del futuro.

C’è poi una seconda domanda ancora più fondamentale. È possibile mantenere l’autonomia dell’individuo, nell’era digitale, dinanzi all’affermarsi delle tecnologie intelligenti d’ambiente? È un quesito tuttora aperto, ma sono convinto che se non ci misuriamo con questo problema delle tecnologie Rfid, e se non sviluppiamo un efficace contesto tecnico e giuridico di riferimento, la risposta potrebbe anche essere “No”.

Vorrei concludere citando dalla Relazione presentata dalla collega Ann Cavoukian dello Stato di Ontario, in Canada, la quale ha scritto molto giustamente che “Le transazioni supportate da strumenti tecnologici o il commercio elettronico non dovrebbero comportare un baratto, per cui i consumatori rinunciano a porzioni sempre più consistenti della loro privacy in cambio di maggiori comodità. In ultima analisi, si tratta di dare effettivi poteri ai consumatori e di generare in loro fiducia”. E, aggiungerei, si tratta di *dare effettivi poteri ai cittadini e di generare in loro fiducia*. La Cavoukian prosegue affermando che “Le aziende che utilizzano dispositivi Rfid devono avere le idee chiare ed applicare con rigore prassi concernenti la disattivazione dei meccanismi di tracciamento, perché disporre di una struttura di produzione e distribuzione efficiente in termini di costi sarebbe praticamente inutile se poi nessuno si fida di un’azienda abbastanza da acquistarne i prodotti. In parole povere, tutelare la privacy fa bene agli affari.”

E, permettetemi di aggiungere, fa molto bene ad una società e ad un governo democratici.

Vi ringrazio.

RFID technology – new challenges to privacy

Dr. Alexander Dix, LL.M.



Landesbeauftragter für den
Datenschutz und für das
Recht auf Akteneinsicht
Brandenburg

Agenda

- **Basic facts**
- **RFID processing personal data ?**
- **Effects on privacy**
- **Technical measures**
- **Legislative measures in Europe and the US**
- **Basic Questions**



Landesbeauftragter
für den Datenschutz
und für Das Recht auf
Akteneinsicht
Brandenburg

2

Basic facts

- **Radio Frequency Identification tags will replace barcodes - so what ?**
- **Considerably more powerful than barcodes
memory up to 100 Bits
no need for line-of-sight reading**
- **Remote readable unique ID numbers**
- **Active transponders can process
(e.g. encrypt) data**



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

3

Types of RFID systems

- **Passive/active tags**
- **Tags with chips
(processors)/chipless tags**
- **Read-only and read-write chip tags**



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

4

Some possible applications (1)

- Logistics, inventories
- Baggage, container tracing
- Travel documents, passports, tickets
- Credit or loyalty cards, banknotes, subdermal chips (Veripay)
- Road pricing (Munich), Fleet management



Landesbeauftragter
für den Datenschutz
und für Das Recht auf
Akteneinsicht
Brandenburg

5

Some possible applications (2)

- Fighting infectious human diseases (e.g. SARS)
- Tracking cattle (mad cow disease) or other animals (pets)
- Tagging of poisonous substances, nanoparticles („smart dust“)



Landesbeauftragter
für den Datenschutz
und für Das Recht auf
Akteneinsicht
Brandenburg

6

„Wearable Computers“

- RFID tags may be integrated in clothes and fabrics (Benetton)
- They are wearable and washable
- We may resist subdermal chips but we will not notice that we wear processors on our skin
- Pervasive, ubiquitous computing



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

7

Processing personal data ? (1)

- **Identification, location and tracing of objects**
- **Proof of authenticity, prevention of product piracy**
- **Prevention of counterfeiting, money laundering**



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

8

Processing personal data ? (2)

- **Link with means of payment (credit cards) for contactless check-out**
- **Link with Customer Relations Management**
- **Product liability, consumer protection**
- **Passports, travel documents, tickets**



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

9

Effects on privacy

- Massive storage of potentially personal data, creation of consumer profiles, steering consumer behaviour
- Invisible and intransparent technology
- Movements of tagged objects and their holders/owners could become traceable
- Data subject's rights ?
- Infrastructure of surveillance possible



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

10

Technical measures for privacy-enhancing design

- **Visibility (marking) of RFID tags, readers and the reading process**
- **User-friendly, easy readability and possibility to correct/(erase ?) data for the data subject**
- **Is „killing“ or de-activating tags at points of sale enough ? Who controls it ? Can it be reversed („sleeping“ tags) ?**



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

11

Possible legislative measures (1)

- **Are rules on smartcards applicable and sufficient ?**
- **Does telecommunications secrecy apply to the communications between tag and reader ?**
If yes, encryption is necessary
- **Prevention of personalization, data scarcity**
- **Ban on RFID tags in specific situations or for certain purposes (to track people, to reduce anonymity)**



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

12

Possible legislative measures (2)

- **Buyer's right to have the tag removed or destroyed**
- **Right to inspect the data in the tag and the entire system (readers and linked communications systems)**
- **Data subject's right to initiate and control the reading of tags**



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

13

Counter-productive legislation (1)

- Directive 2004/48/EC on Enforcement of Intellectual Property Rights
- Commission had proposed to make it a criminal offence to circumvent any technical device to protect IP rights (including RFID tags)



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

14

Counter-productive legislation (1)

- Directive 2004/48/EC on Enforcement of Intellectual Property Rights
- Commission had proposed to make it a criminal offence to circumvent any technical device to protect IP rights (including RFID tags)



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

14

Counter-productive legislation (2)

- This would have led to the criminalisation of blocking privacy-invasive RFID tags
- Fortunately due to the opposition from DP Commissioners this provision was deleted
- But Directive 2001/29/EC contains a similar provision against the circumvention of protection devices



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

1

Legislative measures in the US (1)

- RFID Right to Know Bills in Utah and Missouri
- Sen. Bowen's Bill on RFID systems (California) passed the Senate (now in the Assembly)
- Sen. Leahy called for a national debate („the train is leaving...”)



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

16

Legislative measures in the US (2)

- Right to Know Bills provide only for transparency
- Bowen's Bill more ambitious:
RFID tags may only be used under conditions (lawfully collected information, purpose limitation, only in shops and libraries)



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

17

Legislative measures in the US (3)

- Legislative problems: how to describe the admissible time-span ?
- Bowen's Bill: RFID tags forbidden „before a customer *actually* initiates a transaction or a borrower *actually* attempts to borrow an item...and after the transaction is completed...”



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

18

Basic questions

- 1. Should legislators wait until a technology is „mature” or should they behave proactively („make provisions”) ?**
- 2. Can individual autonomy in the digital age (in the face of ambient intelligence technologies) be maintained ?**



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

19

Contact: Dix@LDA.brandenburg.de

- **Resolution of the 25th International Privacy Commissioners' Conference**
<http://www.privacyconference2003.org/resolutions/res5.doc>
- **Security and privacy in the Post-September 11 Digital Age (EU Commission Joint Research Centre)**
<http://www.jrc.es/home/publications/publication.cfm?pub=1118>
- <http://www.epic.org/privacy/rfid>
- <http://www.privacyrights.org/ar/RFIDposition.htm>



Landesbeauftragter
für den Datenschutz
und für das Recht auf
Akteneinsicht
Brandenburg

20

Alexander Dix⁽¹⁾

Contents: 1. Basic observation; 2. Possible applications; 3. Effects on privacy; 4. Privacy enhancing design; 5. Legislative measures; 6. Conclusions.

A lot of information has already been given to you on Rfid by previous speakers, so I will try to be brief. After giving you some basic facts about this new technology, I will turn to the question “Are these new Rfid tags processing personal data at all?”, which is a crucial question when discussing matters of privacy. In view of the potentially far-reaching effects on privacy I will talk about some technical measures which have not been dealt with so far in the previous presentations. In Europe and in the United States interesting legislative measures are under discussion right now. And then I will end with some basic questions. I may not have the answers, but at least I will formulate such questions.

1. Basic observations

Now the basic facts have already been described in part. Private companies and technologists sometimes say that radio frequency identification tags will simply replace bar codes. This is one very important application. So what is the problem? We have lived with bar codes for a long time. Why should we worry about Rfid tags? The reason for that is that Rfid tags are considerably more powerful than bar codes. They have a memory of up to 124 bits at present. They may include computer chips with tiny microprocessors and an operating system. The sender (Rfid reader) and the antenna in the tag communicate with each other contactless, which means that – unlike with bar codes – there is no need for line-of-sight reading.

On the other hand another basic difference between Rfid tags and bar codes is that Rfid tags provide for a remote, readable unique Id number for each individual object. Bar codes have only identified types of objects, e.g. Gillette razor blades, a certain type of razor blade, while Rfid tags are identifying every single parcel of those razor blades, and maybe in the future each individual razor blade.

WalMart, the great Us supermarket chain, started a pilot project in April of this year on the case and pallet level. That is very much on a general level still: they are only identifying cases and pallets, but they will go on to identify individual items in

(1) Landesbeauftragter für den Datenschutz und für Das Recht auf Akteneinsicht Brandenburg

their stores and their supply chain, and they have required their suppliers to arm their products with Rfid by January of next year. So as you can see, there is considerable economic pressure which will lead to the introduction of this technology. A spokesman for WalMart is reported to have said: "This (by introducing Rfid technology) is how we're really going to drive costs out of the inventory process."

The prices for this technology are decreasing considerably. They started off at 16 to 20 US cents, they have come down already, and will go well below the level of 1 US cent in the near future. The costs of readers are also decreasing rapidly. Readers could read any tags in their vicinity up to ten metres, and 200 tags per second could be read simultaneously at a speed of up to 300 kilometres per hour. So you can see the considerable power of this technology in collecting data: personal or not personal – I will be considering that point in a very short time – while the possible savings for the retail industry are estimated at 20% of the cost of logistics – that may sound not very much, but in real terms it means several billions of dollars at stake.

One also has to see that active transponders can process data, while passive transponders cannot, because they do not have their own energy supply. Active transponders could for instance encrypt data, which is important – I will come back to this when I speak about technological measures. One has to differentiate between passive and active tags: there are chips with processors and also chipless tags. Chipless tags are of course much less expensive than tags with chips, but the tags with microprocessors are more powerful and can fulfil more tasks. Also, one can distinguish between read only and read-write chip tags. There again, there are differences in costs and applications. For instance, a chipless tag or a read-only tag would be enough and affordable for a company for their internal use, within a small shop or on the shop floor.

2. Possible applications

What are some of the possible applications? Logistics inventories –I have talked about that. Baggage and container tracing will obviously be much easier with Rfid tags. And then, after September 11th, governments have started to introduce and plan for arming travel documents: passports and visa: they will have Rfid technology included probably by the end of next year, maybe by 2006.

I would quote one representative of the Chinese Government who recently described the plans of the Chinese Government to introduce Id cards with Rfid tags. He indicated that China would issue over one billion cards, one for each citizen. He expects that further annual consumption will be between 50 million and 100 million cards, as damaged cards are replaced and new cards are issued to newborn children. Going further, he said that 3 million hand-held Rfid readers would be issued,

one for each police officer in China. When asked if this would provoke privacy concerns, he clearly stated that the government does not need to respond to such concerns, and that in China the government does what it wants to despite the opinions of its citizens!

These comments, as the commentator said, offer a crystal-clear case against Rfid in government-issued identity cards unless their usage is very carefully restricted, and the restrictions are very difficult to monitor. Such cards have no place in a democracy⁽²⁾. That is an opinion that should be taken seriously, I think.

Further applications are credit or loyalty cards, bank notes. The European Central Bank has already been mentioned, with their plans to include Rfid in Euro bank notes. In the United States, persons can have chips implanted under their skin to make payments without using any cards but just passing by the check-out point - this is what is known as the Veripay project, which also relies on a very similar technology. And in the City of Munich the Green members of the City Council have proposed the introduction of a road pricing or toll scheme within the city limits, relying on Rfid technology. The management of fleets is again another possible application.

Some more applications have already been mentioned by one of the previous speakers in the area of health. A hospital in Singapore at the height of the Sars epidemic last year gave Rfid tags to all its staff and patients, to find out when a new case of Sars came up, with whom the infected person had been in contact, in order to quickly react and isolate those contact persons – so that Rfid can be very useful in such circumstances. Tracking cattle in the case of the Mad Cow disease is another practical application. This involves a privacy problem, once you start tracking the farmers. Or tracking animals and pets – there is legislation in force in Germany about dangerous dogs, which have to be implanted in some States with Rfid tags in order to detect and track them.

Poisonous substances could be tracked as well, for instance recycling of PCs is now a major problem. With the speed of technological development, a lot of disused or old PCs are recycled, or they may have to be taken care of – and then Rfid technology (if it was integrated in the computer on the production line) could find out if these PCs contain poisonous substances, so that they could be treated differently – this is another possible useful and sensible application for them.

The miniaturization of Rfid tags leads to what has been called “smart dust”: microprocessors smaller than a grain of sand.

The example of Benetton has already been mentioned: Rfid tags can be integrated into clothes and fabrics, and they are wearable as well as washable: you could actually put them into the washing-machine and they will not be damaged or destroyed. Whereas everybody can resist having subdermal chips being inserted into

(2) <http://radio.weblogs.com/0121943/2004/04/21.html>

his body, because this requires surgery, you may quite possibly not notice that you are wearing a processor on your skin. So when male members of the audience enter a clothing store, the shopkeeper might in the future address you as follows: “You are wearing a very nice Brioni suit, but why don’t you wear the fitting underwear?” The underwear has been detected as well, since it is armed with Rfid tags – this example shows us in what direction developments might go⁽³⁾.

“Wearable”, pervasive and *ubiquitous computing* are the buzz-words in this context.

Now, is this technology processing personal data? I am putting this question, since some chief executives of supermarkets are disputing this. They claim that they are only tracking objects and products, not people. This is somewhat short-sighted, because the technology is able at the same time to track the carriers, the possessors of these objects, and that is where privacy protection comes into play. Personal data can also be processed by Rfid tags if authenticity has to be proven. But here the question is whether it is really necessary to process personal data for that purpose. The same is true for the prevention of product piracy and the case of tagging bank notes. The prevention of counterfeiting could be tackled without processing personal data at all. There are numerous features in our currency bank notes already today which are intended to prevent counterfeiting without processing any personal data. Rfid tags could serve the same purpose without necessarily collecting personal data.

There can be links with means of payment. Rfid tags could be linked with credit cards for contactless check-out. This is one of the optimistic visions the proponents of this technology have, although there are limits to this possibility, because Rfid tags cannot be read by readers if they are buried among a pile of tins or cans (because metal blocks radio waves). So there are technical limits to this vision of contactless cheque-out.

Rfid tags may be linked with large customer relations management data bases that each big retail company nowadays holds about its customers. Some companies even argue that they need the Rfid tags in order to fulfil their duties under the product liability laws or for continual protection, because if the consumer has bought an item and leaves the store with an Rfid tag still activated, he may be able to come back to the store later on and complain about the quality of the product. He could then prove via the Rfid tag that the product was sold in that store. Therefore some retailers say that Rfid tags should not be de-activated once the customer has left the store. I think that this is not the right approach since there are various ways of exercising your rights as a consumer without being permanently tracked by such a device.

(3) Example quoted from: Gesellschaft für Informatik, Hintergrundinformationen zu Rfid, <http://www.gi-ev.de/download/Rfid-GI040608.pdf>

3. Effects on privacy

What are the effects on privacy? It is obvious that the deployment of Rfid technology – once a number of technical problems, particularly standardization issues, have been solved – will lead to a massive storage of potentially personal data. Rfid tags will become a central element of “ambient intelligence”. Consumer profiles could be created on a scale unknown so far, and it could even lead to the steering of consumer behaviour.

The whole technology described thus far is invisible and transparent, therefore it is prone to create distrust, because citizens and consumers cannot know nor exactly follow what is happening in an item –very often they do not even realise there are tags on an item which they bought, if it is not marked in a clearly visible manner.

Movements of objects can be traced just as well as the movements of their holders and owners. And what about the data subject’s rights? How can the individual persons whose data are processed by this technology actually exercise their rights to know what kind of data are processed? How can I find out if the data are correct and can I correct or erase them if necessary? These are obvious privacy issues, and in the end, one can – with all due restraint - say that an infrastructure of surveillance becomes more and more likely and possible with the advent of this technology.

4. Privacy enhancing design

What can be done to prevent the gradual creation of such an infrastructure? First of all technology should be designed in a privacy enhancing way. What are possible technical measures for a privacy enhancing design? One obvious measure to take would be to technically ensure the visibility of Rfid tags which is normally not guaranteed. Indeed the very minuteness and increasing miniaturization of tags prevents their discovery. The same applies to readers and the whole reading process. The reading processes, which is wireless, is invisible again. One way to achieve this important aim to create visibility of this kind of data processing could be international standardisation. However, so far I have not seen any attempts by standards bodies – national or international – to tackle this or any other problems to design Rfid technology in a privacy enhancing fashion.

User friendliness and easy readability of the tags, and even creating the possibility of correcting or erasing data for the data subject, would solve some of the problems I have just mentioned about ensuring the exercise of data subject’s rights. And, thirdly, a critical question that is being discussed at the moment in the scientific community is this: Is it really enough to arrive at a process, maybe by blocker tags or other technology, to kill or de-activate the tags at the sale point? Is it not a privacy problem if the customer and consumer is observed and followed even in the

store, before the tag is de-activated. And who initiates and controls the de-activating process? Can the customer really trust the shop-owner who claims to de-activate invisible tags on items at the checkout in a “black box”.

And, finally, can this process of de-activation be reversed? Could tags be re-awakened, as it were: if they were only put to sleep, you could re-awaken them at a later stage, or someone else (e.g. government) could re-awaken them to make use of their tracking capabilities for unknown purposes.

5. Legislative measures

Legislative measures are equally important. There are certain questions at present being discussed in my own country, Germany, where we have a provision of the Federal Data Protection Act⁽⁴⁾ governing smart-cards (mobile storage devices). The question has been raised whether this provision is sufficient to deal with the problems I have just described regarding Rfid tags, because after all in the end these are mobile storage devices as well. I personally believe that this is not enough. The provisions are also too limited, they only provide for transparency and information, but that is not enough as I will show in a minute.

Furthermore telecommunications secrecy is at stake here. The communication between the tag and the reader is telecommunications. Therefore the principle of telecommunications secrecy applies to this communication, and it has to be protected. Encryption would be an obvious solution for that. Senator Patrick Leahy said in a presentation in Washington, D.C., “While we might want the Pentagon to be able to manage its supplies with Rfid tags, we would not want an al Qaeda operative to find out about our resources by simply using a hidden Rfid scanner in a war situation.”⁽⁵⁾ Hackers could likewise attack, read and manipulate the tags used in a shop to change prices and walk out through self checkout.

This is a crucial data security problem how any communication between tags and readers can be effectively protected. Encryption is the obvious solution but this requires more sophisticated and more expensive tags which may be used in the military context but are unlikely to be put on cream cheese boxes in a grocery store⁽⁶⁾.

However, what Prof. Rodotà and others have said, is really fundamental. Before we introduce a technology which collects personal data automatically without asking what it is needed for, we have a basic problem. Therefore we have to insist on the principle of data minimisation, data scarcity, or the prevention of personalisation in the first place, before we then later on tackle the problem of how to deal with the

(4) § 6c Bundesdatenschutzgesetz v. 23. Mai 2001

(5) <http://www.rfidjournal.com/article/view/843>

(6) Rfid tags become hacker target <http://news.com.com/2102-1029_3-5287912.html?tag/>

amount of personal data that has inevitably to be collected in certain specific instances. But first of all we have to put the question, whether personalisation is really necessary. And in very many cases it is not, for instance, for the purpose of organising logistics or making an inventory. Data scarcity and data minimisation therefore should be part of the legal framework as it is the case in Italy and Germany.

Finally one has to think about the idea of even banning by law Rfid tags, at least in certain specific situations or for certain purposes. For example, if Rfid tags were to be used to track people or to eliminate the principle of anonymity, then we would certainly have to erect a certain legal barrier against such practices.

For instance, the European Central Bank is thinking about introducing Rfid tags into Euro bank notes. That is all very well if it is aimed at preventing counterfeiting, but it should not replace the possibility to pay bills and dispense money anonymously in the real world, because any bank note with integrated Rfid technology could actually track and observe what I am doing with this money. There we are crossing a crucial and decisive border.

Regulations in this context can also have a counterproductive effect on privacy. A recent example for this was the proposal by the European Commission for a Directive on enforcement of intellectual property rights. According to the original proposal it would have been a criminal offence to circumvent any technical device to protect intellectual property rights or trademarks including Rfid tags. This would have led to the criminalisation of any attempt to block privacy-invasive Rfid tags. Fortunately the draft was amended in the Council due to strong opposition by European Data Protection Commissioners and the relevant provision was deleted⁽⁷⁾. The previous Directive on the harmonisation of copyright in the information society⁽⁸⁾ contains a similar - but broader - provision against circumvention of technical protection devices.

A positive legislative measure that should be discussed with regard to Rfid technology is the buyer's right to have the tag removed or destroyed; the right to inspect the data in the entire system (tags and readers) should at any rate be guaranteed. These are all legal measures which should be taken. I found it very interesting what Prof. Decina said this morning about the Japanese technical proposal of a personal lock on Rfid tags – I had the same idea on a legal basis: eventually the data subject should have the right to initiate and control the communication between tags and readers. That has also to be secured by law.

In the United States five state legislatures have already discussed and partly adopted legal frameworks for the use of Rfid technology. Bills in the States of Maryland, Missouri, Utah have called for Rfid tags to be conspicuously labeled to

(7) Directive 2004/48/EC

(8) Directive 2001/29/EC, Art. 6 (1)

become visible to the consumers and data subjects;⁽⁹⁾. This takes up an idea first formulated by Simson Garfinkel who called for a Rfid Bill of Rights⁽¹⁰⁾. Virginia is considering as general review of Rfid practices and privacy. Senator Bowen's bill in California⁽¹¹⁾ is more ambitious. Under her bill, tags may only be used in certain specified conditions, namely in shops and libraries, and there is a strict purpose limitation on the use of these tags. Now, this approach does present a certain problem, namely how to describe the admissible time span - and I quote from her bill, which says, "Rfid tags are forbidden before a customer actually initiates a transaction, or a borrower in a library actually attempts to borrow an item, and after the transaction is completed. In these situations tags should be banned". But there you can see the legal problems of how to specify when does a customer actually initiate a transaction.

6. Conclusions

Coming to my conclusions, I want to put two basic questions. The first question is: Should legislators really wait until a technology is "mature" (whenever that may be)? Or should they behave proactively? I personally - to give the answer - firmly believe that they must behave proactively, in fact the English words "to make provisions" literally describes this process. Any Parliament has to take precautions in order to cope with technological developments of the future.

Secondly, a more fundamental question: Can individual autonomy, in the digital age, in the face of ambient intelligent technologies be maintained? This question is an open one, but I believe that, unless we tackle this problem of Rfid technology, and unless we set up an effective technological and legal framework, the answer to this question could possibly be: No.

I want to finalise by quoting a report by my colleague from Ontario, Dr. Ann Cavoukian⁽¹²⁾, who very aptly wrote: "Technology-driven transactions or e-commerce should not involve a trade-off, in which consumers relinquish widening amounts of their privacy in return for greater convenience. Ultimately the issue comes down to consumer empowerment and trust". And - I would add - to *citizens' empowerment and trust*. Dr. Cavoukian continues: "Companies rolling out Rfid must have a clear idea and rigidly enforced policy on the de-activation of their

(9) See Testimony and Statement by EPIC before the Subcommittee on Commerce, Trade and Consumer Protection of the House Committee on Energy and Commerce of July 14, 2004, <http://www.epic.org/privacy/rfid/> for further references

(10) http://www.simson.net/clips/2002.TR.10.Rfid_Bill_Of_Rights.pdf; see also CASPIAN, The Rfid Right to Know Act of 2003 at <http://www.nocards.org/rfid/rfidbill.shtml>

(11) http://info.sen.ca.gov/pub/bill/sen/sb_1801-1850/sb_1834_bill_20040401_amended_sen.pdf

(12) Information and Privacy Commissioner/Ontario, Tag, You're It: Privacy Implications of Radio Frequency Identification (Rfid) Technology, <http://www.ipc.on.ca/docs/rfid.pdf>

tracking mechanisms, as having a cost-effective supply chain would be pretty meaningless if nobody trusts you enough to buy from you at all. Simply put, privacy protection is good for business.”

And – I would add – it is very good for a democratic government and society.

Thank you very much.

Mario Savastano⁽¹⁾

Gentilissimi ospiti, nel ringraziare il Garante per la Protezione dei Dati Personali per cortese ospitalità e per l'organizzazione di questo interessante evento, vorrei iniziare la presentazione con alcune brevi note personali.

Sono un Primo Ricercatore dell'Istituto di Biostrutture e Bioimmagini del Consiglio Nazionale delle Ricerche e da tempo mi occupo di tecniche biometriche. In qualità di esperto in questo specifico settore di ricerca, sono il responsabile scientifico di varie convenzioni in atto tra il nostro Istituto ed alcuni Ministeri italiani e, a livello internazionale, coordino un gruppo di lavoro nell'ambito dell'Iso (International Organization for Standardization) inerente gli aspetti giuridici, etici e sociali che caratterizzano la biometria. Non solo perché sono il coordinatore del gruppo, ne condivido appieno gli scopi avendo, della biometria, una visione ragionevolmente critica, soprattutto per ciò che attiene a precisi limiti che non si dovrebbero mai travalicare.

Oggi mi spetta l'impegnativo compito di descrivere, e in qualche modo, "difendere" le tecnologie biometriche con particolare riferimento alle delicate intersezioni con la privacy, oggetto del presente convegno.

Sono profondamente convinto che, nell'affrontare il problema della "coabitazione" fra biometria e privacy debbano prevalere essenzialmente la buona volontà ed il dialogo fra le parti. L'uomo e gli aspetti legati alla sua dignità debbano essere il perno fondamentale attorno al quale ruota questa affascinante tecnologia e che una buona applicazione biometrica, in linea di massima, è quella che raggiunge un compromesso tra tutti gli attori coinvolti nel processo e cioè utenti, gestori dei processi, organizzazioni sindacali o anche associazioni dei consumatori.

Nell'entrare nel vivo della presentazione, vorrei ricordare la figura di Alphonse Bertillon, inventore, alla fine dell'800' di una tecnica di identificazione, che, in qualche modo, ha rappresentato uno dei primi tentativi di standardizzazione della biometria. Bertillon, aveva infatti perfezionato una tecnica antropometrica attraverso una standardizzazione degli strumenti e delle modalità di acquisizione dei dati fisici. Anche se il cosiddetto "Bertillonage" aveva in realtà fini tipicamente investigativi, orientati più che altro all'identificazione di soggetti recidivi, esso può essere a ragione considerato una delle prime applicazioni, consolidate e generalizzate, di riconoscimento delle persone.

Il metodo di Bertillon introduce alla definizione classica di biometria che in-

(1) Università "Federico II" di Napoli – Facoltà di Ingegneria – Istituto di Bio-strutture e Bio-immagini

tende quindi *“il riconoscimento automatizzato di un soggetto o la verifica della sua identità sulla base di sue caratteristiche fisiche e comportamentali”*

Anche se apparentemente simili, identificazione e verifica di identità, sono in realtà completamente differenti e implicano, come vedremo in seguito, un coinvolgimento della privacy di peso assolutamente diverso. Il processo di identificazione necessita infatti di un archivio di dati biometrici (con tutte le conseguenze per la doverosa tutela dei dati) mentre la verifica di identità può avvenire anche senza di esso.

La moderna biometria, oltre che sul riconoscimento delle impronte digitali (che hanno soppiantato alla fine del milleottocento il metodo di Bertillon) si basa sulla valutazione di varie caratteristiche fisiche o comportamentali quali, ad esempio, la geometria della mano, le caratteristiche dell'iride, quelle del volto, della voce, la vascolarizzazione del dorso della mano o anche la modalità di apposizione della propria firma. Una attenzione particolare merita infine il cosiddetto “riconoscimento della retina” a causa di presunte intersezioni con la privacy. La tecnica biometrica, seppure oggi poco diffusa, è stata infatti spesso messa all'indice a causa della “sensibilità” della zona interessata dall'analisi biometrica anche se andrebbe messo in evidenza che, il metodo più conosciuto e noto come “retinal scanning”, non forniva in realtà informazioni mediche di rilievo e non poteva assolutamente essere paragonato, ad esempio, ad una fluoroangiografia retinica.

Nella biometria ricorre spesso il termine “template”, definito generalmente come il modello matematico della caratteristica fisica. Il template assume un particolare ruolo nei rapporti fra biometria e privacy in quanto esso, pur rappresentando una caratteristica fisica, è ben differente dalla sua immagine. Dal template è praticamente impossibile ricostruire la caratteristica fisica di partenza, con un certo sospiro di sollievo per ciò che attiene al rispetto della privacy.

Il “template” di una caratteristica biometrica ha un “peso” dal punto di vista informatico che va dal migliaio di bytes fino a pochi bytes. Anche ai meno esperti nel settore, dovrebbe essere evidente che con un modesto numero di bytes il grado di “sensibilità” del dato biometrico diventa alquanto moderato.

Oltre all'uso del template della caratteristica biometrica al posto della sua immagine, un altro accorgimento per la tutela della privacy consiste, come abbiamo già messo in evidenza, nel preferire l'implementazione di processi di verifica di identità piuttosto che di identificazione. In particolare depositando le caratteristiche biometriche solo sul titolo in possesso dell'utente (ad esempio una smart card) si può evitare l'uso di archivi e dei problemi connessi all'uso di essi. La caratteristica fisica sulla carta può essere cifrata ed anche il furto o lo smarrimento del titolo non dà luogo a problemi in quanto esso diventa inutilizzabile se non prodotto dal legittimo proprietario.

I campi di applicazione delle tecnologie biometriche sono vari e di pertinenza

sia della Pubblica Amministrazione che del settore privato. Alla base dell'uso della biometria c'è, ovviamente, l'esigenza di fondo di proteggere l'accesso ad edifici e luoghi o a risorse di calcolo. Una obiezione mossa spesso alla biometria è se l'uso sia davvero indispensabile nei confronti di un metodo di autenticazione tradizionale. È ovvio che la situazione va valutato caso per caso anche se valide argomentazioni possono essere rappresentate dai pericoli per la sicurezza derivanti dal furto o smarrimento dei titoli personali e dalla praticità di evitare di dovere ricordare un numero di password in costante e preoccupante aumento.

Il discorso sulla biometria implica ovviamente anche quello della vulnerabilità. Ci sono parecchi studi in corso sulla effettiva sicurezza offerta dalla biometria e c'è addirittura un esperto che ha proposto (su internet) una metodologia per la creazione di false impronte digitali in gomma (le cosiddette "gummy fingers"). Al di là dell'aspetto puramente scientifico, comunque di rilievo, andrebbe sottolineato che le "gummy fingers" hanno comunque, almeno per il momento, buona probabilità di successo solo con sensori dattiloscopici di fascia economica e, l'uso di dispositivi di acquisizione di classe superiore comporta livelli di vulnerabilità nettamente più rassicuranti.

Il discorso sulla vulnerabilità, o meglio, sulla percezione della vulnerabilità, va di pari passo con quello delle "leggende" più o meno metropolitane sugli usi "buoni" e "cattivi" della biometria. Se è vero che qualcuno teme che le proprie impronte, in forma di "gummy fingers", possano essere catturate depositate ad arte sulla scena del delitto dal proprio vicino di casa invidioso (classica ed improbabilissima fobia) è anche vero che in questi circa 30 anni di storia della biometria, a dispetto di tantissime preoccupazioni, la cronaca non ha riportato casi eclatanti di veri problemi legati alla biometria.

Certo, non va abbassata la guardia, alcune applicazioni come la cosiddetta "sorveglianza" (ricerca di soggetti all'interno di un archivio basata sul riconoscimento biometrico del volto) vanno guardate con la meritata cautela, ma, nello stilare un giudizio complessivo sulla biometria, penso che le si dovrebbero riconoscere i giusti meriti perché biometrica significa anche tanti vantaggi, fortunatamente, tangibili e concreti.

Con la dovuta esclusione delle applicazioni investigative, che rappresentano un caso a parte, la biometria che funziona, a mio parere, è quella in cui l'utente ha la percezione di ricevere attraverso di essa un vantaggio concreto (anche se a volte non immediato).

Un utente che gode di benefici immediati è, ad esempio, quello che, nell'aeroporto di Amsterdam, autenticato biometricamente, può espatriare automaticamente, attraverso varchi separati, evitando lunghe file grazie al programma Abc (Automated Border Crossing). Un utente compensato sul lungo periodo potrebbe essere quello che partecipa ai nuovi programmi governativi in tema di immigrazione e do-

cumenti di viaggio con identificatori biometrici che offre il suo contributo per un indispensabile incremento della sicurezza collettiva.

A questo proposito, è d'obbligo ricordare che gli Stati Uniti sono attualmente impegnati nel più complesso ed ambizioso progetto biometrico realizzato finora.

Il progetto Us Visit (United States Visitor and Immigrant Status Indicator Technology) prevede che, a regime, tutti i visitatori stranieri, all'atto di entrare negli Stati Uniti, lascino le proprie impronte digitali (oltre ad una fotografia del volto scattata dal funzionario dell'immigrazione). Us Visit non si applica ancora ai visitatori provenienti dai paesi Partecipanti al cosiddetto Visa Waiver Program (i cui cittadini sono esentati dall'obbligo del visto per entrare negli Stati Uniti), tra cui l'Italia, ma, è ormai prossimo il momento in cui la nuova procedura interesserà anche noi.

Oltre alla raccolta delle impronte digitali all'arrivo negli Stati Uniti, una ulteriore fase di Us Visit (attualmente in fase sperimentale) prevederà che esse siano acquisite anche all'uscita degli Stati Uniti allo scopo di controllare se esse coincidono con quelle acquisite all'ingresso.

Uno degli argomenti "caldi" ancora in discussione è la gestione dei "visitatori" degli Stati Uniti le cui impronte all'uscita non coincideranno con quelle raccolte all'ingresso dal momento che qualsiasi metodo biometrico è affetto da un (inevitabile) tasso di errore.

L'esperienza americana su un progetto biometrico di così ampia portata, i problemi sociali ed etici da affrontare e le procedure ipotizzate per la cosiddetta "gestione delle eccezioni" forniranno indicazioni essenziali nell'affrontare applicazioni biometriche e daranno forte impulso al tema della "accessibilità" che fa parte della attività di standardizzazione svolta nell'ambito del gruppo di lavoro Iso⁽²⁾ di cui ho parlato all'inizio.

Per "accessibilità" in ambito biometrico, si intende lo studio di opportune procedure od accorgimenti tecnici che diano la possibilità anche a persone portatrici di handicap fisici o psicologici di fruire degli eventuali benefici o servizi ottenibili attraverso l'autenticazione biometrica. Il tema è ovviamente molto complesso ma, allo stesso tempo, la accessibilità rappresenta un presupposto inderogabile per una concreta diffusione della biometria.

Un altro tema di interesse affrontato nel gruppo di lavoro Iso è quello della privacy ed è qui che naturalmente si intersecano le strade tra Iso e Garante per la Protezione dei Dati Personali. Non posso nascondere che le difficoltà per un gruppo di lavoro internazionale sono parecchie, ad esempio a causa delle, a volte, forti diffe-

(2) Il gruppo di lavoro 6 (ISO/IEC JTC1 SC37 "Biometrics" WG6 on "Cross-jurisdictional and societal aspects of biometrics") è stato varato come gruppo di studio nel Dicembre del 2002 l'Iso nell'ambito della creazione, da parte dell'ISO di un apposito sottogruppo dedicato alla biometria. Nell'ambito della riunione plenaria di Roma del Settembre del 2003 il gruppo di studio è divenuto gruppo di lavoro ed ha quindi acquisito lo status di permanente

renze esistenti fra Paese a Paese in tema di privacy. Per quanto riguarda questo problema, il primo passo è quello di trovare regole semplici in grado di essere accattate dalla quasi totalità dei paesi partecipanti ai lavori. Ad esempio, è allo studio una raccomandazione a livello Iso perché società, imprese od Amministrazioni che intendano usare sistemi biometrici possano indicare un figura professionale in qualche modo responsabile per l'applicazione biometrica. I compiti di questa persona dovrebbero spaziare dalla vigilanza sulla corretta raccolta, l'immagazzinamento ed accesso dei dati biometrici, all'informazione agli interessati in tema di sicurezza del processo biometrico fino alla conservazioni di manuali ed allegati tecnici per eventuali consultazioni da parte, ad esempio, di organizzazioni sindacali.

Mi rendo conto che il discorso si fa lungo e complesso ed il tempo a disposizione è praticamente scaduto e vorrei terminare con una informazione ironica in tema di privacy: ogni anno viene assegnato, con una buona pubblicità su internet, il cosiddetto "Big Brother Award", in italiano il "premio del grande fratello", che è attribuito da una giuria internazionale a coloro che si distinguono per avere realizzato, durante l'anno, progetti in qualche modo lesivi delle libertà personali. Anche se talvolta il premio è andato anche a qualche applicazione biometrica, ritengo che l'auspicio di tutti è che, dopo qualche fisiologico ed inevitabile aggiustamento, rispetto della privacy e biometria possano, con il tempo, andare serenamente su due binari paralleli e ricordare insieme, con ironia, i "vecchi tempi" del "Big Brother Award".

Vi ringrazio per l'attenzione

Claudio Manganelli⁽¹⁾

Questa é una occasione che mi emoziona poiché mi dà l'opportunità di tornare in questa sede che mi ha visto impegnato per un quadriennio, con l'onore di sedere nel primo Collegio dell'Autorità, a trattare di innovazione tecnologica e del suo impatto nella vita dei cittadini.

Avendo sentito le relazioni del mattino, in particolare quella del presidente Santaniello e del presidente Rodotà, credo che tutto sommato l'etichetta di "talebani della privacy" che a volte viene attribuita agli uomini dell'Autorità possa anche essere sopportabile se si considera, con adeguata obiettività, tutto lo sforzo che essi fanno nel razionalizzare e normalizzare l'impiego delle nuove tecnologie informatiche e di telecomunicazione, sempre più permeanti la nostra società. Anche perché sono convinto che, malgrado l'impegno profuso dall'Autorità, l'ambiente politico e burocratico appare spesso distratto nell'emissione di norme che comportano l'utilizzo di dati personali. Un punto di vantaggio lo ha certamente segnato il vostro codice unico, caratterizzato dall'approvazione unanime delle Camere, ma mi sono sempre chiesto se questa unanimità è stata convinta o distratta; questo perché molte volte, colgo iniziative che partono con un indirizzo poco rispettoso di quelli che sono i contenuti normativi esistenti nella legge.

A parte questa nota polemica, comunque, il nostro dovere è sempre quello di lavorare perché certe linee guida vengano tenute alte, vengano rispettate. Quali sono i fondamenti sui quali si deve basare l'analisi dei prodotti biometrici? Innanzitutto aleggia questa necessità sociale di sicurezza.

Abbiamo sentito alcuni relatori, stamattina, parlare della necessità di certezza indiscutibile delle transazioni nel mondo web, della necessità di far fronte con tempestività e precisione alle richieste provenienti dal mercato globale, dalla società globale e quindi il bisogno dei suoi cittadini di poter navigare, poter viaggiare, poter spostarsi senza avere ogni volta problemi di moneta, problemi di riconoscimento, problemi di documento; però tutto questo sembra confliggere con l'ultimo fondamentale e cioè il rispetto della dignità degli individui e quindi bisogna trovare le soluzioni per conciliare le due diverse facce della medaglia. Ora la biometria sembra essere una risposta a questi problemi ed in particolare alle necessità di sicurezza però crea molti interrogativi ai difensori della privacy: conosciamo tutti le vicende dell'11 settembre; da allora la biometria da molti Governi viene considerata come una soluzione d'obbligo, almeno per quel che riguarda l'identificazione delle persone.

(1) Componente Cnipa

In Italia è in corso una intensa attività di trasformazione del tradizionale metodo di funzionamento dell'apparato amministrativo e burocratico della Pubblica Amministrazione, verso un modello che adotti più elettronica, per una maggiore trasparenza ed efficienza dell'azione della Pubblica Amministrazione: quindi sono necessarie migliori garanzie per l'autenticazione e la biometria promette di essere la migliore strada per una sicura autenticazione. È fondamentale però che tutto questo avvenga con una mentalità serena e senza avere dei pregiudizi su cosa si può o cosa non si deve fare, ma trovare ogni volta la soluzione che contemperi le due realtà.

Di questo tema si sta facendo carico il Cnipa: il Centro Nazionale per l'Informatica nella Pubblica Amministrazione è nato da una trasformazione dell'Autorità per l'informatica nella Pubblica Amministrazione.

Alla fine del precedente Governo e all'inizio dell'attuale legislatura si è molto discusso sulla proliferazione delle autorità e sulla necessità di razionalizzare il settore; si sono fatti studi, ricerche e progetti; sono state elencate le autorità poste a garanzia di valori costituzionali come quella che oggi ci ospita distinguendole da quelle che forse potevano essere più un modello di agenzie: per il momento l'Aipa è stata l'unica ad essere trasformata.

Personalmente credo che sarebbe stato più tattico rafforzarne i poteri attraverso la disponibilità di strumenti sanzionatori per trasformarla in un efficace organismo al servizio del Ministro e del Governo; infatti se si chiede alla Pubblica Amministrazione di rispettare gli standard di evoluzione della tecnologia e adeguarsi ai tempi, spendendo sì, ma con oculatezza e in sintonia colle regole comunitarie, e convergere sugli obiettivi rispettando la pianificazione dei tempi e gli standard applicativi e di comunicazione, senza troppe ridondanze antieconomiche, sarebbero stati utili, a mio avviso, dispositivi più efficaci della semplice "moral suasion". Però siccome serviva una grossa operatività probabilmente la trasformazione in Centro per l'informatica, che sta accompagnando l'azione del Ministro per l'Innovazione Tecnologica, nei progetti evolutivi, soprattutto quelli interministeriali, interdisciplinari è stata una cosa necessaria, che ci permetterà di avere una visione più diretta anche nel mondo delle Pubbliche Amministrazioni locali che sinora, nel corso della vita dell'Aipa, sono state un po' lasciate andare per la loro strada. Un fatto fondamentale questo, credo di poterlo dire, essendo il Cnipa una forte concentrazione di esperienze tecnologiche che ci permetterà di tracciare in anticipo percorsi evolutivi dell'innovazione tecnologica, non solo in ambito pubblico ma anche nella società, prevedendo percorsi che, se il Garante vorrà affiancarci, potranno essere condotti insieme.

Intravediamo una strada di supporto alle attività che fa il Garante e quindi istituire una sede, un tavolo permanente di consultazione, che possa armonizzare i principi fondamentali e il rispetto dell'individuo con quelli offerti dall'evoluzione della tecnologia. Cosa ha fatto il Cnipa per quanto riguarda la biometria? Visto che

nella Pubblica Amministrazione esistono oggi iniziative che permettono di utilizzare soluzioni biometriche, in particolare l'impronta digitale, quali la carta di identità elettronica, il passaporto elettronico, la previsione del permesso di soggiorno elettronico per gli immigrati, la carta multi servizi della difesa, altre come l'Afis per l'identificazione delle persone sospette, dei pregiudicati, il Cnipa ha realizzato un centro di competenza per poter presiedere questa area della biometria, sia a favore delle Pubbliche Amministrazioni centrali che delle locali.

Ora per poter sistematicizzare il rapporto delle Pubbliche Amministrazioni stiamo cercando di mettere a fattor comune una serie di conoscenze che sono disseminate negli ambiti universitari, presso i fornitori di tecnologie, presso i System Integrator. In Italia sono forse questi ultimi la sponda più critica perché molte delle tecnologie biometriche sono importate dall'estero e qui semplicemente assemblate; quindi a volte c'è anche una certa carenza delle capacità di prestazioni così come del loro adattamento ai principi applicativi europei, una sorta di "prendere come viene". Un problema, come ricordava stamattina il presidente Rodotà, deriva dal fatto che, in materia di riconoscimento delle impronte digitali, esistono ancora casi di alte percentuali di errore a seconda delle soluzioni, ma a seconda soprattutto dei dispositivi elettronici che vengono utilizzati, errori che si manifestano come falsi riconoscimenti o false accettazioni. Ecco, abbiamo pensato anche che una volta individuate le soluzioni migliori, potesse farsi strada il riuso delle "best practices" e cioè avere la possibilità, una volta trovate le soluzioni per una certa applicazione, portare avanti questo tipo di discorso anche su applicazioni compatibili e poi allinearsi a progetti internazionali. Quindi è in fase di attivazione un rapporto diretto con le altre realtà europee e perché no anche Americane. Poi siccome l'organo collegiale del quale faccio parte, cioè il collegio del Cnipa, è rimasto il modello che c'era prima nell'autorità, esso dovrà emettere pareri di congruità sui progetti che gli verranno sottoposti.

Quando si tratterà di congruire progetti contenenti soluzioni di tipo biometrico, ovviamente, noi dovremmo essere in grado di dare una risposta sia sulla congruità, sia sulla utilità e compatibilità con i principi fondamentali che sono alla base delle norme sulla protezione dei dati personali. Il gruppo di lavoro che abbiamo avviato sul tema delle biometrie confluirà in un centro di competenza che predisporrà delle linee guida che sono in fase già di avanzata realizzazione.

Dovremmo nel mese di luglio rilasciare un documento, creare un osservatorio in questo campo sperimentando anche soluzioni biometriche, se possibile, congiuntamente ai diversi laboratori di fornitori e poi attraverso una convegnoistica presentare anche i risultati che si raggiungeranno. Per quanto riguarda le linee guida, il gruppo di lavoro si è avvalso, oltre che, del personale interno del Cnipa e anche su rappresentanti del mondo accademico e dalla ricerca, tra questi il prof. Savastano che ha

parlato prima di me. Ci sono, poi, delle amministrazioni di riferimento come il Ministero degli Interni che sta applicando soluzioni biometriche, utilizza l'Afis - per esempio - e pensa di utilizzare le impronte digitali oltre che quelle palmari, rappresentanti di grandi amministrazioni direttamente coinvolti in progetti come "giustizia" e "difesa" e poi le associazioni di fornitori di tecnologie di comunicazioni e informatica. Abbiamo chiesto al Garante, che ha accettato, la presenza di un suo rappresentante in qualità di uditore o assistente che ci da la possibilità di capire tempestivamente se ci stiamo muovendo in linea con i punti di vista del Garante stesso. La predisposizione delle linee guida, dicevo prima, dovrebbe essere completata prestissimo, poiché dovrebbe essere rilasciata in luglio. I contenuti di queste linee guida sono: gli obiettivi, il processo biometrico e la sua descrizione, le diverse soluzioni che oggi esistono sul mercato e le applicazioni relative nei vari Paesi del mondo.

Gli aspetti normativi, là dove esistono evidentemente, come diceva il prof. Savastano, gli aspetti non tecnici che in qualche modo hanno diretta implicazione sul modello organizzativo di una soluzione biometrica. I livelli di sicurezza: come realizzarli, come proteggerli e quali sono le soluzioni, la valutazione complessiva della biometria e poi chiaramente ci sarà una appendice, un glossario, una bibliografia.

Pensiamo anche di fare un convegno e ne abbiamo già concordato, in linea di massima, date e temi con il Garante; vorremmo discutere proprio in questa sede nel prossimo mese di ottobre, la posizione che c'è in Italia sulla biometria, negli Stati Uniti e nell'Unione Europea, fare una rassegna delle diverse tecnologie biometriche e soprattutto analizzare gli aspetti, gli impatti, diciamo, che la biometria può avere sulla società.

Un classico: le impronte digitali. Le soluzioni di rilevazioni delle impronte digitali non sono molto accettate, gradite, perché in ciascuno di noi c'è il concetto della schedatura che, chiaramente, prevede che per essere schedato con le impronte digitali significa aver avuto dei trascorsi con la legge. Quindi ciascuno di noi si sente, in qualche modo, in difficoltà di fronte ad una soluzione biometria; è quindi necessario rimuovere i vecchi schemi culturali, come diceva il prof. Savastano, magari ricercando anche soluzioni premianti, cioè delle facilitazioni.

Ad esempio nell'aeroporto di Fiumicino si sta sperimentando una soluzione del genere per il personale dell'aeroporto. Applicando soluzioni del genere ai "frequent fliers" si darebbe a loro un vantaggio, perché a fronte del fastidio di natura psicologica, assicurando loro tutte le necessarie garanzie sugli aspetti della privacy, essi potrebbero accedere ai voli con comodità, piuttosto che sobbarcarsi alle lunghissime code di attesa che, in alcuni giorni, caratterizzano i voli da Roma e Milano.

Vorrei concludere con un concetto: c'è sicuramente una crescita costante e forse più dinamica del bisogno di sicurezza rispetto a quello di tutela della vita personale. Bisogna seguire passo passo, con estrema attenzione, questa crescita e armoniz-

zare la seconda con la prima. Trovare l'equilibrio non è certamente facile, ma è un compito che ritengo esclusivo del Garante, ma al quale noi tutti partecipare: chi legifera, chi progetta, chi utilizza. Credo però, che ci sia un punto fermo che ormai non si può più evitare: io lo interpreto in questo modo, proprio per il mio passato trascorso al Garante e ricordando il principio alla base della privacy, quell'ormai lontano concetto di privacy nato negli Usa, il diritto ad essere lasciati soli. Ecco: la tecnologia, l'abbiamo sentito stamattina, è ubiqua, è pervasiva, è indossabile. Quindi questo diritto a non essere lasciati soli probabilmente dovremmo trasformarlo in un diritto a non essere coinvolti, cioè il fatto che la raccolta delle informazioni debba essere pertinente e non eccedente; su questo tema abbiamo avuto certamente discussioni con organismi dello stato quando ero al Garante.

Successivamente, nel mio nuovo ruolo, ho avuto ancora scambi franchi di questi principi in alcuni gruppi di lavoro con alcuni rappresentanti che, considerando la tecnologia una sorta di rete da pesca a maglie fittissime, riterrebbero opportuno catturare la maggior quantità di informazioni possibile e conservarla il più a lungo possibile nel tempo, per poi scandagliarla con comodo e per ogni occorrenza, quali ad esempio le informazioni che sono alla base di una comunicazione telefonica fissa o mobile, con il rischio quindi di coinvolgere, magari fra 10 anni, in vicende perseguibili cittadini inconsapevoli che hanno avuto rapporti puliti con personaggi che nel tempo si sono trasformati da cittadini onesti a malavitosi, imponendo così agli ignari sospettati il difficile onere di dover provare la loro estraneità a fatti che potrebbero anche essere troppo remoti.

È questo il senso del mio slogan: un nuovo tipo di diritto alla privacy: quello di non essere coinvolti se non esistono fondati ed aggiornati motivi di coinvolgimento. Secondo me, è un principio fondamentale che noi dovremmo curare sia sugli aspetti più tradizionali della tecnologia sia soprattutto sugli aspetti biometrici, perché questo ultimo settore applicativo è ancora più delicato e importante.

Grazie per l'attenzione.

Alessandro Musumeci⁽¹⁾

Desidero ringraziare per prima cosa il presidente Rodotà e il presidente Santaniello per questo invito che mi permette di focalizzare la vostra attenzione sulle problematiche di sicurezza e di privacy del mondo della scuola, del mondo dei giovani. Problematiche che sono sotto i nostri occhi quotidianamente e che proprio per questo motivo richiedono osservatori attenti e scrupolosi.

Ad esempio oggi è il giorno della seconda prova degli esami di Stato; proprio in questa occasione noi abbiamo lavorato in collaborazione con la Polizia delle Comunicazioni, per assicurare la massima riservatezza delle prove scritte e per evitare, prevenire o limitare fughe di notizie riguardanti le tracce e le soluzioni da parte delle scuole.

Questo e altri argomenti verranno trattati nel mio intervento, in quanto strettamente legati sia al concetto di protezione dei dati personali che alle problematiche di sicurezza già presenti nelle scuole. Tali problemi si sono affacciati alla porta delle scuole negli ultimi anni sulla base della velocissima diffusione delle tecnologie informatiche nella scuola che ha avuto un boom in questi ultimi tre anni e che ha visto un coinvolgimento molto forte dei docenti, dei studenti e delle famiglie.

Nelle scuole italiane siamo passati in tre anni, dal 2001 al 2004 da un personal computer ogni 28 studenti ad un personal computer ogni 11 studenti, con oltre 530.000 computer nelle scuole. Docenti e studenti sono forti utilizzatori di tecnologie informatiche; dal recente rapporto Federcomin emerge che due terzi delle famiglie italiane che hanno figli in età scolare (dall'asilo all'università) ha almeno un personal computer e molte di queste macchine sono connesse ad internet.

Se poi verifichiamo un grafico nel quale sono riportate le età di utilizzo del personal computer vediamo che l'utilizzo massimo avviene fra i 15-17 anni con una discesa, poi, lenta e progressiva dell'utilizzo del personal computer, fino ad una risalita dell'utilizzo da parte degli anziani (in particolare le donne che lo utilizzano essenzialmente come strumento di comunicazione con amiche, figli e nipoti).

In alcune fasce, come quella già menzionata dei 15-17 anni l'uso di internet prevale addirittura rispetto alla visione della televisione, e questo dimostra la forte attitudine dei giovani ad utilizzare anche a scuola, e non solo a casa, i mezzi tecnologici e le innovazioni tecnologiche ovunque sono disponibili. Partendo da queste considerazioni abbiamo individuato alcuni aspetti, alcuni punti focali sui quali concentrare la nostra attenzione e assicurare il massimo livello di sicurezza possibile, adeguato alle esigenze delle scuole, salvaguardando al tempo stesso i dati personali

(1) Direttore Generale Sistemi Informativi (DGSi) del Ministero dell'Istruzione, dell'Università e della Ricerca

e quindi la possibilità di accedere alle varie informazioni.

Il primo punto sul quale ci siamo concentrati è la posta elettronica; abbiamo messo a disposizione dei docenti un sistema denominato “cruscotto docente”, dove sono disponibili una serie di funzionalità e applicazioni per il docente, non solo di posta elettronica ma, per esempio, di consultazioni via internet di orari e ricevimenti dei docenti, di suggerimenti o fruizioni di informazioni riguardo il proprio status (ad esempio la propria graduatoria). Tutte queste informazioni sono accessibili, previa autenticazione dal sito internet del Ministero e ciò fa crescere ovviamente in modo veloce il numero di accessi. In questi giorni il sistema sta lavorando con oltre 14 milioni di “hits” al giorno e con oltre 500.000 utenti (perlopiù studenti, docenti e famiglie). Tale numero di accessi è destinato ad aumentare considerando che i dipendenti della scuola sono circa un 1 milione di persone e la popolazione degli studenti è di circa 7 milioni e 600 mila studenti.

Tale sito possiede tutta una serie di servizi e informazioni che vanno salvaguardati, assicurando però un accesso contemporaneo al maggior numero possibile di fruitori. In particolare per un'applicazione, quella per l'inserimento delle domande di graduatoria on line, della quale hanno usufruito circa ventimila docenti, per la quale era necessario assicurare un valore legale alla domanda effettuata via internet, e quindi un valore pari a quello della raccomandata personale, abbiamo inserito anche la firma elettronica.

Con una speciale firma elettronica, disponibile presso i principali uffici postali, del costo di tre euro e mezzo, abbiamo ottenuto una sorta di francobollo elettronico, con una logica “usa e getta”, con l'obiettivo di assicurare piena validità legale a questo strumento.

Ovviamente diffondendo il servizio di posta elettronica (attualmente abbiamo oltre 300.000 docenti e Ata registrati) uno dei problemi che stiamo affrontando è l'aumento del fenomeno dello spamming. Sono stati implementati una serie di prodotti antivirus per consentire un rigoroso filtraggio delle mail, salvaguardando al tempo stesso le caratteristiche di privacy dei docenti, in modo da garantire lo scambio di messaggi senza interferire sui loro contenuti.

Sempre a proposito di minacce in ambiente Internet un altro problema che stiamo affrontando è quello di garantire alle scuole la navigazione sicura sul web; anche in questo caso uno specifico gruppo di lavoro sta lavorando per assicurare un buon livello di sicurezza all'interno del nostro sistema informativo. Tale ambiente è ormai essenzialmente basato su internet, e in esso esiste un'insieme di accessi, alcuni dei quali riservati per docenti, altri specifici per gli uffici scolastici, oppure per gli uffici del ministero; altri accessi sono liberi e sono adatti per l'accesso degli studenti e delle famiglie.

Questa massima apertura del sistema informativo che cosa ha comportato? Ha reso necessario filtrare e verificare periodicamente tutti i computer all'interno del si-

stema internet delle scuole, che sono come già detto oltre 500.000. Tale controllo è stato facilitato grazie all'utilizzo del Garr, la rete dell'Università, che stiamo estendendo progressivamente alle scuole di tutta Italia.

Inoltre con un recente accordo tramite Consip, sono stati estesi alle scuole i collegamenti Adsl, con l'84% attuale delle Istituzioni scolastiche principali cablate con collegamenti Adsl a larga banda. In molti casi inoltre si è diffuso anche l'utilizzo di reti senza fili nelle scuole; ad oggi oltre 700 scuole possiedono ed utilizzano reti wireless.

In alcune di queste scuole sono stati segnalati episodi di abuso di risorse, non tanto da parte di docenti o di studenti, che per definizione sono abilitati all'uso di risorse nella scuola, quanto da parte di soggetti estranei alla scuola che si sono intrufolati via radio nei collegamenti di tale tipo, che in alcuni casi erano stati lasciati non protetti.

Per tal motivo abbiamo messo a disposizione delle scuole, sul nostro sito internet, e quindi disponibile pubblicamente (vi invito a consultarlo), un manuale di policy che è sufficientemente semplice da essere utilizzato da tutti gli utenti della scuola, ma al tempo stesso con delle indicazioni molto precise su come configurare le reti in modo essenziale ma sicuro e su come fornire indicazioni per evitare il ripetersi questi fenomeni.

Come dicevo prima, una delle scelte di fondo che abbiamo fatto è stata quella della centralizzazione degli accessi, non solo per assicurare un livello maggiore di riservatezza ma anche per evitare la fruizione nelle scuole di contenuti dannosi per i giovani. Sono state per tal motivo implementate una serie di black list sul sistema centralizzato di accesso delle scuole; tale sistema previene e filtra in modo opportuno i contenuti, impedendo di fatto l'accesso a siti non pertinenti il mondo dell'istruzione. Questo sistema funziona abbastanza bene, ed è in fase di implementazione in quanto questa black list ha un aggiornamento quotidiano ma stiamo anche studiando la modalità per renderla più sensibile e aggiornata automaticamente per prevenire le principali minacce.

Dalle scuole quindi posso accedere liberamente a tutti i siti italiani, europei e mondiali riguardanti il mondo dell'istruzione, a quelle di tutte le Università, su una serie di siti con contenuto culturale, oppure ai sistemi delle biblioteche; in pratica si può usufruire di un complesso mondo di risorse che costituisce un complesso sistema di knowledge management.

In questa direzione, comunque, è possibile fare di più, in particolar modo per quanto riguarda la formazione di una cultura della sicurezza da parte dei giovani, particolarmente importante in un mondo nel quale aumentano le minacce non solo sulla rete. Vorrei pertanto concludere il mio intervento toccando proprio quest'ultimo tema, quello della formazione.

Nel corso degli anni, analizzando minacce e mettendo in atto contromisure di vario tipo, ci siamo resi conto che, al di là di qualunque implementazione tecnologica, il punto più debole della sicurezza in un sistema complesso sia senz'altro il fattore umano.

Gli utenti di un sistema così vasto e così complesso, che è a disposizione dei cittadini, devono essere formati alla sicurezza, educati ad utilizzare tali sistemi in modo accorto. Occorre in qualche modo indurre in comportamenti virtuosi, che consentono di applicare all'interno delle scuole tutti gli idonei comportamenti atti ad evitare pericoli.

In tale ambito sono state realizzate un gran numero di azioni investendo all'interno delle scuole per creare una cultura della sicurezza, partendo dalla formazione dei più giovani.

Posso citare ad esempio alcune pubblicazioni on-line che abbiamo messo a disposizione sul nostro sito; questa è una delle tante: "Un ragno per amico", realizzata dalla Direzione Regionale del Piemonte, ed è specifica per gli alunni delle scuole medie ed elementari; abbiamo iniziative in collaborazione col Ministero Innovazione e Tecnologie, al fine di educare famiglie, studenti e soprattutto i docenti, alla cultura della sicurezza, con una serie di indicazioni molto precise, per bambini, ragazzi e genitori.

Per i bambini ad esempio tali indicazioni vengono viste come un gioco, come un qualcosa di non obbligatorio, per aiutare chi naviga oggi su internet, sia a casa che a scuola.

Ecco, credo che questa sia la strada che dobbiamo seguire, al di là di quelle che sono le diverse possibilità tecnologiche, che peraltro sono in fase di ulteriore evoluzione. È necessario investire, nel nostro paese, sulla cultura della sicurezza, e credo che questo sia il ruolo che compete alla scuola, che ha un gran numero di accessi e che ha il dovere di salvaguardare una risorsa preziosa che è di noi tutti.

In tale attività ci sta dando una gran mano la Polizia delle Telecomunicazioni, proprio perché a fronte di questo complesso sistema nel quale è necessario verificare e controllare migliaia di accessi, sentiamo la necessità di avere qualcuno più competente che abbia visibilità su tutte le principali problematiche di sicurezza e della protezione dei minori. Abbiamo sempre la Polizia delle Comunicazioni al nostro fianco per tutto quello che riguarda le problematiche di analisi dei casi sospetti ed eventualmente, di repressione di quelle che sono eventuali problematiche.

In conclusione, io credo, al di là delle innovazioni tecnologiche che stiamo vivendo e alle quali ci dovremo abituare, il Garante della Privacy, possa offrirci un valido aiuto per la definizione di questo piano di formazione per la creazione di una cultura della sicurezza che non può che partire dalle scuole, che necessariamente deve coinvolgere i ragazzi, per aiutarli a "navigare" su Internet senza rischi e in modo

sicuro, rafforzare il senso di sé, e distinguendo realtà e immaginazione, mondo reale e mondo virtuale.

Dalle prime esperienze che abbiamo fatto, emerge che molto spesso i ragazzi, di ogni età e sesso, immersi nella realtà mediatica di ogni giorno, non distinguono con chiarezza il passaggio dal mondo reale al mondo internet e si abituano a volte a “navigare” su internet senza o con pochi controlli, senza abituarsi a sapere dire di no a situazioni spiacevoli, chiedendo aiuto alle persone adulte quando si tratta di affrontare dei problemi di sicurezza personale.

Da queste semplici constatazioni emerge come il problema non possa essere risolto solo in termini tecnologici, ma vada affrontato con un coinvolgimento culturale, non possa essere affrontato solo in termini di normativa, ma debba coinvolgere studenti e famiglie, e soprattutto docenti.

Noi stiamo investendo in modo forte sulla formazione dei docenti sulle tecnologie, proprio perché crediamo che questo coinvolgimento culturale debba essere alla base di un sistema realmente sicuro nelle scuole. E credo che questo metodo, arricchisca effettivamente di valori il nostro sistema scolastico ed educativo, contribuendo ad una crescita dei nostri giovani in una chiave realmente europea.

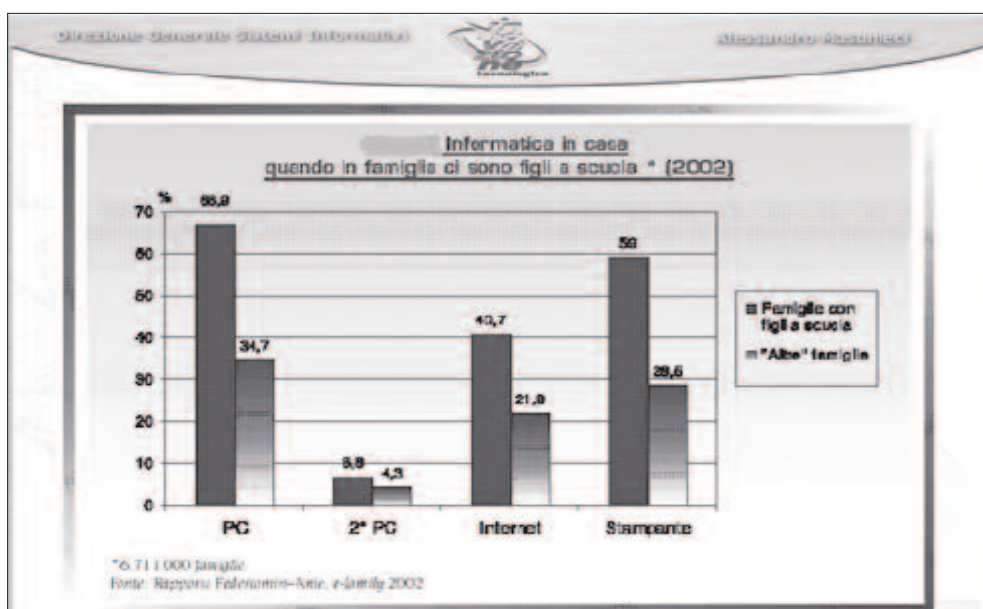
Grazie per l'attenzione.

Direzione Generale Sistemi Informativi 
 Alessandro Musumeci

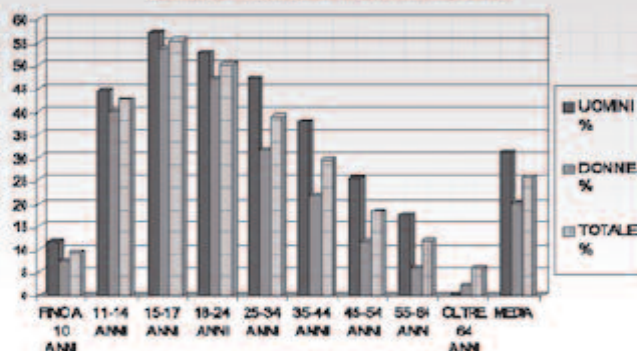
Ministero dell'Istruzione, dell'Università e della Ricerca

in internet@scuola

Alessandro Musumeci
Direttore Generale Sistemi Informativi



Utilizzatori di pc in casa
In % sull'universo delle persone (2002)



Fonte: Rapporto Intercom-Azi. e-famig 2002

L'utilizzo di Internet nelle scuole

- **La posta elettronica**
- Lo spamming
- La navigazione su Web
- Il filtering dei contenuti
- La diffusione della netiquette

Ministero dell'Istruzione, dell'Università e della Ricerca

Allegato al Decreto

Il progetto prevede un "Cruscotto docente" per:

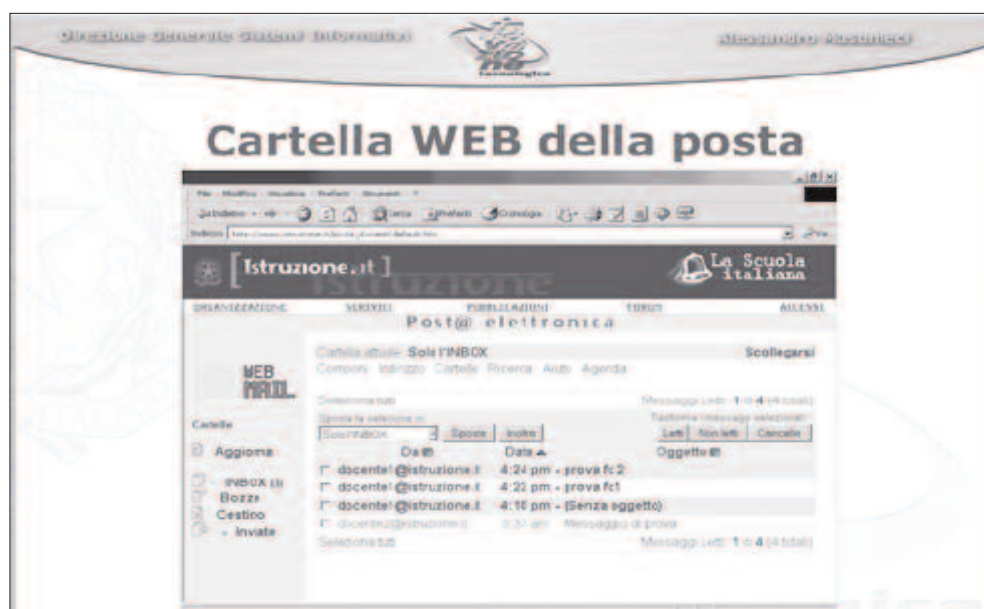
- Utilizzo della Posta elettronica nome.cognome@istruzione.it
- Consultazione via Internet degli orari di ricevimento dei docenti da parte delle famiglie e di eventuali avvisi
- Fruizione di programmi didattici, software, dispense preparati da altri docenti (tramite autenticazione)
- Funzioni di comunicazione con studenti (tramite e-mail o SMS)
- Richiesta di informazioni tramite suggerimenti@istruzione.it
- Consultazione di convenzioni di acquisto specifiche per scuole e docenti (software, hardware, ADSL)
- Accesso a funzionalità di e-learning
- Consultazione del SBN per prestiti e riproduzioni di libri
- Consultazione di normative (concorsi, ecc...)

Ministero dell'Istruzione, dell'Università e della Ricerca

Allegato al Decreto

Interfaccia WEB del sistema

The screenshot shows the web interface of the 'Istruzione.it' system. At the top, there is a navigation bar with links like 'Indirizzo', 'Indirizzo', 'Indirizzo', 'Indirizzo', 'Indirizzo', 'Indirizzo', 'Indirizzo', 'Indirizzo', 'Indirizzo', 'Indirizzo'. Below this, the main header features the 'Istruzione.it' logo and the 'La Scuola Italiana' logo. The central part of the page is titled 'Post@ elettronica' and 'Accesso posta Docenti/Dirigenti scolastici'. It contains a login form with fields for 'Codice Utente' and 'Password', and buttons for 'Accedi' and 'Annulla'. To the left of the login form, there are links for 'Non hai registrato il tuo indirizzo email?', 'Non hai cambiato la password?', 'Hai dimenticato la password?', and 'Inviare il plugin di Adobe Acrobat'. To the right, there is a section for 'Completa la registrazione' and a list of links: 'Come registrarsi', 'Parametri di configurazione', 'Guida WebMail', and 'Intranet'.



L'utilizzo di Internet nelle scuole

- La posta elettronica
- **Lo spamming**
- La navigazione su Web
- Il filtering dei contenuti
- La diffusione della netiquette



Uso di tools di Content Security per il Mail/Web

Uso massiccio di Mails e del Web



Minacce - spamming & spoofing

- 1° livello 1 – **spam** : E-mail inutili
- 2° livello – bombing, files di ampi dimensioni: disfunzioni o congestione della rete
- 3° livello – attacchi esterni, **spoofing**

Analisi & decomposizione ricorsiva



L'utilizzo di Internet nelle scuole

- La posta elettronica
- Lo spamming
- **La navigazione su Web**
- Il filtering dei contenuti
- La diffusione della netiquette



Scenari di sicurezza delle WLAN



L'utilizzo di Internet nelle scuole

- La posta elettronica
- Lo spamming
- La navigazione su Web
- **Il filtering dei contenuti**
- La diffusione della netiquette

Internet Content Rating Association

Home Mappa sito

Informazioni su ICRA

Chi, come, perché

Notizie e comunicati

Trust ICRA?

Complaints

Contacti

Informazioni utili

Webmaster

Genitori

Bambini

Complaints

FAQ

Area di download

Etichettare un sito

ICRAfilter

Generatore di etichette

Test di etichette

Filigrana digitale

Comunità ICRA

Memori

Associati

Adesione a ICRA

Affiliati

Casi concreti

Hotline

Link

Internet Content Rating Association

francese Deutsch English

Ad

Get Green

Il nostro di pubblico contributo a sostenere ICRA, un'organizzazione senza fini di lucro

Webmaster

Perché e come etichettare. Come le etichette garantiscono la libera scelta invece della censura.

Genitori

Proteggere i vostri bambini quando navigano in Internet: usate il nostro filtro gratuito.

Bambini

Ecco dei consigli utili per navigare sicuri in Internet.

Internet a misura di bambino

ETICHETTATE IL VOSTRO SITO

Offrite ai genitori la possibilità di proteggere i propri figli da materiale potenzialmente dannoso, senza limitare la vostra libertà di espressione.

NOVITÀ

Associate Membership now available - now you can join the biggest names on the internet supporting ICRA. [More...](#)

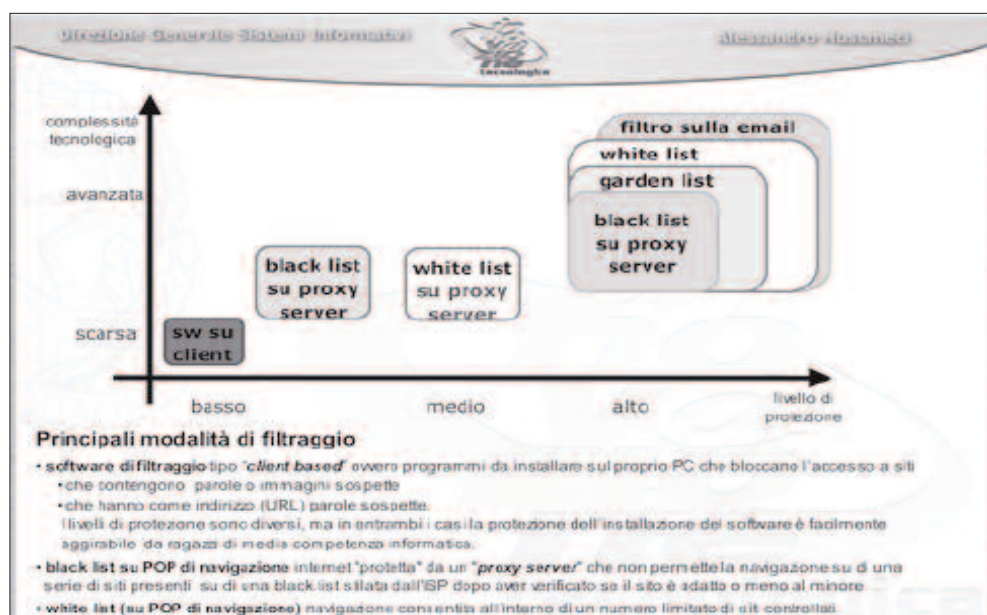
Delivering a Safer Internet - 1 launches new 5-year plan. [More...](#)

Customization and Personalization through RPT - major new project launched. [More...](#)

Adesione a ICRA...

... è un'opportunità importante per operatori Internet nell'autorevole costruire una comunità Internet sicura per i bambini.

La Internet Content Rating Association è un'organizzazione indipendente, senza fini di lucro, con uffici in Europa e negli Stati Uniti. ICRA possiede e gestisce il sistema di etichettatura ICRA e il suo predecessore, RSAC.



L'utilizzo di Internet nelle scuole

- La posta elettronica
- Lo spamming
- La navigazione su Web
- Il filtering dei contenuti
- **La diffusione della netiquette**

L'utilizzo di Internet nelle scuole



CHI HA PAURA... DELLA RETE?

per un uso consapevole
di Internet



✓Internet è...

...è una grande e inesauroibile enciclopedia. Ogni movimento del mouse apre una nuova pagina che poi mostrarti posti lontani e interessanti, fornirti tutte le informazioni che desideri, farti conoscere nuovi amici e compagni di viaggio. Insomma con un solo click puoi davvero visitare tutto il mondo! Con Internet hai non solo la possibilità di comunicare senza limiti di spazio e di tempo, oltre ogni confine geografico e culturale, ma disponi anche di una gamma vastissima di servizi che vanno dalla posta elettronica alle operazioni finanziarie, dalle attività commerciali fino alle conferenze telematiche.



I benefici e i vantaggi che l'utilizzo di Internet può portare nella vita di tutti i giorni sono enormi, ma è indispensabile, se volessimo ricorrere a un'immagine diffusa, che di una medaglia esista solo una facciata.

Anche Internet, come accade nella realtà, può nascondere delle brutte sorprese. Per questo appare indispensabile favorire un uso consapevole della rete, un utilizzo delle moderne tecnologie che sia dettato da buon senso e ragionevolezza, ma soprattutto dalla conoscenza delle immense potenzialità della rete.

Per saperne di più...

- ☐ navigatori per caso
- ☐ acquisti on line
- ☐ chat lines
- ☐ dipendenza da internet
- ☐ peer to peer
- ☐ filtri...

Consiglio Regionale del Piemonte
COMITATO
Strade - Energie Sicure



CHI HA PAURA... DELLA RETE?

per un uso consapevole
di Internet



home navigatori per caso

✓per i Bambini

qui puoi giocare per scoprire molte cose su Internet; alla fine del gioco ti sarà consegnata la patente del "buon navigatore".

✓per i Ragazzi

qui puoi imparare come utilizzare Internet, conoscere le regole da rispettare e i diritti da far valere per essere un "buon navigatore".

✓per i Genitori

qui puoi trovare utili consigli e la possibilità di scaricare un prodotto software per filtrare i contenuti che non ritieni adatti ai tuoi figli.



Per saperne di più...

- ☒ navigatori per caso
- ☐ acquisti on line
- ☐ chat lines
- ☐ dipendenza da internet
- ☐ peer to peer
- ☐ filtri

Ministero dell'Istruzione, dell'Università e della Ricerca  [Altre risorse](#)

CHI HA PAURA... DELLA RETE?

per un uso consapevole di Internet

[home](#) [navigatori per caso](#) [bambini](#)

✓ Bambini

Internet è un mondo meraviglioso che può offrirti molto ma che, come il mondo reale, nasconde delle insidie che lo rendono pericoloso.
Conoscere questo mondo fantastico e le insidie che in esso si nascondono ti aiuterà a navigare tranquillo.



Scopriamo insieme...

- a cosa serve Internet
- cosa si può e cosa non si deve fare
- i diritti

Se vuoi conoscere il significato dei termini più usati vai al Glossario

Ministero dell'Istruzione, dell'Università e della Ricerca  [Altre risorse](#)

CHI HA PAURA... DELLA RETE?

per un uso consapevole di Internet

[home](#) [navigatori per caso](#) [ragazzi](#)

✓ Regole



3. In rete puoi trovare molto materiale per la tua tesina.

- raccolgo tutto il materiale a disposizione, ne faccio un rapido collage e consegno la tesina
- consegno una tesina che ho trovato in rete già fatta grazie alle informazioni che ho trovato su Internet farò la tesina più originale
- il materiale che ho trovato in rete è prezioso: decido che metterò on line anche la mia tesina così qualcun altro potrà usufruirne del mio lavoro

« Torna all'elenco »

Direzione Generale Sistemi Informatici



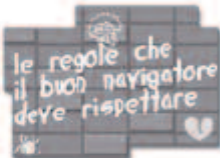
Sistemi di Informazione

CHI HA PAURA...
per un uso consapevole
di Internet...
DELLA RETE?



home | navigatori per caso | ragazzi

✓ Regole



c.grazie alle informazioni che ho trovato su Internet farò la tesina più originale

BRAVO !!!

Grazie a migliaia di persone che ogni giorno decidono, spontaneamente e senza fini di lucro, di **condividere** in rete le loro conoscenze, Internet è una risorsa inesauribile di informazioni per continuare sempre a imparare e a migliorare.

Il passo successivo è decidere di **condividere** con gli altri le conoscenze che la rete ti ha aiutato ad acquisire.

Continua »

Direzione Generale Sistemi Informatici



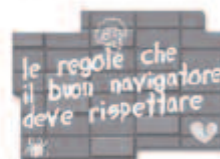
Sistemi di Informazione

CHI HA PAURA...
per un uso consapevole
di Internet...
DELLA RETE?



home | navigatori per caso | ragazzi

✓ Regole



d.il materiale che hai trovato in rete è prezioso: decidi di mettere on line anche la tua tesina appena l'avrai finita così qualcun altro potrà usufruire del tuo lavoro

BRAVO !!!

Ma c'è in più lo spirito di **condivisione** che anima le comunità di Internet e tutte le altre importanti iniziative che rendono la rete una sterminata risorsa di informazioni che persone generose e lungimiranti decidono ogni giorno di condividere con tutto il mondo.

Continua »

CHI HA PAURA... DELLA RETE?

per i tuoi computer
di internet



Home > navigatori per caso > genitori

✓ Consigli



1. Non tenere il computer in un ambiente isolato. Internet deve essere considerato come uno strumento di famiglia.



2. Condividi i principi con tuo figlio. Scrivi insieme a lui la carta delle regole di comportamento in internet.



3. Gallega con tuo figlio. Accetta e chiedi che ti mostri quali sono i suoi siti preferiti e ascolta le sue osservazioni.



4. Fai vedere a tuo figlio come internet possa essere utile. Utile con la quando devi organizzare per esempio una vacanza.



5. Cerca di navigare insieme a tuo figlio, non lasciarlo da solo per troppo tempo, ricorda che internet non è una babysitter.



6. Se trovi in rete materiale illegale o presumibilmente dannoso per i bambini, puoi segnalarlo al sito della Polizia delle Telecomunicazioni.

7. Fa che il suo rapporto con internet sia equilibrato.



8. Educato alla prudenza, a non dare notizie personali, ad abbandonare un sito dai contenuti evasivi e a non incontrare persone conosciute in internet senza averne prima parlato con te.



9. Evidenza l'importanza dell'educazione e del rispetto nelle chat e nella posta elettronica.



10. Insegna a tuo figlio che non deve acquistare nulla in internet senza averne parlato con te.



11. Stabilisci contatti con altri genitori nella rete, diventa più esperto nell'utilizzo di internet.



La Polizia delle Telecomunicazioni

Vigilare sull'uso distorto delle tecnologie ed impedire che esse diventino veicolo di illegalità è questo lo scopo che si prefigge la Polizia Postale e delle Comunicazioni che, attraverso il Servizio centrale, i 19 Compartimenti con competenza regionale, e le 76 Sezioni con competenza provinciale, assicura una presenza articolata e diffusa in tutto il territorio.

Fenomeni come la pedofilia on-line, gli attacchi a sistemi informatici, le truffe perpetrate grazie all'utilizzo fraudolento di codici di carte di credito, la diffusione di virus informatici, l'illegittima duplicazione di materiali e diffusione di programmi tutelati dalla normativa sul diritto d'autore, sono alcuni esempi delle attività delittuose che vengono contrastate con sempre più intensità dal personale della Specialità.

A seguito dell'entrata in vigore della legge 269 del 1998, che ha previsto innovativi strumenti investigativi, la Polizia Postale e delle Comunicazioni è impegnata quotidianamente con tutte le drammatiche periferie in delicati servizi di polizia giudiziaria come le intercettazioni telematiche, le attività sotto copertura, l'acquisto simulato di materiale pornografico afferente minori e le relative attività di intermediazione.

È inoltre stato predisposto un sistema di messaggistica elettronica dotando la Specialità di indirizzi telematici ai quali far pervenire segnalazioni di violazione di norme penali nei settori di impiego.

A fini preventivi è stata implementata l'attività di monitoraggio della rete Internet riguardo alcuni fenomeni come la pedofilia, le sette religiose ed altre organizzazioni di vario tipo le cui attività potrebbero sconfinare in manifestazioni criminali o di odio razziale.



Conclusioni

- L'EDUCAZIONE È L'UNICO MEZZO PER ASSICURARE L'USO DI TUTTE LE OPPORTUNITÀ OFFERTE DALL'INFORMATION TECHNOLOGY MINIMIZZANDO I RISCHI RAPPRESENTATI DA QUESTA TECNOLOGIA; RISCHI LE CUI DIMENSIONI NON SONO ANCORA CHIARE: AD ESEMPIO IL 47% INSEGNANTI DENUNCIA DI ESSERE INVOLONTARIAMENTE VENUTO A CONTATTO CON MATERIALE PORNOGRAFICO

Conclusioni

- RAFFORZARE IL SENSO DI SÉ
- RENDERE RAGAZZE E RAGAZZI CAPACI DI DISTINGUERE TRA IMMAGINAZIONE E REALTÀ
- IN GRADO DI SAPER DIRE DI NO A SITUAZIONI SPIACEVOLI
- DETERMINANTE È DARE AGLI INSEGNANTI UNA FORMAZIONE SPECIFICA IN MODO CHE POSSANO AFFRONTARE IL PROBLEMA DELLA "SICUREZZA" DEGLI STUDENTI IN SENSO PIÙ AMPIO

Conclusioni

- LA GENERAZIONE ATTUALE ACCEDE AD INTERNET SENZA ALCUNA PREPARAZIONE
- BISOGNA QUINDI PENSARE A METODI PEDAGOGICI COME AIUTO: REGOLE QUINDI DI "BUONA EDUCAZIONE" (NETIQUETTE), SVILUPPO DELLA RESPONSABILITÀ INDIVIDUALE E DEL SENSO CRITICO, SONO STRUMENTI DA USARE ANCHE NELLA VITA REALE.
- IL CONTROLLO TECNICO (FILTRI, CONSERVAZIONE DEI LOG, SUPERVISIONE DELLE PROCEDURE) PUÒ SUPPORTARE LE MISURE EDUCATIVE MA NON PUÒ RICADERE SULLE SPALLE DEI DOCENTI, CHE DOVREBBERO INVECE POTERSI CONCENTRARE SULL'ASPETTO DIDATTICO.

Domande e risposte



alessandro.musumeci@istruzione.it



Tavola rotonda

SESSIONE I
TUTELA DELLA PERSONA
ED EFFICIENZA SOCIO-ECONOMICA

COORDINATA DA FRANCO CARLINI

Sessione I - Tavola rotonda

Tutela della persona ed efficienza socio-economica

Coordinata da Franco Carlini⁽¹⁾

Interventi di: 1. Gaetano Rasi; 2. Francesco Beraldi; 3. Domenico Campisi; 4. Stefano Quintarelli.

1. Gaetano Rasi⁽²⁾

In una società civilmente sviluppata non può non esistere - tra le qualità intrinseche dell'attività di produzione e distribuzione - la tutela dei dati personali in tutti i beni che l'incalzante innovazione tecnologica mette a disposizione dell'individuo non più atomo disperso nella massa, ma persona titolare del diritto alla sua riservatezza, alla sua libertà di scelta ed alla identità personale.

Per dimostrare quanto sopra partirò, in questa tavola rotonda, da una riflessione preliminare sul concetto di *efficienza socio-economica*.

Vanno infatti considerati i due aspetti relativi al progresso civile, nel quale si risolve il concetto di efficienza sociale, ed alla crescita produttiva, nella quale si risolve il concetto di efficienza economica.

Sul *primo* aspetto penso che non ci si debba soffermare più di tanto perché possiamo dare per acquisite due equivalenze. La prima: un più alto grado di civiltà comporta una elevata capacità culturale e di benessere dei singoli.

L'altra equivalenza consiste nella diffusione ad un sempre maggior numero di individui di quelle regole etiche e giuridiche che organizzano ed elevano il vivere comune.

Il problema si pone in maniera più acuta per quanto riguarda il *secondo* aspetto: quello dell'efficienza economica.

A questo proposito gli economisti distinguono il termine di *crescita* da quello di *sviluppo*.

Il termine *crescita* è impiegato nella dinamica economica per indicare l'andamento della produzione in senso puramente *quantitativo* e si differenzia dal termine *sviluppo*, concetto più complesso, che implica anche essenziali componenti *qualitative*.

Per questo secondo aspetto si parla di una *economia in sviluppo* quando non so-

(1) Giornalista

(2) Componente Garante per la protezione dei dati personali

lo la produzione cresce in senso assoluto, ma anche aumenta in senso distributivo, ossia rispetto alla popolazione.

È ovvio che non si tratta solo di una media statistica ottenuta dividendo la produzione globale (prodotto interno lordo, Pil) per il numero degli abitanti di una determinata società territorialmente individuata: Città, Paese, Stato, Nazione, Comunità, Confederazione, Area, etc. Deve trattarsi, per parlare di *sviluppo*, di produzione o di reddito pro capite *reali*, ossia *effettivamente distribuiti e apprezzati*.

In questa espressione *effettivamente distribuiti e apprezzati* sta anche il concetto di *qualità diffusa* nel godimento individuale dei beni prodotti ed offerti.

Dunque perché si parli di sviluppo in senso completo – e qui vengo al nocciolo del problema che ci interessa – è necessario che migliori il tenore di vita dei singoli per cui contano sia la qualità della produzione, sia il funzionamento delle infrastrutture, sia l'efficienza del mercato.

La più moderna sociologia economica accoglie come possibile una concezione di *crescita senza sviluppo*, ossia un aumento quantitativo di beni a detrimento della qualità della vita e quindi in presenza di un ridotto progresso civile (caso dei Paesi sottosviluppati, ma ricchi di materie prime), così come può concepirsi uno *sviluppo senza crescita* ossia in condizioni stazionarie della produzione purché tale circostanza sia accompagnata da una armonica ripartizione tra investimenti pubblici e consumi privati, e la produzione stazionaria sia ripartita equamente. Ovviamente lo sviluppo è compromesso da una “decrescita”!

Nella moderna concezione dunque l'elemento che caratterizza il concetto di *sviluppo*, rispetto a quello di crescita, non sta solo nell'aumento in termini reali, monetariamente misurati, del reddito medio pro capite. Tale caratterizzazione è infatti insufficiente.

Dunque, quello che conta - e che definisce pertanto la premessa del moderno processo di sviluppo - è la condizione nella quale opera una società in una determinata situazione di crescita diffusa per cui ad ogni movimento dei redditi maggiori corrisponde anche un aumento dei redditi più bassi. Ma il punto centrale non è ancora questo perché ormai si è consapevoli che lo sviluppo può avere dei limiti in due direzioni diverse ma alla fine produttrici degli stessi effetti negativi: da un lato l'esaurimento delle fonti delle materie prime ed energetiche e, dall'altro, l'inquinamento degli elementi essenziali alla vita: aria, acqua, terra.

Ed arriviamo così al *concetto di sviluppo civile*, per cui nei fattori di aumento del benessere entrano prepotenti e pervasive la *cultura* l'*eticità* e la *giuridicità*. La regolamentazione e, ove possibile, l'autoregolamentazione sono essenziali nel processo di sviluppo cosciente e condiviso.

Il passaggio successivo si riferisce, dunque, non tanto ad una società concepita come massa indifferenziata capace soltanto di produzione e di consumo, ma come

aggregazione consapevole e partecipativa di singole persone che hanno coscienza di se stesse, capacità di vita di relazione, discernimento nell'accesso ai beni della natura ed alle trasformazioni dell'uomo e, soprattutto, in grado di organizzarsi giuridicamente in istituzioni ed ordinamenti di garanzia e di sicurezza.

L'uomo moderno, e soprattutto quello post-moderno, viene così configurandosi come uomo sociale nella vita di relazione, ma anche come uomo-individuo titolare di dignità e di diritti inalienabili e ciò non solo per il fatto di esistere, ma anche perché impegnato a rispettare la dignità ed i diritti degli altri.

Non si tratta di utopismo perché l'uomo moderno è largamente convinto che la moralità e la giuridicità non si sviluppano in un costante progresso, ma danno luogo spesso a soste e a ripiegamenti e che le sempre più diffuse consapevolezze etiche e giuridiche non corrispondono alla integralità dei rispettivi comportamenti.

Il progresso civile è, infatti, frutto di una continua opera di contrastata conquista.

In quest'ambito, a mio avviso, va compreso nel moderno concetto di efficienza socio-economica, come sopra individuato nello *sviluppo*, il diritto alla tutela dei dati personali, come protezione della persona umana specie nell'era della comunicazione e dell'identità elettroniche.

Come è stato l'assunto iniziale, dunque, deve esistere in una moderna società sviluppata tra le qualità intrinseche delle merci e dei servizi, la tutela dei dati personali in particolare a seguito dell'incalzante innovazione tecnologica.

A questo punto va considerato il problema della formazione della volontà dei singoli nelle attuali configurazioni delle scelte di mercato. La questione non può essere affrontata sotto l'aspetto apparentemente più semplice, ma anche più fuorviante, secondo cui ad un maggiore interventismo regolatorio corrisponderebbe automaticamente una minor espansione del mercato (a causa dei vincoli alla libera circolazione delle informazioni, delle persone, dei capitali e dei beni) e, viceversa, una minore regolamentazione determinerebbe un aumento della domanda e dell'offerta.

Bisogna infatti evitare di confondere nei rapporti di scambio, i vincoli derivanti dalle norme fiscali e contrattuali e, in generale, dalle difficoltà esterne di accessibilità e di disponibilità, con le valutazioni di maggiore o minore convenienza e di maggiore o minore certezza delle parti nell'assumere le decisioni di vendita e di acquisto.

L'elemento personale è decisivo nella formazione della volontà rivolta alla vendita o all'acquisto delle merci e dei servizi. La determinazione si fonda, come detto, su valutazioni sinallagmatiche aventi per oggetto a) il rapporto tra il sacrificio per il prezzo da pagare e l'utilità prevista per il bene da acquisire; b) la convenienza a privarsi del bene in relazione al guadagno calcolato nell'incasso del corrispettivo; c) il grado di rischio nelle modalità di vendita o di acquisto: fornitura immediata o differita, pagamenti in contanti o dilazionati; d) garanzie rispetto ad eventuali vizi occulti; e) bontà dei mezzi di pagamento; f) fiducia nella assistenza post vendita (pez-

zi di ricambio, riparazioni, celerità intervento, ecc.); g) grado di affidabilità nella gestione del rapporto (professionalità, riservatezza, personalizzazione, continuità, grado del servizio, qualità della prestazione, adeguatezza delle informazioni, istruzioni per l'uso, ecc.).

I punti c) e g) riguardano i trattamenti dei dati personali e la regolamentazione delle informazioni per es. delle centrali rischi. Come appare evidente una corretta gestione delle informazioni riguardanti coloro che le raccolgono o le forniscono danno *certezza* al mercato: i venditori tendono ad espandere l'offerta e gli acquirenti sentono tutelati i diritti e incrementano la domanda. La regolamentazione dell'elemento *responsabilità* nei comportamenti a prestazioni corrispettive fornisce fiducia e costituisce la base alle fasi espansive del ciclo economico.

Il rispetto del cliente nel trattamento dei dati personali non viene più a costituire un costo che incide negativamente sul prezzo del prodotto finale, ma rappresenta un valore aggiunto che fa premio e quindi determina la selezione nella competizione del mercato.

L'esperienza in Italia (e non solo) di questi primi anni di vigenza ed applicazione della legge sulla tutela dei dati conferma, insieme con l'accrescimento culturale, la validità delle ricadute economiche connesse all'elevazione qualitativa dei rapporti negoziali.

Un'ultima considerazione. Com'è noto, per Schumpeter (il grande economista europeo, poi emigrato negli Stati Uniti) nei mercati delle economie aperte è il saggio di progresso tecnico che regola il saggio di profitto e quindi determina il saggio di interesse. E poiché, oggi più che ieri, l'*accelerazione* nell'introduzione di *innovazioni* è il centro del processo evolutivo del sistema economico contemporaneo e, a livello macroeconomico, del comportamento dei singoli operatori, è necessario che si crei un equilibrio virtuoso tra l'espansione economica e le garanzie per i soggetti destinatari degli impulsi che spingono le innovazioni le quali, a loro volta, determinano l'espansione economica.

Tra le garanzie, come abbiamo visto, fondamentali sono quelle che tutelano l'uomo nel trattamento dei suoi dati personali.

L'imprenditore innovativo, il moderno imprenditore schumpeteriano non può più competere e vincere nel mercato evoluto senza il rispetto del protagonista destinatario della produzione: nello scambio bene/prezzo emerge sempre più il diritto dell'uomo alla dignità, alla riservatezza, alla identità, alla libertà ed alla sicurezza nel trattamento dei dati personali.

2. Francesco Beraldi⁽³⁾

Il prof. Rasi ha citato un economista della prima metà del Novecento, Schumpeter, contemporaneo di Keynes, che mi è molto caro poiché nel '98, fondando quest'azienda ho deciso di utilizzare la leva dell'innovazione tecnologica, come modello di business per farne la base per lo sviluppo della mia impresa. Mi è stata subito chiara l'importanza e la incisività che i sistemi che andiamo a proporre sul mercato hanno nei riguardi della società in generale.

Schumpeter era una persona che sottolineava molto l'aspetto sociale dell'impresa anche perché riteneva che non erano tanto i capitali che facevano la cultura d'impresa, ma bensì che era la cultura imprenditoriale, e quindi quella capacità che in pochi hanno di individuare le innovazioni in grado di modificare un ciclo produttivo, che sta invecchiando e non è più competitivo.

Questa è la storia della mia azienda, il motivo per cui sono stato invitato a questo convegno.

Ritengo necessario approfondire due temi: il primo è una conseguenza di quello che ho ascoltato stamattina, ma che è utile ribadire. Da quando la tecnologia digitale ha pervaso il mondo (vi ricordo che questa è stata la leva che ha permesso agli Stati Uniti d'America di acquisire un vantaggio economico molto importante e la prossima probabilmente saranno le biotecnologie) si è reso necessario fare cultura dell'uso di questa tecnologia. Il saggio di sviluppo economico deriva dal saggio di impiego delle tecnologie.

Il secondo tema riguarda la responsabilità sociale. Noi che facciamo cultura informatica abbiamo il dovere di sensibilizzare il pubblico su quali sono le conseguenze di un uso non corretto dell'informatica.

Quindi sono molto d'accordo sui temi toccati che spingono verso l'utilizzazione di tecnologia vedendola come un'opportunità per creare sistemi che siano compatibili con quelli che sono i contesti sociali. Questo spesso non viene fatto poiché la cultura delle aziende che vendono tecnologia è quella di vederla come un fine, non come un mezzo per aiutare le imprese e la pubblica amministrazione a migliorare complessivamente sia la produzione sia l'azienda nell'ottica delle conseguenze sociali.

Dopo questa premessa causata dalle riflessioni fatte ascoltando i relatori precedenti, l'argomento su cui sono stato invitato a parlare riguarda le caratteristiche della nostra azienda impegnata da due anni nel cercare di costruire prodotti e soluzioni innovative e non solo tecnologia. Da poco abbiamo annunciato i primi prodotti per la gestione del cosiddetto *rischio* nella Sanità.

La Sanità è un argomento che da qualunque punto lo si tocchi, ha dei risvol-

(3) Presidente Orangee srl

ti sociali. Non ho certo la capacità di trattare tutte le problematiche che coinvolgono la Sanità, ma credo possa essere utile raccontarvi la mia esperienza da imprenditore che due anni fa era completamente all'oscuro dei problemi nella Sanità (salvo che anch'io ho qualcuno a me vicino che è stato un paziente nelle strutture Sanitarie!) raccontarvi cioè come, partendo da un'idea di innovazione tecnologica, stiamo ora cercando di occupare un importante segmento del mercato e a dover affrontare i problemi che riguardano anche la privacy.

Tra il 1999 ed il 2000, cercando una finalizzazione per l'azienda che non fosse solo tecnologia, abbiamo individuato un'area che era quella della nuova evoluzione dei sistemi informativi, cioè la gestione delle informazioni come *gestione della conoscenza* basata su una serie di strumenti che si chiamano *Ontologie di Dominio*.

Per fare questo abbiamo affrontato il mercato della Sanità che ci pareva l'unico settore - scusate se lo chiamo settore industriale - che utilizzava certamente tutte le tecnologie possibili, ma non le utilizzava in quello che tipicamente è il processo produttivo, cioè nella gestione dei pazienti, ovvero nella gestione dei percorsi sanitari di cura.

Nell'esaminare la letteratura in materia ossia leggendo decine e decine di libri che trattano il *Rischio in Sanità* è emerso che gli errori in medicina, sono tanti. Si contano circa 50.000 errori che causano danni alle persone in Italia, 120.000 in America; si tratta di statistiche dell'Institute of Medicine americano, e dell'Asinform Rischio Sanità in Italia.

In quest'ambito la cultura medica ha sviluppato la teoria dell'analisi del *Rischio in Sanità* al fine di assicurare la *qualità* nelle prestazioni sanitarie. Il paziente va accompagnato in un percorso sanitario guidato da quelle che sono le indicazioni chiamate *Evidence Based Medicine*, e da tre principi fondamentali l'*accuratezza*, l'*efficacia* e l'*efficienza*.

L'*accuratezza*, perché bisogna individuare il percorso: gli esami giusti, le somministrazioni giuste; l'*efficacia* ossia il risultato positivo (talvolta le cure hanno delle controindicazioni): bisogna raggiungere il miglioramento della salute; l'*efficienza*, ossia un rapporto ottimale spesa/risultati, perché nella Sanità vi sono questioni di costi spesso eccessivi o inutili.

Nell'affrontare questi argomenti si è però sorvolato il problema della privacy. Ho fatto un po' di ricerche sia frequentando gli ospedali sia consultando Internet. La giostra della documentazione cartacea in un ospedale da quando un paziente viene accettato è allucinante; si cammina solo ed esclusivamente, quando si è fortunati, con pezzi di carta che girano tra le corsie dall'infermiere al medico, dal medico all'infermiere e ai laboratori di analisi. Pensate anche al problema che ha il medico in una corsia con dei malati, noi lavoriamo nel settore oncologico, ove la comunicazione al paziente avviene spesso in prossimità di altri pazienti.

Poi c'è un altro problema. Una statistica del *British Journal*, evidenzia che le violazioni della privacy sono sistematiche. Studenti medici hanno rilevato che su 113 percorsi in un ascensore, 11 volte era stata violata la privacy: i medici a fianco di estranei parlavano di problemi inerenti un paziente e la sua malattia. Aggiungiamo a questo quanto ha scritto il presidente Rodotà, che va ancora più avanti in merito alla prevenzione affrontando il discorso del genoma umano e della delicatezza delle informazioni in materia che potrebbero arrivare a determinare o meno l'assicurabilità di un paziente o l'offerta di un posto di lavoro.

Questi sono alcuni dei temi che mi sono trovato ad affrontare nel cercar di dare delle linee guida per un moderno sistema Sanitario, fondato sulla tecnologia informatica nella gestione dei percorsi Sanitari.

La prima fase della qualità sanitaria è la cosiddetta *formalizzazione scritta* con la quale affrontare e risolvere il problema della tutela dei dati riguardanti la persona.

Questo si può fare grazie alle tecnologie informatiche che garantiscono sia la riservatezza dell'accesso, sia anche la criptazione dei dati; la cosa più importante riguarda la strutturazione dei percorsi sanitari, i dati medici e gli episodi del percorso di cura che debbono essere distinti dai dati anagrafici del paziente.

Non è vero che per fare la ricerca scientifica, su quelle che sono le conseguenze della somministrazione di un farmaco, per es. in un percorso chemioterapico, si debba accedere anche ai dati e alle informazioni di chi è oggetto di quella cura.

Certamente molto è affidato alla sensibilità di ciascun operatore, anzitutto quello sanitario, ma anche noi che facciamo cultura dell'informatica e delle tecnologie siamo responsabili nell'allestimento degli strumenti informatici.

Sappiamo tutti che questa non è materia di studi universitari, ove non vi sono esami che preparino e informino su questi aspetti.

Io assumo mediamente 5 o 6 giovani all'anno e purtroppo questi temi non sono presenti nel loro bagaglio intellettuale.

Grazie per l'attenzione.

3. Domenico Campisi⁽⁴⁾

L'innovazione tecnologica, con riferimento alla privacy, pone problemi che possiamo classificare come facili ovvero difficili.

I problemi facili possono essere risolti con un uso intelligente della tecnologia, con l'applicazione di poche norme, e l'utilizzo del buonsenso. Tuttavia, anche su questi problemi semplici c'è ancora parecchio da fare, e ciò giustifica la mole non trascurabile del lavoro ordinario di questa Autorità; ed anche le richieste, talvolta banali, che provengono da un pubblico sempre più vasto ed attento. Io stesso qualche tempo fa ho richiesto un parere sull'uso nelle aule universitarie di video telefoni da parte di colleghi o studenti.

I problemi semplici possono essere definiti, quindi, come quelli che possono essere risolti senza il coinvolgimento invasivo di competenze specifiche e che necessitano, tuttavia di una costante e, qualche volta, strenua sorveglianza.

Accanto ai problemi facili ci sono quelli che possiamo classificare come difficili o molto difficili. Il fatto che siano difficili, motiva il fatto di essere qui tutti assieme: i problemi difficili richiedono l'intervento di specialisti di vari settori e momenti di riflessione e pausa; sono problemi che non si risolvono attraverso la semplice emanazione di atti accompagnati dalla sorveglianza e l'attenzione.

Richiedono un intervento più alto in cui le diverse competenze vengano integrate nel rispetto dei punti di vista disciplinari. Sono questi i problemi in cui è necessaria una forte interazione di competenze tecnologiche e scientifiche, di un coeso consenso sociale, di fonti giuridiche accreditate.

Fra i problemi più difficili, cito quelli di schedatura per il riconoscimento e la mappatura del Dna, oppure più semplicemente per il trapianto di organi o del midollo: Interventi che vanno in direzione del progresso medico, verso l'allungamento della vita ed il miglioramento della sua qualità. Problemi in cui, per la loro natura (la vita e la morte), i fattori etici possono essere considerati dominanti.

Possiamo individuare, anche, problemi moderatamente difficili, in cui i fattori etici non sono dominanti. Mi riferisco a quei casi in cui la società si è già data delle regole e la difficoltà nasce solo dall'uso di nuove tecnologie o dalla loro non facile utilizzazione. Sono questi i casi legati al commercio di beni e più in generale alle transazioni. Più specificamente, alle transazioni che sempre di meno vengono perfezionate nei luoghi fisici convenzionali (il mercato ortofrutticolo; la borsa valori...) e sempre di più su rete o attraverso la rete. Pensiamo alle transazioni di borsa ma anche ai semplici acquisti effettuati on-line. Acquisti reali e non virtuali effettuati nelle diverse catene di supermercati ed ancora attraverso siti specializzati anche: libri, musica, beni durevoli e non, mutui e consulenze che vengono distribuiti da ogni

(4) Ordinario di ingegneria gestionale – Università di Roma “Tor Vergata”

parte del mondo in ogni parte del mondo. In questi casi la difficoltà nasce dal fatto che lo scambio, non solo non è contestuale ma, non nasce o si esaurisce in un luogo fisico o geografico preciso.

Le transazioni viaggiano su rete in tutta la rete: talvolta in violazione di norme e principi contrari non solo alla privacy ma ai codici ordinari. La tipica risposta, in questi casi è di tipo legislativo e repressivo: intervengono corpi speciali, la Polizia Postale, ecc. Anche in questi casi, tuttavia, la semplice repressione può non bastare ed occorre stabilire regole sociali innovative per fare fronte all'irruenza della tecnologia.

Definisco questi problemi come moderatamente difficili perché le innovazioni, spesso, non sono originali bensì mutate da altri contesti: pensiamo all'analogia fra l'uso dei collaboratori di giustizia, ed il reclutamento degli hacker che in vari paesi del mondo vengono utilizzati proprio per migliorare la vigilanza e la repressione, per addestrare ed aggiornare gli esperti di reato informatico.

Le transazioni su rete sono più perniciose di quelle convenzionali perché, in questi casi, è proprio, l'informazione a fornire valore aggiunto al bene o servizio scambiato. Commentiamo insieme qualche dato: negli Stati Uniti, nel 92% dei casi di transazioni on line, ci sono stati dei problemi, problemi semplici, che hanno infastidito le transazioni. Secondo recenti stime, nel 2002, un terzo del mercato potenziale, è stato perso a causa della scarsa trasparenza e protezione del mercato. Eppure eravamo nell'anno successivo alle Torri Gemelle, il mercato che già era fortemente controllato ma l'efficacia dei controlli non era pienamente percepita.

Dal mio punto di vista, il mercato su rete è un mercato che pone problemi di privacy difficili. Problemi difficili perché gli interessi leciti e meno leciti, molteplici e diffusi, acquistano valore e si diffondono con ogni singola transazione: l'economia della rete è un'economia con rendimenti di scala crescenti il cui fattore di crescita è amplificato dalla qualità delle singole informazioni. Un mercato di questo tipo non si autoregola: gli interessi sono diffusi ma anche in conflitto: è possibile aprire siti con gli stessi contenuti un po' dovunque nei paesi del mondo.

Le reti stesse sono gestite da imprese ad alto potere di mercato calmierate e sorvegliate con molta difficoltà da enti e garanti diversi (in Italia: Ministero delle Tlc, garante delle Tlc, Antitrust ...).

Come conseguenza, anche la protezione della privacy elettronica è un mercato esso stesso altamente profittevole. Un mercato fatto di una miriade di semplici interventi e tuttavia ricco abbastanza da poter rilasciare benefici sociali o collettivi affatto trascurabili. Penso ad un mercato costituito da una miriade di interventi efficaci e tracciabili ma con invasività che sia temporalmente limitata.

Quando siamo di fronte a problemi difficili, la soluzione non solo non mai immediata (anche se semplice) ma non viene mai individuata da chi sta sul campo. Se pensate all'inventore delle buste di plastica trasparente (in cui vengono sigillati gli ac-

quisti antecedenti) che protegge i supermercati dal taccheggio, non dovete pensare ad un gestore della sicurezza ma ad esperto di sicurezza che ha ideato il dispositivo.

Così i problemi difficili legati all'uso di nuove tecnologie spesso non sono risolti direttamente da lavoro sul campo, ma da chi ha una, visione laterale e quindi più creativa del problema.

Siamo lontani dal 1929 quanto tramontò, con il crollo delle Borse, il mito dell'inviolabilità del postulato della mano invisibile di Adamo Smith; il mito dell'auto-regolazione dei mercati, della necessità di mantenere lontano l'intervento dello Stato.

A valle della crisi del ventinove, due signori imposero il loro punto di vista.

Un dandy inglese, Lord Keynes, che finalmente riuscì, viaggiando negli Stati Uniti, a divulgare la sua idea, che lo Stato che dovesse intervenire per salvare le sorti di milioni di disoccupati: da lì nacque la macro-economia, oggi strumento di analisi proposta da scuole di pensiero diverse, sia essa quella di Chicago ovvero quella di Cambridge ma anche strumento di intervento di ogni nazione.

L'altro signore che intervenne, contemporaneamente nella scena mondiale, fu Pio XI che con un'enciclica introdusse il concetto di sussidiarietà: non intervenga lo Stato quando i privati si dimostrino competenti; collaborino altrimenti i privati con lo Stato perché interesse privato e bene pubblico possono essere conciliati.

Queste due principi, sono ancora validi e possono essere mutuati in situazioni difficili quando i sistemi tendono a non autoregolarsi. Nei casi difficili di cui abbiamo bevante discusso non occorrono nuovi principi ma una nuova applicazione di principi consolidati. Per questi problemi occorre più Stato. Ma non è un intervento coercitivo quello che serve quanto un tavolo attorno a cui sedersi, un pensatoio.

Per fare il punto il punto sulla situazione, per fissare i paletti. Un pensatoio, ampio, allargato nella dimensione spaziale (l'Europa) e nelle competenze. Un tavolo che ci consenta di affrontare con dettaglio i problemi e le soluzioni di cui stiamo dando solo dei cenni accennando qui ed ora: arrivederci.

4. Stefano Quintarelli⁽⁵⁾

Ci sono un paio di temi che mi sono piaciuti molto nella mattinata, sono stati toccati dal dott. Dix, dal professor Rasi, riguardano la fiducia e le regole del mercato.

Io credo che noi siamo di fronte ad una trasformazione epocale, sono circa 10.000 anni che l'uomo ha incominciato con l'agricoltura. La nascita dell'agricoltura, ha comportato di fatto la fine del nomadismo, l'uomo stanziale, e da qui è nato poi in sequenza tutto.

Il mercato, cioè il mondo nel quale abbiamo vissuto, sino ad oggi, è frutto dell'inizio dell'attività agricola, come diceva prima il professor Campisi.

Mi ritrovo perfettamente; chiunque di noi potrebbe scrivere un saggio di 400 pagine sui pomodori dalla coltivazione alla commercializzazione, dai fertilizzanti all'industria dei trattori.

Sono solo 10 anni che affrontiamo, che c'affacciamo, sul mondo della smaterializzazione.

In Italia Internet nasce commercialmente, di fatto, nel 1994; sono passati 10 anni, e qui stanno cambiando tutte le regole del gioco, spostare atomi ha delle conseguenze di cui è stato detto molto chiaramente anche questa mattina, dal presidente del Clusit, prof. Bruschi.

Spostare atomi ha delle regole completamente diverse dallo spostare l'informazione; l'informazione vive 24 ore al giorno, viaggia alla velocità della luce, è globale, non ci sono latenze, c'è tutta una nuova generazione di problemi, e noi dobbiamo cercare di capire come questo fenomeno cambierà il mondo.

In un'intervista di qualche settimana fa su Il Sole 24 ore, l'ing. Catania, all'epoca presidente dell'Ibm Italia, diceva: l'80% del valore dei prodotti, sta al di fuori del prodotto, ovvero sta nella parte informativa.

Questa è la cosa che dobbiamo capire intimamente: ci avviciniamo a un mondo dove è sempre più predominante la parte di informazione; è un nuovo mercato, è un nuovo mondo.

Le regole del mercato precedente, probabilmente, non sono sufficienti.

Il mercato è basato su regole che lo governano, l'autorità, la sorveglianza, sono essenziali per far funzionare il mercato; senza il mercato non c'è sviluppo economico; non c'è sviluppo sociale, eccetera.

Io credo che siamo ad un punto di svolta, alcuni cambiamenti evidenti sono questi: l'I-Pod consente di avere 10.000 canzoni sempre con noi.

C'è un'intervista oggi, mi sembra sul Wall Street Journal o sul Financial Times, in cui Steve Jobs parla dell'evoluzione dell'audio e della distribuzione del video: oggi la tua musica sempre con te. Domani, perché no, anche i tuoi video

(5) Direttore strategie Equiliber.org

sempre con te. È una questione di dimensione dei dischi, un problema che non è così rilevante.

iTunes, il servizio di commercio elettronico di musica online della Apple, ha venduto in poco più di sei mesi circa 80 milioni di canzoni; su iTunes già si distribuiscono trailer video.

Voglio incrociare alcune cose che sono attuali:

Ci sono delle Società Telefoniche, mi consta per esperienza diretta, che “ascoltano di nascosto”, con dei sistemi automatici le conversazioni fatte verso i call center, e sulla base delle richieste degli utenti, propongono all’operatore le schermate informative più attinenti rispetto a quello che l’utente dall’altro lato del filo sta richiedendo: telefona una signora e dice: “sono interessata al telefono rosso”, il sistema percepisce il “telefono rosso”, e propone la videata giusta all’operatore che a questo punto può chiedere precisazioni: “quale telefono rosso? Quello col display o quello con la segreteria?”

In questo modo si personalizza il rapporto e si aumenta la qualità del dialogo dell’operatore.

Sistemi del genere vengono usati anche per i promotori finanziari, che quando fanno le telefonate devono fornire disclaimer vari; per assicurarsi che queste informazioni vengano date ci sono dei sistemi automatici che ascoltano il parlato,

Nota bene: indipendentemente dall’operatore.

Sistemi di questo genere esistono e sono già in uso da anni, quindi il problema di passare da un segnale fonico, da una curva audio, da un segnale audio, a informazione digitale, è un problema sicuramente risolvibile, risolto e risolvibile, è solo una questione di costo, e il costo è solo una questione di tempo.

Nel 1994, quindi 10 anni fa, Bill Gates aveva aperto il Comdex rinforzando lo slogan che in realtà, aveva lanciato prima: “information at your fingertips”. Nel 2005 ci sarà una grandissima quantità di informazione nel pianeta, raggiungibile direttamente dalle vostre dita, dal vostro personal computer, o dal vostro dispositivo mobile. Questo è evidente che è successo, è nell’esperito di tutti noi.

Un’altra cosa meno nota sono le tecnologie linguistiche e i motori semantici.

Ovviamente avere tutta l’informazione alla portata delle punta delle dita vuol dire capacità di indicizzazione, e capacità di reperimento delle informazioni. Le tecnologie linguistiche e i motori semantici sono in grado di estrarre in qualche modo il significato a partire da un testo.

Un oggetto molto bello che io uso che si chiama Copernic Summarizer: un prodotto canadese. A fronte di un testo gli chiedi: fammi un riassunto su 5 righe. È un modo col quale io riesco a leggere qualche centinaia di articoli leggendo solamente il riassunto; sbaglia veramente poco.

Mettendo insieme queste cose, combinando questi 4 ingredienti che vi ho da-

to, vi lancio una provocazione, beninteso non è detto che accada mai a livello di utente finale.

Incrociamo questi 4 ingredienti, immagazzinamento del video, riconoscimento automatico del parlato, l'indicizzazione automatica, e la possibilità di creare riassunti con relazioni con pezzi di documenti.

Supponiamo 75 anni di vita di una persona, registrando 16 ore al giorno il video, e mi chiedo fra quanto sarà possibile farsi il film della vita?

Facciamo due calcoli sulla base delle tecnologie attuali per attuali non intendo quelle che sono oggi sul mercato ma quelle che sono oggi all'interno dei laboratori e che usciranno fra poco sul mercato.

Questi dati, come si vede, sono ovviamente del laboratorio di ricerca dell'Ibm, che sullo Storage sono fortissimi. Su un hard disk da 6 centimetri e mezzo di diametro, la tecnologia sarà disponibile intorno al 2005.

Quindi potrà esistere un oggetto che io mi tengo in tasca, con una video camera ad esempio sugli occhiali, collegata via wireless con il sistema ultrawideband, a un mio storage tipo I-Pod che mi tengo in tasca. Potrò registrare 16 ore, e naturalmente a questo punto posso fare subito attività di indicizzazione, categorizzazione, eccetera.

Se penso ad un hard disk di 2 centimetri e mezzo di diametro, grosso modo quello delle macchine fotografiche, la tecnologia sarà disponibile intorno al 2007/2008, queste sono previsioni di questo gruppo che si occupa di superparamagnetic effect ai laboratori dell'Ibm.

Naturalmente il prezzo sarà esorbitante, e la domanda giusta è (ripeto, è una provocazione): quand'è che un dispositivo, questo genere potrà avere un market price orientativo di 500 dollari? (Oggi l'I-Pod costa 400 dollari e ha il 70% del mercato della musica digitale)

Con un hard disk da 6 centimetri e mezzo, grosso modo siamo intorno al 2006. con un hard disk da 2 centimetri e mezzo, grosso modo, siamo intorno al 2015.

Ora, è evidente, non siamo in grado di dire se questa è una cosa che potrà accadere, ma il messaggio che vi voglio passare è che il futuro non è immediatamente predicibile e le conseguenze sociali, giuridiche ed economiche lo sono ancora meno.

Riallacciandomi a quello che diceva scherzosamente Campisi, la sua vita non è cambiata nel '29, quando è nata sua suocera; la sua vita è cambiata 40 - 50 anni dopo quando ha sposato sua moglie. Nel '29 si sono determinate le condizioni perché cambiasse la sua vita.

Anche adesso si stanno determinando delle condizioni, ma i cicli si abbreviano, i cicli si abbreviano e questo richiede velocità di analisi ed intervento.

Pensiamo al fenomeno Napster; una caratteristica dei sistemi materiali, in cui l'informazione viaggia alla velocità della luce, e in cui le barriere si dissolvono, può

portare a posizioni pervasive, in tempi estremamente brevi, e una volta date queste condizioni, è molto difficile poter tornare indietro, quindi occorre un'attività di sorveglianza, di regolamentazione in quel senso.

Questo serve a dare fiducia agli utenti che si trovano in un mondo così turbolento e di evoluzione tecnologica, altrimenti la non comprensione di queste evoluzioni costituisce un freno al mercato, quindi è fondamentale che ci sia un'attività di controllo e di monitoraggio che deve avere, necessariamente dei tempi molto veloci di intervento.

Ci sono delle cose che viviamo già oggi, che ci passano abbastanza in modo impercettibile, forse perché sono destinate ad un pubblico limitato di utenti, però già oggi è possibile, e ci sono svariate centinaia di migliaia di persone, in Italia, che lo fanno, fruire dei contenuti audio/video via Internet.

Questa è un'indagine fatta dalla Aiip, commissionata alla Swg alla fine dell'anno scorso, e viene fuori abbastanza evidentemente che la stragrande maggioranza degli utenti, ha paura a fornire i propri dati a fronte della fruizione di un contenuto audio/video.

Ma questa è un'attività che già viene erogata, che già viene fatta, e sul quale non c'è una legislazione specifica; se pensassimo ad un sistema del genere legato alla televisione tradizionale, tutti gli ovvi problemi li capiremmo tutti.

Vado avanti, direi che i grafici sono abbastanza autoesplicativi, la cosa interessante è che c'è una parte grosso modo il 7 / 8 % degli utenti che considera che non vorrebbe fornire i dati perché lo troverebbe scomodo, ma se il sistema lo potesse fare in automatico, sarebbe accettabile.

Questa è una cosa sulla quale, ribadisco, ci sono già delle attività commerciali in corso, e probabilmente un intervento per capire e stabilire le regole del gioco, consentirebbe di aumentare la fiducia degli utenti, e quindi sviluppare di più il mercato.

Il Tricorder è un oggetto di fantascienza, è il comunicatore di Star Trek, un oggetto che è uno dei rari esempi in cui la scienza ha anticipato la fantascienza, il tricorder era posizionato nei film di Star Trek intorno al 2300, è un oggetto che è molto simile a un telefonino di oggi.

È un mercato molto tumultuoso, capire che cosa sarà possibile, che cosa non lo sarà, è molto difficile, ed è molto difficile soprattutto perché il mercato è composto dalla massima parte da persone che non sono esperte di tecnologia, altrimenti saremmo tutti tecnologi e non ci sarebbe altro mercato, quindi per definizione sono persone normali, il mercato è composto da maggioranza da persone non tecnologiche.

E qui vengo al fine di Equiliber. Equiliber è un'associazione che abbiamo fondato insieme con un pò di tecnologi di tutta Italia, che ha l'obiettivo di migliorare le conoscenze, offrendo informazioni, facendo studi, conferenze, e divulgazione, su

materie tecnologiche, con un linguaggio divulgativo, il target è che mio padre di 83 anni, debba capire gli articoli.

Controlliamo molto attentamente quelle che sono le discontinuità, che possono generare cambiamenti nei mercati, e quindi opportunità e crisi (che sono la stessa cosa, da un certo punto di vista).

Il web ha cambiato il paradigma, da “stampa e distribuisci” a “distribuisci e stampa”, l’Rfid sarà un’altra discontinuità e quindi non mi dilungo, ne ha parlato questa mattina molto bene Dix, la Voice over Ip sarà un’altra cosa che cambierà le regole del gioco, la Voice over Ipp in sede d’utente.

Questa mattina abbiamo sentito parlare anche di spam da Musumeci, se la telefonata non costa nulla, io potrei avere un robottino che mi telefona per cercare di vendermi il Viagra, e avere lo spamming su internet phone, causandomi un danno di tempo, e questo rischierebbe addirittura di fermare il mercato della Voice over Ip, quindi è necessario che ci siano delle regole.

Altre discontinuità sono il free open source, il superparamagnetic effect nella parte dello storage, ecc.

Concludo dicendo che la tecnologia è complessa. È difficile anche per gli addetti ai lavori, capire quali saranno i trend.

Occorre dal nostro punto di vista, un controllo e un intervento rapido per la creazione di regole di mercato, perché senza la creazione delle regole si distrugge valore e non se ne crea.



Interventi

SESSIONE II
NUOVE TECNOLOGIE
E SOCIETÀ DELL'INFORMAZIONE

PRESIEDUTA DA MAURO PAISSAN

Sessione II – Nuove tecnologie e società dell'informazione

Sicurezza e transnazionalità

Mauro Paissan⁽¹⁾

Sommario: 1. Sicurezza; 2. Transnazionalità

“Nuove tecnologie e società dell'informazione”: questo il titolo attribuito alla sessione che sono stato invitato a coordinare. A me spetta dar la parola agli oratori, e a questo compito mi atterrò. Mi sia consentita solo una breve introduzione, su due profili specifici delle tematiche implicate dalle nuove tecnologie. Si tratta di aspetti particolari che stanno a cuore al Garante, e in generale alle Autorità di controllo, e che rappresentano una vera sfida per l'effettività della protezione dei dati: 1) la sicurezza nelle tecnologie e 2) le implicazioni della dimensione sopranazionale tipica delle reti di comunicazione.

1. Sicurezza

Ho parlato di “sfida per le Autorità di protezione dei dati” perché esse vengono messe di fronte ad una realtà continuamente mutevole, rispetto alla quale devono dotarsi anzitutto di un patrimonio conoscitivo tecnologicamente elevato per essere in grado di assolvere ai propri compiti istituzionali. Si possono discutere le forme di soluzione del problema (personale interno o collaboratori indipendenti esterni), ma non la sua sostanza; comunque, non può (più) essere eluso né sottaciuto.

Si tratta di un aspetto che ci porta dritti dritti al problema delle risorse assicurate alle Autorità indipendenti affinché le medesime possano svolgere la propria funzione, pena l'esclusione del mondo “virtuale” (delle tecnologie) dalle garanzie che, pur a fatica, l'ordinamento cerca di apprestare per il mondo “reale”.

Noi dovremmo intervenire sulla mutevole realtà tecnologica e rappresentarne i rischi per i diritti fondamentali della persona (questi, in sintesi, i compiti istituzionali attribuitici). E dovremmo farlo parlando sia agli interlocutori istituzionali – Parlamento e Governo – sia ai cittadini, che hanno un “diritto” ad essere infor-

(1) Componente Garante per la protezione dei dati personali

mati sulle vicende che tanto direttamente li coinvolgono. Ma per fare ciò, dobbiamo avere una seria e approfondita comprensione della realtà, con competenze e sensibilità realmente pluridisciplinari. Quanto meno questa sensibilità il Garante vorrebbe dimostrare nell'organizzare anche iniziative quali quella di oggi.

Se il profilo della sicurezza nelle tecnologie (si è usato a questo proposito il termine “sicurmatica”) ha i caratteri della trasversalità, essendo funzionale ad assicurare protezione ad una pluralità di beni protetti dall'ordinamento giuridico, esso gioca un ruolo centrale nella protezione dei dati personali e della riservatezza delle persone. Il Garante non può osservare dalle seconde file le evoluzioni che caratterizzano questo settore. È – deve essere – al contrario, uno degli *attori* principali.

Se fosse necessaria una prova di queste mie affermazioni, si pensi al ruolo attribuito al documento programmatico per la sicurezza nella disciplina di protezione dei dati e alle costanti richieste provenienti dalle Autorità di garanzia e rivolte al mercato, tuttora per lo più inevase, di sviluppo di *privacy enhancing technologies* (PETs).

Se, dunque, la sicurezza, quale preconditione della *privacy*, rappresenta lo sfondo di alcuni interventi che seguiranno, questi si concentreranno su una specifica tecnologia, quella delle reti “senza fili”, rispetto alle quali – spesso all'insaputa degli utenti – problemi di sicurezza sono certamente presenti.

2. Transnazionalità

Le reti di comunicazione, lo sperimentiamo fin troppo bene ogni giorno, esaltano un altro degli aspetti che caratterizza la “società dell'informazione”: la transnazionalità.

Transnazionalità delle tematiche e, dunque, loro omogeneità al di là dei confini nazionali. Ma anche transnazionalità nel senso che le violazioni alle discipline di protezione dei dati possono essere realizzate al di fuori dei confini nazionali: e dunque, al di là dei poteri delle Autorità nazionali di controllo.

Una efficiente ed intelligente cooperazione internazionale è allora la preconditione perché i frutti avvelenati della “irrilevanza dei confini” possano essere efficacemente combattuti. Ma la cooperazione è un tesoro difficile da conquistare: richiede sforzi mirati e valori di riferimento condivisi. La cosiddetta “globalizzazione dei diritti” rischia di ridursi a bello slogan.

Nel 2000, in occasione della Conferenza mondiale sulla privacy, si approvò a Venezia una Carta che tra l'altro diceva:

“Alla luce del riconoscimento della privacy come diritto fondamentale della persona e quale elemento costitutivo della libertà del cittadino, il nostro obiettivo dovrebbe essere il riconoscimento a livello globale di linee-guida per il trattamento dei dati personali. (...)”

Ai cittadini verrebbe così assicurato universalmente un livello di garanzie adeguato e maggiormente condiviso, indipendentemente dal luogo in cui i dati sono trattati e dagli strumenti con i quali tali garanzie sono attuate a livello nazionale e internazionale”.

Le conclusioni della Carta di Venezia devono oggi più che mai essere sostenute. Più realisticamente, però, è necessario consolidare a livello “regionale” la conquista rappresentata dalla protezione dei dati. Essa, pur nel difficile processo costituenti europeo, ha ormai fatto ingresso – data la sua presenza nella Carta dei diritti fondamentali e nel Progetto di trattato europeo – nel Dna dei cittadini europei.

I principi di protezione dei dati, entrati, un pò di soppiatto, dalla porta larga della circolazione dei beni e servizi, e dunque del mercato (con la direttiva 95/46/CE), a fatica possono essere tenuti incatenati a questo solo contesto. Più alte aspirazioni dei costituenti europei vorrebbero finalmente attribuire loro una collocazione centrale nello statuto delle libertà fondamentali del futuro cittadino europeo.

Giulio Carducci⁽¹⁾

Sommario: 1. Considerazioni introduttive; 2. Breve storia del concetto “Privacy”; 3. Privacy, tecnologia e minacce; 4. Chi è interessato a violare la privacy. Mobilità ed evoluzione dei valori; 5. Aziende e privacy; 6. Conclusioni

1. Considerazioni introduttive

Sono molto onorato di essere stato invitato a tenere una breve relazione nel corso di questo qualificato incontro cui partecipano nomi tanto illustri. L'occasione mi ricorda epoche ormai lontane, risalenti alla prima metà degli anni '90, in cui si “fondava” la prima legge italiana in materia di privacy (la 675/96), allorché avemmo gratificanti occasioni, io personalmente e i miei colleghi, nella nostra qualità di “ingegnerizzatori” della protezione delle informazioni nelle aziende, di fornire qualche utile supporto attuativo per le aziende medesime e le organizzazioni.

Ero stato inizialmente richiesto da parte degli organizzatori del convegno di effettuare una presentazione di quello che è lo stato attuale del recepimento della norma nelle aziende, in virtù della mia esperienza professionale e di quella dei miei colleghi di Securteam (oggi, come si sa, parte di Marconi Selenia e di Finmeccanica). Pur riservandomi di dire qualcosa su questo argomento in conclusione dell'intervento, ho preferito proporre un argomento correlato, ma diverso: quale privacy sia “sostenibile”, e a quali condizioni, in una società ormai così fortemente interconnessa e “tecnologizzata” (mi si passi il termine, non proprio musicale).

Ovviamente, per un tema così complesso, certamente ambizioso, non penso di poter fornire scenari e proposte definitive: sarebbe già per me motivo di soddisfazione poter esporre e condividere con voi alcune considerazioni e proporre alcuni temi che potrebbero essere in futuro (magari già, in parte, nel corso delle tavole rotonde di questa conferenza) meglio discussi e approfonditi. D'altra parte, sono consapevole di inserirmi in una corrente di dibattito già in atto da parte di giuristi, sociologi e tecnologi di me assai più qualificati.

2. Breve storia del concetto “privacy”

Il sostantivo equivalente al termine “privacy”, com'è noto, non esiste nella lingua italiana, tant'è che utilizziamo correntemente la sua versione anglosassone, nel-

(1) Presidente di Securteam – Marconi Selenia Communications

la duplice pronuncia “oscillante” americana (“*praivacy*”) e britannica (“*privacy*”). Esiste in italiano solo il corrispondente aggettivo (privato) e s’inizia, da poco, il tentativo di instaurare il non esaltante vocabolo “privatezza”.

La cosa non è poi così anomala se si considera che nell’ordinamento giuridico italiano fino alla metà degli anni ’60 non esisteva il concetto del diritto alla riservatezza, tanto meno una particolare sensibilità al riguardo da parte dei soggetti sociali, schierati, per così dire, sui due fronti.

Mentre infatti negli Stati Uniti già negli 1988-90 i giudici Warren, Brandeis e Cooley deliberavano e pubblicavano sull’argomento, in particolare coniando la definizione di *privacy* come “*right to be let alone*”, in Italia ancora a metà degli anni ’50 (per l’esattezza il 22 dicembre 1956, con la sentenza della Cassazione n.4487), a proposito di una controversia sorta in merito alla realizzazione di due film riguardanti il celebre tenore Enrico Caruso, si affermava testualmente:

“Nell’ordinamento giuridico italiano non esiste un diritto alla riservatezza, ma soltanto sono riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona; pertanto non è vietato comunicare, sia privatamente che pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti o che impongano l’obbligo del segreto”.

A metà degli anni ’60 s’iniziava a intravedere un cambiamento di rotta nell’orientamento della Suprema Corte a proposito della pubblicazione di un libro riguardante il Duce e Claretta Petacci. Nella sentenza (20 aprile 1963, n. 990), si legge testualmente:

“Sebbene non sia ammissibile il diritto tipico alla riservatezza, [il fatto] viola il diritto assoluto di personalità, inteso quale diritto “*erga omnes*” alla libertà di autodeterminazione nello svolgimento della personalità dell’uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito ed ove non sussista, per la natura dell’attività svolta dalla persona e dal fatto divulgato, un preminente interesse pubblico di conoscenza”.

Come si può notare la sentenza, pur “aprendo” in qualche modo al riconoscimento di un diritto oggettivo in materia di *privacy*, forniva l’estro all’interpretazione, del tutto aberrante ampiamente utilizzata in alcuni settori della stampa scandalistica, che i “*Vip*” non avessero alcun diritto in materia.

Ma è proprio grazie ad una controversia instaurata con i giornali da parte di una famosa e bella rappresentante del “*Jet set*” dell’epoca, Soraya Esfandiari, che si deve, il 27 maggio del 1975 (n. 2129), una sentenza del Supremo Collegio:

“Il nostro ordinamento riconosce il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali ... non sono giustificate da interessi pubblici preminenti”.

Nel periodo 1975-1996, grazie anche all’escalation della tecnologia teleinfor-

matica, si susseguivano le promulgazioni, in ambito europeo, di leggi nazionali e di raccomandazioni e direttive del Consiglio d'Europa e dell'Ue, fino alla promulgazione, in Italia, della fondamentale e tanto discussa legge 675/96, recentemente superata dal Codice.

3. Privacy, tecnologia e minacce

Non è una novità l'affermazione che l'escalation della tecnologia (segnatamente teleinformatica e delle comunicazioni, ma non solo) abbia acuito notevolmente l'attualità e l'esigenza di una normativa che difendesse la privacy.

Da sempre la tecnologia ha svolto, nei confronti del Diritto e della Società, un ruolo duale: promuovendone la maturità e la complessità, ma anche costituendo una minaccia di gravità crescente: basta pensare alla filiera, succedutasi nei secoli, linguaggio • stampa • telecomunicazioni • teleinformatica.

Oggi i casi pratici più noti (senza pretesa di esaustività: la casistica è troppo numerosa ...) di pervasività tecnologica e di potenziale minaccia della nostra privacy sono i seguenti:

- telefoni cellulari
- telepass sulle autostrade
- accesso ai centri storici cittadini
- telesorveglianza in luoghi pubblici e privati (supermercati, banche, etc.)
 - Connessione a Internet:
 - Frequentazione di siti e-commerce (cookies)
 - Acquisto di software, sia on-line che per via tradizionale (cookies), fornitura di aggiornamenti del software (spyware)
 - File di log sulle stazioni di lavoro personali periodicamente inviati, in modo automatico, all'azienda produttrice del software
 - File di log mantenuti dai connectivity provider
 - Programmi di monitoraggio dei visitatori di ciascun singolo sito (AccessWatch: indirizzo IP, orario, pagine visitate, sistema operativo installato, risoluzione video, browser utilizzato)
 - Lo "spamming"
- Televisone digitale interattiva.

Va detto, ovviamente, che se da un lato la tecnologia costituisce, per la sua pervasività, una minaccia, dalla tecnologia (oltreché dai comportamenti individuali) scaturiscono anche le difese, che non staremo qui ad esaminare essendo materia ampiamente trattata in altre sedi che esula dal tempo concessoci e dal filo primario di questa presentazione. Qui si vuole solo osservare che, sia per il notevole numero dei protagonisti e degli intermediari in gioco, sia per la complessità (e, a propria volta,

pervasività) di certe contromisure, l'adozione delle contromisure stesse, anche in relazione alla loro efficacia, deve essere oggetto di attenta considerazione, secondo il procedimento oggi ampiamente raccomandato dell'analisi dei rischi.

4. Chi è interessato a violare la privacy. Mobilità ed evoluzione dei valori

Giunti a questo punto e per proseguire sulla linea logica dell'analisi dei rischi, è opportuno provare ad individuare che è potenzialmente interessato a violare la privacy. Una sintetica (e incompleta) rassegna degli attori più importanti potrebbe comprendere:

- i mass media
- gli addetti al marketing aziendale
- le aziende, nei confronti dei propri dipendenti
- le istituzioni, per fini di repressione del crimine e di pubblico interesse
- le organizzazioni criminose organizzate, con particolare riferimento a mafia e terrorismo
- i competitors (ma questo caso ricade sotto quello più ampio della violazione del segreto industriale)
- i ricattatori (anche qui si ricade nel caso più ampio della ordinaria, piccola criminalità).

Sembra evidente che i “poteri imprenditoriali forti”, le grandi aziende che offrono servizi e prodotti al mercato globale, sono quelle maggiormente “motivate” alla violazione della privacy, grazie al proprio interesse per la “profilatura” dei comportamenti di acquisto, e non solo, del potenziale mercato. Al riguardo, si osserva che il principio di proporzionalità della sanzione rispetto al potere economico del contravventore di cui all'articolo 161 del Codice della privacy meriterebbe una più ampia e severa applicazione.

Su di un altro piano, si osserva che una componente importante, nel modello di analisi dei rischi che si va delineando, destinato a spostare, nel tempo, la soglia di percezione della propria privacy individuale ai fini di stabilire, sempre individualmente, se e quanto valga la pena di sostenere l'onere economico, operativo e psicologico delle contromisure da parte degli interessati, è l'evoluzione di quello che potremmo definire *il comune senso della privacy*, in analogia con il ben più noto *comune senso del pudore*.

È evidente, infatti, che dall'accorato e intenso pamphlet di William Faulkner del 1955 (intitolato “Privacy” e ben noto al prof. Rodotà che ne promosse la conoscenza qualche anno addietro) e la situazione odierna, in un arco di cinquant'anni, le cose sono notevolmente cambiate. Se per i grandi protagonisti pubblici (soprattutto dello spettacolo, ma stiamo parlando di qualche decina di soggetti a livello

mondiale) la violazione della propria privacy costituisce una vera aggressione psicofisica, la stessa cosa non può dirsi per la maggioranza dei comuni mortali. In una società ormai dominata dai valori del “mostrare” e del “comparire”, in qualche modo di “essere protagonisti” comunque, al di là di quanto abbiamo effettivamente da dire e da dare, anche la percezione dell’intimo, del personale, dell’affettivamente riservato stanno subendo evoluzioni notevolissime.

E cosa dire, poi, dell’esigenza, in un mondo sempre più globale e interconnesso, di “esserci” e di “essere percepiti” da parte di professionisti, operatori e anche semplici individui? Mi pare possibile affermare che, tutti noi, quando siamo collegati ad Internet, in tanti casi, se abbiamo l’occasione di farci conoscere una volta di più, lo facciamo con motivazione positiva. In definitiva, una relazione in più è una potenziale occasione di maggior successo, e raramente pensiamo, in quel momento, alle possibili controindicazioni.

D’altra parte, le dichiarazioni di “outing” che di questi tempi numerose appaiono sulla stampa e che tendono a rendere pubbliche le proprie abitudini sessuali, il proprio credo religioso, le proprie malattie superate o meno, costituiscono una novità certamente positiva e fortemente innovativa rispetto all’atteggiamento di riserbo cui la società sembrava costringere queste persone fino a pochi anni or sono.

La crescente minaccia da parte dei terrorismi nazionali e di quello islamico sta contribuendo ulteriormente ad aumentare quanto ciascuno è disposto a concedere relativamente alla propria privacy. Sempre più frequentemente, conversando con gli amici, mi sento dire: “Ma io, in definitiva, non ho nulla da nascondere: se per essere più sicuro, le istituzioni hanno bisogno di sapere tutto o quasi su di me, e in cambio mi danno maggior sicurezza, io non ho problemi.

La percezione di questo stato di cose da parte e di questa “deriva” (in senso geologico e cinetico, non morale) della percezione della privacy è forse presente nel legislatore e nell’Authority quando si incoraggia l’emanazione di codici di autoregolazione, peraltro con riserva di approvazione da parte dell’Authority, nei comportamenti delle varie categorie protagoniste nella Società di oggi: giornalisti, fornitori di servizi di telecomunicazione telematica, marketing e altro.

5. Aziende e privacy

Le aziende sono di questi tempi in notevole agitazione (e apprensione) per l’approssimarsi delle scadenze imposte dal recente Codice. È un segnale non proprio positivo: come succede in altri casi consimili, ridursi all’ultimo momento è sempre segno di bassa priorità assegnata all’argomento, scarso coinvolgimento dei vertici aziendali, considerazione prevalentemente formale del tema.

Ovviamente fortunatamente esistono significative eccezioni.

Nelle aziende, il tema dell'ottemperamento alla normativa privacy è fortemente connesso con quello, più generale, della tutela delle informazioni in genere. Sono circa dieci anni che l'argomento è alla ribalta (seminari, dibattiti, mostre, convegni ... si sprecano) ma sono prevalentemente frequentati da fornitori e da giovani in cerca di primo impiego (o meno giovani in necessità di riciclarsi). I vertici aziendali, coloro che, in definitiva, decidono l'attività e la relativa spesa, sono quasi sempre assenti.

Il mercato degli apparati di protezione dei dati è piuttosto tonico: il processo di governo e gestione è invece ancora da consolidarsi.

Notevoli progressi sono stati registrati, nel corso degli ultimi anni, sul fronte del governo della sicurezza informatica volto alla Pubblica Amministrazione, in connessione con la promozione di numerosi servizi di e-government. L'attuazione concreta, tuttavia resta ancora limitata.

Nelle aziende del comparto privato, con eccezione di alcuni casi, segnatamente di operatori di telecomunicazione nati con l'avvento della e-economy, la protezione dei beni e delle informazioni in particolare stenta a istituzionalizzarsi come processo. Nel mondo anglosassone, il Security Manager ha responsabilità, livello, retribuzione e risorse del tutto analoghe a quella di un Financial Manager. Da noi, siamo ancora agli inizi, anche se qualche segnale positivo in qualche azienda illuminata si sta verificando, grazie, ahimè, anche alle pressioni che derivano dalla minaccia terroristica, dal tema delle infrastrutture critiche (Critical National Infrastructure) e dalle relazioni di business internazionali.

In questo contesto, l'attuazione della normativa privacy risente, in analogia, di una percezione orientata più verso l'adempimento amministrativo che di una reale convenienza aziendale. Anche in questo caso, il ricorso all'autoregolamentazione, al di là degli adempimenti di base previsti dal d.lg. 196/2003, potrebbe procurare una svolta di percezione, cultura e mentalità.

6. Conclusioni

Proviamo a trarre qualche considerazione conclusiva dalle riflessioni proposte in questa relazione.

1. La percezione sociale della privacy come "diritto a essere lasciati soli", tipica dell'inizio del secolo scorso, va oggi sostituita da una visione volta a difendere il diritto del controllo, anche caso per caso, delle proprie informazioni.
2. L'attuazione di tale contratto vedrà, al disopra e in aggiunta a una baseline normativa essenziale intesa ad assicurare uno zoccolo duro di principi, criteri e norme minime, la definizione di pattuizioni tra le parti, affidate alle norme deontologiche di categoria e agli specifici contratti tra

le parti. Dovrebbe inoltre prevedere un inasprimento di sanzioni per i “poteri forti” economicamente interessati alla violazione della privacy.

3. La tecnologia, non solo teleinformatica, continuerà a costruire ulteriori opportunità e meccanismi per consentire agli interessati di appropriarsi delle informazioni personali altrui. È vero che la tecnologia offrirà anche migliori sistemi di difesa, ma la sperequazione tra il potere e la motivazione di chi attacca e di chi si difende è destinata ad accrescersi.

In questo scenario di difficoltà crescenti, in cui la protezione della privacy e il concetto stesso di privacy risentiranno profondamente del livello medio di etica presente nella nostra Società, un rimedio preventivo è certamente costituito dal fatto, ciascuno di noi, di avere, da un lato, poche cose da nascondere e, dall'altro di contribuire, ciascuno per la propria parte, per il recupero di certi valori dell'intimo, dello spirito e del sacro che, al momento, sembrano essere un pò dimenticati.

Yves Poullet⁽²⁾

Sommario: 1. Caratteristiche dell'ambiente dei servizi di comunicazione elettronica; 2. Verso il riconoscimento di nuovi diritti; 3. Occorrono specifici strumenti giuridici che siano ulteriori rispetto alla Convenzione 108 del Consiglio d'Europa per regolamentare gli specifici rischi per le libertà derivanti dall'utilizzazione delle tecnologie dell'informazione e della comunicazione?

1. Caratteristiche dell'ambiente dei servizi di comunicazione elettronica

Onnipresenza e crescente polifunzionalità delle reti di telecomunicazione

- Proliferazione delle reti (Gps, Rfid, Internet, Gsm, Wi-Fi, Bluetooth, Grps, Sms, ecc.), soprattutto di tipo wireless, e della rispettiva interattività (digitalizzazione termino-terminale, packaging; standardizzazione globale).
- Proliferazione di comportamenti che richiedono l'uso di tali reti (lettura di quotidiani, ordinativi di merci o servizi, Tv, noleggio di videocassette, ricerca di informazioni, pubblicazione o lettura di annunci a pagamento, consultazione di conti correnti, effettuazione di pagamenti virtuali, ecc.).
- Tendenza a rendere disponibili un numero crescente di oggetti provvisti di dispositivi informatici connessi ad una rete (intelligenza d'ambiente).
- Concetto di servizio universale: l'accesso ad Internet e determinati servizi sono considerati "vitali" nella società dell'informazione.
- Passaggio da un modello di fatturazione basato sulla durata della comunicazione ad un sistema forfetario basato sulla durata della disponibilità della rete e sulla connettività permanente.

Interattività di rete

- L'utente genera informazioni sempre più particolareggiate utilizzando la rete.
- L'interattività della rete spiega per quale motivo sia l'utente stesso a generare i dati personali verosimilmente oggetto di trattamento da parte

(1) Il presente contributo è una versione leggermente modificata del documento preliminare presentato da Jean-Marc Dinant e dall'Autore in occasione del 20^{mo} incontro del Comitato consultivo del Consiglio d'Europa sulla protezione dei dati (Strasburgo, 28-30 giugno 2004) e non contiene l'analisi delle disposizioni della Convenzione 108 del Consiglio d'Europa. Il testo completo può essere richiesto al Garante per la protezione dei dati personali.

(2) Direttore del CRID – Université de Namur, Belgio

del destinatario o di terzi che intervengono durante o dopo la trasmissione del messaggio.

- L'interattività della rete può far sì che si dia maggiore importanza al consenso, se è facile manifestarlo (ad esempio, cliccando sul mouse) e raccoglierlo. Vi sono tecnologie come la P3P [*Platform for Privacy Preferences*, Piattaforma di preferenze in materia di privacy] che si fondano, pertanto, sull'idea del controllo relativo dell'ambiente da parte degli utenti, i quali sarebbero in grado di scegliere se rendersi o meno identificabili, di selezionare i siti che corrispondono alle rispettive preferenze in materia di privacy, e di negoziare la comunicazione dei propri dati personali (mito del "controllo da parte dell'utente") (v. infra l'analisi relativa all'assenza di trasparenza sulla rete).
- L'apertura di reti sulla base di protocolli http crea infinite possibilità di spostarsi da un servizio all'altro e permette di tenere traccia degli spostamenti dei singoli utenti.
- Aumentano le opportunità di trattare i dati che si generano in tal modo a livello dei terminali della rete (sistemi di profilazione, ecc.). Creazione di nuovi trattamenti sulla base dei dati raccolti (problema dei trattamenti cosiddetti "incompatibili").
- Aumentano le opportunità di raccogliere e trasmettere informazioni attraverso le reti, e di trattare i dati a livello dei terminali delle reti (sistemi di profilazione, ecc.).

Polifunzionalità e convergenza dei terminali di telecomunicazione in direzione del computer

- Il terminale Internet, il telefono cellulare, i Pda [*Personal Digital Assistant(s)*, assistenti digitali personali come i palmari o le agende elettroniche], i chip Rfid e le carte intelligenti (o a microprocessore) possono essere definiti "computer" in termini funzionali.
- Convergenza di reti e terminali, a differenza delle separazioni funzionali precedentemente note (Tv via cavo, onde elettromagnetiche, cavetti telefonici, ecc.). Digitalizzazione spinta (voce/dati) e abbandono della prassi di distinguere gli operatori a seconda delle tecniche di comunicazione utilizzate.
- Fa parte della natura stessa del computer il fatto di conservare, copiare e trasferire informazioni.
- Tutte queste apparecchiature terminali memorizzano e trasmettono in modo sistematico tracce delle (tele)comunicazioni all'insaputa dell'utente.
- Rischi in termini di sicurezza e di violazioni della riservatezza.
- Impossibilità di verificare le finalità per le quali si utilizzano le informa-

zioni messe in rete.

- Crescente polifunzionalità dei terminali.

Assenza di controlli da parte dei governi

- Per vari decenni i governi hanno imposto il rispetto di requisiti obbligatori come condizione per ottenere l'approvazione di terminali telefonici o facsimile.
- La situazione non era cambiata quando sono stati introdotti i telefoni cellulari e l'Isdn [*Integrated Services Digital Network*, Rete digitale di servizi integrati], essendo stata regolamentata la possibilità di visualizzare o nascondere il numero del soggetto chiamante (Clir, Clip, ecc.).
- Nessun governo ha mai regolamentato i computer, che tendono in misura crescente a trasformarsi in terminali polifunzionali, soprattutto per quanto concerne la televisione online ma anche in rapporto alla telefonia (*Voice-over-Ip*).
- La standardizzazione dei protocolli avviene sostanzialmente ad opera di organismi privati attraverso strutture che non garantiscono sufficiente trasparenza (W3C, Ietf, ecc.).
- I governi non intervengono nella definizione degli standard applicabili alle telecomunicazioni, che sono sviluppati dalle imprese del settore avendo in mente i benefici conseguibili.
- Gli standard suddetti comprendono talora disposizioni finalizzate alla tutela della privacy, che però hanno in genere carattere non vincolante e prendono la forma di raccomandazioni riferite all'attuazione degli standard in oggetto.

Assenza di controlli da parte degli utenti

- Al momento di dare attuazione agli standard definiti per il software utilizzabile dai terminali di telecomunicazione, è prassi ormai consolidata che delle suddette raccomandazioni non si tenga alcun conto. Attualmente i parametri del software utilizzato nelle telecomunicazioni sono settati su valori di default che eliminano ogni privacy, ma per gli utenti provvisti di opportune conoscenze ed abilità è possibile modificare tali parametri. Selezionando parametri che garantiscano maggiore privacy, l'utente va incontro quasi sempre a limitazioni, avvertimenti e svantaggi. Inoltre, le scelte effettuate dal singolo utente sono in genere note alla rete, a terzi o ai destinatari della telecomunicazione.
- Vi sarebbe la possibilità di verificare la situazione sia prima, sia durante,

sia al termine dell'utilizzazione di un terminale di telecomunicazioni. È raro, tuttavia, che tali controlli siano effettuati in via preventiva, perché gli utenti non sono avvertiti dei possibili rischi prima di utilizzare un terminale (per quanto riguarda i dispositivi Rfid, può darsi che credano semplicemente di avere acquistato una maglietta). L'applicazione di misure di sicurezza durante l'utilizzazione produce sempre effetti negativi sulla funzionalità e la rapidità delle telecomunicazioni. È raro, infine, che sia possibile effettuare controlli *ex post*, in quanto l'interfaccia-utente progettata dalle imprese del settore mira esattamente a non consentire agli utenti di visualizzare il proprio traffico.

- Il terminale di telecomunicazione presenta talora interfacce aperte rispetto ad alcuni soggetti operanti sulla rete, senza che di ciò vi sia contezza (*spyware* [software spia], *peepholes* [lett. "spioncini"; si tratta di software che periodicamente verificano, ad esempio, i messaggi e-mail memorizzati su un server di posta elettronica sulla base di determinate parole-chiave], virus, ecc.).
- Il software installato nei terminali di telecomunicazione può essere dotato di funzionalità di aggiornamento automatico e potenziamento/depotenziamento senza che l'utente ne sia a conoscenza o possa opporvisi.

Assenza di trasparenza delle reti e dei terminali di telecomunicazione

- Assenza di trasparenza del terminale: "*chattering*" [lett. "chiacchiericcio", il fatto di trasmettere continuamente informazioni durante il normale funzionamento] da parte del terminale, *spyware*, *cookies*, legami ipertestuali invisibili verso soggetti terzi, memorizzazione invisibile delle telecomunicazioni effettuate, possibilità per qualsivoglia programma di accedere alla rete in modo occulto.
- Proliferazione ed assenza di trasparenza dei soggetti in causa e dei rapporti intercorrenti: operatori identificati, operatori non identificati, finalità dichiarate e non.
- Domanda: è necessario regolamentare le apparecchiature terminali di telecomunicazione e gli operatori di rete?

Carattere internazionale delle reti

- Assenza di tutela in alcuni Stati di destinazione e/o provenienza delle informazioni.
- Problema della sovranità statale alla luce dell'esistenza di un'infrastruttura globale (caso Yahoo!).

- Problema della localizzazione del sito e, più in generale, dei servizi della società dell'informazione.
- Domanda: è necessario applicare gli strumenti tipici della sovranità statale (ad esempio, fornitori di accesso ad Internet su base regionale, progettazione di infrastrutture, ecc.)?

2. Verso il riconoscimento di nuovi diritti⁽³⁾

L'utilizzazione delle tecnologie dell'informazione e della comunicazione comporta molteplici rischi per le libertà e la dignità umana, ed è necessario riconoscere l'esistenza di nuovi diritti per tenere conto di tali rischi. Si tratta di diritti sanciti per effetto di strumenti adottati recentemente da organismi nazionali o internazionali, sulla base di articoli di dottrina, ovvero frutto di riflessioni personali. Il nostro obiettivo è di tracciare un percorso di discussione.

Il diritto ad un anonimato “reversibile”

Non v'è dubbio che sia necessario rivedere il concetto di “anonimato”, al quale si dovrebbero forse preferire altri concetti (come “pseudonimo” o “inidentificabilità”) qualora esso si riveli ambiguo. Spesso quello cui si aspira non è un anonimato assoluto, bensì la “inidentificabilità” funzionale del mittente rispetto a determinati soggetti.

Chiunque utilizzi i moderni mezzi di comunicazione deve avere la possibilità di mantenere la propria inidentificabilità rispetto a qualsivoglia soggetto terzo che intervenga nella comunicazione del messaggio, ai fornitori di servizi che partecipino alla catena comunicativa, o ai destinatari della comunicazione stessa; inoltre, deve essere messo in grado di esercitare tale opzione in forma gratuita oppure a costi ragionevoli.

Non si tratta, tuttavia, di prevedere un diritto assoluto all'anonimato o alla “inidentificabilità”, per quanto necessari. Il diritto dei cittadini all'anonimato confligge con l'interesse superiore dello Stato, che può imporre limiti se questi ultimi costituiscono misure necessarie “per la salvaguardia della sicurezza nazionale, per la difesa o la sicurezza pubblica, e per la prevenzione, l'accertamento, le indagini ed il perseguimento di (alcuni) reati penali”. Si potrebbe trovare un bilanciamento fra il legittimo controllo della criminalità e le esigenze poste dalla protezione dei dati attraverso sistemi che prevedano l'assegnazione ai singoli di “pseudoidentità” da parte di un fornitore di servizi specializzato⁽⁴⁾, il quale sarebbe in grado di ripristinare il legame fra

(3) V. in proposito, Y. Poulet, *Internet et vie privée, entre risques et espoirs*, JT, 2001, n. 6000, p. 161 e segg., n. 22 f. Contiene numerosi riferimenti a testi o articoli di dottrina a sostegno delle tesi dell'Autore.

(4) Cosa dire di un sistema di autorizzazione per tali provider che comporti un importante vincolo di riservatezza sia nei confronti di terzi sia nei riguardi degli utenti dei rispettivi servizi?

l'identità reale dell'utente ed il rispettivo pseudonimo sulla base di procedure previste per legge, esclusivamente nei casi specificati. Altre soluzioni potrebbero essere rese obbligatorie attraverso la regolamentazione delle apparecchiature terminali: soppressione del “*chattering*” da parte dei browser, creazione di indirizzi effimeri e differenziazione fra i dati di indirizzamento in rapporto ai terzi che potranno accedere ai dati relativi al traffico o all'ubicazione, ed eliminazione di identificatori univoci universali tramite la standardizzazione dei protocolli di indirizzamento.

Il diritto alla reciprocità di benefici

È un diritto che può essere formulato come segue: poiché le tecnologie facilitano considerevolmente la raccolta, il trattamento e la diffusione delle informazioni, l'interessato deve poter esigere che il titolare, beneficiando di tali fonti di informazione, utilizzi le stesse tecnologie per facilitare all'interessato l'esercizio dei diritti che gli sono riconosciuti.

Si possono immediatamente ipotizzare numerose e diverse applicazioni di tale diritto:

- il *diritto dell'interessato* di essere informato deve essere esercitabile in qualsiasi momento con un semplice click (o, più in generale, con un semplice gesto elettronico di natura positiva) su un tasto recante un acronimo che permetta di accedere alla *privacy policy*; quest'ultima è auspicabile che sia tanto più precisa e completa quanto più l'utilizzo di supporti elettronici consente di ridurre i costi di distribuzione. La procedura deve garantire l'anonimato rispetto al server sul quale si trova la pagina interessata (chi naviga in rete con un occhio alla privacy teme che i propri dati personali siano registrati).
- il *diritto di accesso* dell'interessato deve essere esercitabile a breve attraverso gli strumenti elettronici, sulla base del ricorso alla firma elettronica. Ciò dovrebbe imporre al titolare di organizzare i propri archivi in modo da permettere al singolo interessato di esercitare il diritto di accesso senza alcuna difficoltà. La messa a disposizione di informazioni ulteriori, come l'origine dei dati o l'elenco dei terzi ai quali i dati siano stati comunicati, dovrebbe avvenire in forma sistematica.
- il *diritto di rettifica e/o opposizione* dovrebbe essere esercitabile online contattando una persona specifica incaricata di esaminare ricorsi o segnalazioni, ovvero di gestire le opposizioni, e della quale si potrebbero definire ruolo e qualifiche.

Il diritto dell'utente di disporre di apparecchiature terminali il cui funzionamento impedisca attività illecite e sia trasparente

Questo diritto sarà esercitabile dagli utenti nei confronti di società che non sono necessariamente ricomprese nell'ambito consueto nella normativa sulla protezione dei dati, in quanto non sono in alcun modo responsabili del trattamento dei dati – ad esempio, le società che forniscono apparecchiature terminali e vari prodotti software, in particolare programmi di navigazione, i quali spesso sono incorporati nell'apparecchiatura terminale per facilitare la ricezione, il trattamento o la trasmissione di comunicazioni elettroniche.

Inoltre, si tratta di un diritto che chiama in causa gli enti di normazione, pubblici e privati, incaricati di definire la configurazione dell'apparecchiatura in oggetto.

L'idea di fondo è che non dovrebbe essere possibile che un prodotto fornito agli utenti di servizi di comunicazione elettronica consenta attività illecite – vuoi da parte di terzi, vuoi da parte del produttore stesso – esattamente in ragione della configurazione che lo caratterizza. Alcuni esempi possono meglio illustrare l'importanza di questo concetto:

- confrontando i browser presenti sul mercato, si osserva che il “*chattering*” esula in misura considerevole da quanto strettamente necessario per l'instaurazione della comunicazione;
- i browser si differenziano per le modalità di gestione della ricezione, della soppressione e del blocco della trasmissione di cookie. Pertanto, le possibilità di trattamenti sleali o non corretti aumentano o si riducono a seconda del browser utilizzato;
- è necessario puntare il riflettore anche sull'impiego di identificatori univoci o *spyware* da parte dei fornitori di strumenti di navigazione o software di comunicazione.

A parte segnalare queste preoccupazioni di carattere generale, si propone un concetto di terminale trasparente in termini di funzionamento, che consenta all'utente di mantenere il pieno controllo dei dati inviati e ricevuti. Pertanto, l'utente dovrebbe avere la possibilità di individuare con facilità il livello preciso del “*chattering*” svolto dal proprio computer, i file ricevuti, le finalità ed i rispettivi mittenti.

Diritto dell'utente e del consumatore su Internet di beneficiare delle disposizioni a tutela del consumatore, con particolare riguardo alle azioni collettive

La diffusione del ricorso alle tecnologie dell'informazione e della comunicazione, un tempo riservate alle imprese, e l'utilizzo crescente di tali tecnologie in rapporto allo sviluppo del commercio elettronico, che comporta un aumento nel numero di servizi online, fanno sì che l'approccio alla privacy sia basato in misura crescente su un'ottica di tipo consumeristico. È da consumatore di questi nuovi servizi che il

navigatore nel web subisce violazioni della propria privacy (spamming, profilazione, personalizzazione dei prezzi, rifiuto dell'accesso a determinati servizi, ecc.).

Questa convergenza fra gli interessi dei consumatori ad una tutela di tipo economico e le libertà dei cittadini apre alcune interessanti prospettive. Impone il riconoscimento del diritto di esperire un'azione legale collettiva in caso di violazioni della privacy, diritto che è già riconosciuto nell'ambito della tutela del consumatore. A parte ciò, si potrebbero applicare con effetti positivi tutta una serie di disposizioni tratte dal diritto del consumo; ad esempio, si potrebbe imporre agli operatori che offrono servizi consistenti in via primaria nella gestione o nella fornitura di dati personali l'obbligo di fornire informazioni o raccomandazioni (ad esempio, fornitori di accesso ad Internet, server di database nominativi [contenenti informazioni giuridiche, o motori di ricerca]). Alternativamente, si potrebbe applicare la normativa concernente le condizioni e disposizioni contrattuali standard (in rapporto alla *privacy policy*), oppure quella relativa alle prassi commerciali abusive o vessatorie.

Un'altra strada da percorrere riguarda la possibilità di estendere la responsabilità per danno da prodotto (apparecchiature terminali e software) non solo al danno fisico o finanziario, ma anche alle violazioni della privacy. In quale misura un soggetto fornitore di programmi di navigazione il cui funzionamento standard comporti violazioni della privacy potrebbe non essere chiamato a rispondere di violazioni operate da terzi?

3. Occorrono specifici strumenti giuridici che siano ulteriori rispetto alla Convenzione 108 del Consiglio d'Europa per regolamentare gli specifici rischi per le libertà derivanti dall'utilizzazione delle tecnologie dell'informazione e della comunicazione?

Ci interessa rispondere ad un quesito fondamentale: abbiamo bisogno di norme specifiche per la protezione dei dati nella società dell'informazione, diverse da quelle contenute nella Convenzione 108 del Consiglio d'Europa, oppure è sufficiente sviluppare i principi di tale Convenzione per tenere conto in modo adeguato delle questioni sollevate in materia di protezione dei dati dallo sviluppo delle tecnologie dell'informazione e della comunicazione?

Per rispondere a questa domanda, passeremo in rassegna le disposizioni della Direttiva 2002/58/CE relativa al trattamento di dati personali ed alla tutela della privacy nel settore delle comunicazioni elettroniche.

Le disposizioni più importanti di tale Direttiva riguardano:

1. i limiti posti al trattamento dei dati relativi al traffico ed all'ubicazione;
2. le comunicazioni indesiderate;
3. la riservatezza;

4. la configurazione tecnica delle apparecchiature terminali;
5. l'identificazione della linea chiamante.

Si possono anche ricordare i punti seguenti:

1. l'estensione della tutela alle persone giuridiche, relativamente ad alcune disposizioni;
2. la distinzione fra abbonato ed utente.

Le disposizioni di cui sopra suscitano le seguenti considerazioni:

1. Per quanto concerne i dati relativi al traffico ed all'ubicazione, la considerazione speciale di cui godono nella Direttiva è riferibile alle rispettive finalità, che incontrano subito precise limitazioni: la comunicazione di messaggi destinati a o provenienti dagli utenti di servizi di comunicazione elettronica, ed i rischi associati al trattamento sistematico di tali dati, in grado di rivelare i movimenti, le abitudini di consumo e lo stile di vita dei soggetti in questione. Inoltre, il requisito del consenso, necessario per utilizzare questi dati al fine di fornire servizi a valore aggiunto, non si giustifica, in particolare, con la circostanza che, essendo facile manifestare il consenso utilizzando le tecnologie disponibili, si può presumere che esso venga a costituire l'unico fondamento di legittimità dei trattamenti connessi a tali servizi aggiuntivi?
2. La spiegazione relativa alla facilità con cui è possibile ottenere il consenso attraverso l'uso delle tecnologie giustifica probabilmente il rifiuto da parte dell'Ue dei meccanismi di opt-out [opposizione a posteriori], che in ultima analisi si fondano sul bilanciamento di interessi tradizionalmente applicato nell'ambito del marketing diretto. Un altro argomento è rappresentato dall'invasività della comunicazione, che penetra direttamente nel domicilio virtuale dell'interessato, nonché dalla facilità di inviare i messaggi in questione e dal fatto che il mittente non deve sostenere alcun costo.
3. Le disposizioni concernenti la riservatezza delle comunicazioni sono ascrivibili al fatto che, oggi, le tecnologie interattive di rete consentono all'utente di comunicare con ogni altro soggetto connesso alla rete, e di farlo per scopi del tutto personali. Ciò spiega perché il principio di riservatezza della corrispondenza ed il divieto di intercettazione debbano essere estesi d'ora in poi a tutte le comunicazioni elettroniche, sia in termini di contenuto sia in termini di presenza di tali comunicazioni. Si pone, inoltre, la questione del ruolo da attribuire alle società che trasportano i messaggi o intervengono nei relativi processi: si deve forse seguire l'esempio della regolamentazione adottata per i servizi postali ed i tradizionali operatori telefonici, imponendo a tali società il rispetto di norme tese a garantire la riservatezza in oggetto?
4. I due ultimi punti sopra menzionati hanno carattere più innovativo. Es-

si sanciscono il diritto dell'utente dei servizi in questione di disporre di apparecchiature terminali che siano "costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali", e l'obbligo degli operatori delle reti di comunicazione di disegnare un'infrastruttura che renda possibile per gli utenti esercitare il diritto di non essere identificati.

5. Per quanto riguarda l'ambito della direttiva "ratione personae", si può osservare che sarebbe opportuno analizzare le motivazioni dell'estensione della tutela alle persone giuridiche in rapporto ad alcune (ma non alla totalità) delle disposizioni, così da stabilire se tale estensione rappresenti effettivamente un principio innovativo oppure se non si possa realizzarne la ratio legis in altri modi – ad esempio, ampliando la definizione di "persona fisica identificabile". Spesso si legge della distinzione che può sussistere fra abbonati ad un servizio ed utenti reali di tale servizio. Fra gli esempi menzionati al riguardo, citiamo il caso di un abbonamento familiare ad una rete Asdl e quello di una società che doti i propri dipendenti di telefoni cellulari. È una distinzione che solleva temi assai delicati, in quanto aumenta le possibilità per l'abbonato di controllare l'utilizzo dei servizi coperti dall'abbonamento ad opera del singolo utente. La persona da tutelare non è più soltanto l'abbonato nei confronti del fornitore di servizi di comunicazione, ma anche l'utente nei confronti dell'abbonato. Si tratta di tematiche già oggetto di analisi in riferimento alla sorveglianza dei lavoratori sul luogo di lavoro. Per quanto riguarda la sorveglianza all'interno del nucleo familiare, bisogna prendere in esame il concetto di privacy endofamiliare.

In conclusione, non è chiaro se lo sviluppo dei dispositivi di comunicazione elettronica renda necessaria l'adozione di una specifica Convenzione di settore, poiché gran parte delle soluzioni individuate nelle legislazioni nazionali o nella Direttiva europea rappresentano semplicemente lo sviluppo di principi generali in materia di protezione dei dati. Tuttavia, questa affermazione comporta in prima istanza due riserve: la necessità di regolamentare i prodotti, soprattutto le apparecchiature terminali, e la definizione di norme o obblighi speciali per gli operatori di rete che necessariamente partecipano alla comunicazione dei messaggi. Questa duplice esigenza risulta sussistere in quanto l'interessato, utilizzando mezzi di comunicazione elettronica, si trova dinanzi ad una doppia interfaccia sulla quale non ha alcun controllo: da un lato, le apparecchiature terminali che rendono possibile connettersi alla rete, e d'altro lato gli intermediari tecnici fra l'utente ed il destinatario della comunicazione o i soggetti che vi intervengono per conto di quest'ultimo.

Yves Poullet⁽²⁾

Contents: 1. Characteristics of the electronic communications services environment; 2. Towards the recognition of new rights; 3. Is there a necessity for specific legal instruments that go beyond Convention No. 108 in order to regulate the specific risks of attacks on freedom through the use of the information and communication technologies?

1. Characteristics of the electronic communications services environment

The omnipresence and growing multifunctionality of telecommunications networks

Proliferation of networks (Gps, Rfid, internet, Gsm, Wifi, BlueTooth, Grps, Sms, etc), especially wireless networks, and of their interactivity (end-to-end digitisation; packaging; global standardisation).

Proliferation of human practices involving these networks (reading a newspaper, ordering goods or services, watching Tv, renting a video cassette, seeking information, placing or reading a small ad, consulting a bank account, making a cashless payment, etc).

Trend towards providing more and more objects with a computer connected to a network (ambient intelligence).

Idea of a universal service: access to the internet and certain services considered “vital” needs in the information society.

Development from a call duration based charging model to a flat-rate system based on the duration of the availability of the network and permanent connectivity.

Network interactivity

The user generates ever more detailed information through the use of the networks.

The interactivity of the network explains why the user himself or herself creates the personal data likely to be processed by the recipient or by third parties who intervene either during or after the conveyance of the message.

(1) This article is a lightly revised version of the preliminary document presented by J.Marc Dinant and the author at the 20th meeting of the Council of Europe Consultative Committee on Data Protection (Strasbourg, 28-30 June 2004).

(2) Director of the Crid, University of Namur - Belgium

The interactivity of the network may result in greater importance being attached to consent if consent is easy to generate (by a simple mouse click) and collect. Technologies like P3P are accordingly based on the idea of the relative control of their environment by the users, who can choose whether or not to identify themselves, to select the sites that meet their preferences with regard to privacy and to negotiate the passing on of their personal data (myth of “user empowerment”) (see our analysis below of the lack of network transparency).

The opening of networks by means of http protocols creates infinite possibilities for passing from one service to another and enables the user’s path to be tracked.

The increasing possibility of processing data thus created within and at the terminal end of the networks (profiling system, etc). Creation of new processings on the basis of the data collected (problem of so-called “incompatible” processing).

There is an increasing possibility for information to be collected and transmitted via the networks and for the data to be processed within and at the terminal end of the networks (profiling system, etc) Creation of new processings on the basis of the data collected (problem of so-called “incompatible” processing).

Multifunctionality and convergence of telecommunications terminals in the direction of the computer

The internet terminal, the mobile telephone, the Pda, the Rfid chip and the chip card may be functionally defined as computers.

Convergence of networks and terminals, in contrast to the previous functional separations (cable Tv, electro-magnetic waves, telephone cables, etc). Full digitisation (speech/data) and abandonment of the practice of dividing up players according to communication techniques.

The very nature of the computer is to preserve, copy and transfer information.

All these terminals systematically store and transmit traces of telecommunications without the user’s knowledge.

Risks associated with security and breaches of confidentiality.

Impossibility of checking on the purposes for which information put on the network is used.

Growing multifunctionality of terminals.

Lack of government controls

For some decades, governments imposed mandatory standards for the approval of telephone or fax terminals.

This was still the case when mobile telephones and Isdn were introduced, with

the regulation of the ability to display or hide the caller's number (Clir, Clip, etc).

Governments have never regulated computers, which are increasingly becoming multifunctional terminals, especially for online television but even for telephony (voice-over-Ip).

The standardisation of protocols is essentially the work of private organisations concerning structures lacking in transparency or openness (W3C; Ietf; etc).

Governments do not intervene in the establishment of telecommunications standards, which are devised by the industry with its own advantages in mind.

Provisions aimed at the protection or privacy are sometimes included in the wording of these standards but generally in a non-binding way in the form of advice concerning their implementation.

Lack of user controls

When it comes to implementing standards in programs in telecommunications terminals, these pious recommendations have long been widely disregarded. The current tendency is for the telecommunications software parameters to be set to privacy-killing default values but to enable a competent and informed user to modify these settings. The choice of parameters that provide more privacy protection almost always involves restrictions, warnings and disadvantages for the user. Moreover, the user's choices may be generally known to the network, a third party or the recipients of the telecommunication.

Checks could be carried out before, during or after the use of a telecommunications terminal. They are rarely carried out beforehand since users are not warned of the risks before using a terminal (in the case of Rfid chips, they may believe they are just buying a simple shirt). The use of security measures during the use always has an adverse effect on the functionality and speed of the telecommunication. Ex post facto checks are rarely made possible as the aim of the user interface designed by the industry is not to enable users to visualise their own traffic.

The telecommunications terminal may have open interfaces with respect to certain network players without being aware of this (spyware, peephole, virus, etc).

The software installed on the telecommunications terminals may be able to update themselves automatically and modify their functionalities upwards or downwards without the user being informed or being able to object.

Non- transparency of networks and telecommunications terminals

Lack of transparency of the terminal: "chattering" on the part of the terminal, spyware, cookies, hyperlinks invisible to third parties, invisible storage of telecom-

munications carried out, actual technical ability of any program to access the network silently.

Proliferation and lack of transparency of players and the relationships between them: players identified, players not identified, declared and undeclared aims .

Question: Should telecommunications terminals and network operators be regulated?

International character of networks

Lack of protection in certain states in which information is transmitted and/or from which information is sent.

Problem of the sovereignty of states in the light of a global infrastructure (Yahoo case).

Problem of site location and, more generally, the services of the information society.

Question: Should the resources of sovereignty be imposed (eg, regional IAPs, infrastructure design, etc)?

2. Towards the recognition of new rights

The use of the information and communication technologies holds many risks of attacks on freedom and human dignity, and new rights must be recognised to take account of these risks. These rights are established as a result of recent texts from national or international bodies, learned articles or personal reflections. Our purpose is to draw up a formulation for discussion.

The right to “reversible” anonymity

The notion of anonymity should no doubt be defined, and other concepts such as “pseudonym” or “unidentifiability” should perhaps be preferred where this notion is ambiguous. What people are looking for is often not absolute anonymity but the functional “unidentifiability” of the originator of a message vis-à-vis certain persons.

Anyone who uses modern means of communication must have the choice of remaining unidentifiable by any third parties that intervene in the conveyance of the message, by service providers that intervene in this chain of communication or by the recipient(s) of the communication and must have the means of exercising this choice available either free of charge or at an affordable price.

The necessary anonymity or “unidentifiability” is, however, not an absolute right. The citizens’ entitlement to anonymity collides with the higher interest of the state, which may impose limitations when they constitute measures necessary “to safeguard national security, defence or public security and for the prevention, investigation, detection and prosecution of (certain) criminal offences”. A balance between the legitimate control of crime and the requirements of data protection could be found in systems that involve a “pseudo-identity” assigned to an individual by a specialised service provider, which could establish the link between the actual identity of a user and his or her pseudonym through procedures laid down by law, and only in such cases. Apart from that, other solutions could be imposed by regulating terminal equipment: the suppression of “chatter” on the part of the browsers, the creation of ephemeral addresses and differentiating between addressing data according to third parties that will have access to traffic or location data and the elimination of global unique identifiers through the standardisation of addressing protocols.

The right to the reciprocity of advantages

This right may be formulated as follows: since the technologies considerably facilitate the collection, processing and dissemination of information, the person concerned must be able to demand that the data controller that benefits from these sources should use the technologies to make it easier for the person concerned to exercise his or her rights.

Many different applications of this right can be suggested forthwith:

- the right to information of the person concerned must be able to be exercised at any time by means of a simple click (or, more broadly, a simple, positive electronic and immediate gesture) on an acronym button that provides access to a privacy policy, which will hopefully be all the more precise and complete as the distribution costs are reduced in the case of the use of the electronic media. This procedure must remain anonymous for the page server (privacy-concerned surfers’ fear of their details being recorded).
- the right of access of the person concerned must be able to be exercised tomorrow via the electronic media on the basis of the use of an electronic signature. It should oblige the person responsible to organise these files in such a way as to enable the individual to exercise this right of access without any difficulty. The provision of additional information such as the origin of the data or the list of third parties to whom the data have been passed on should be systematic.
- the right to correct and/or raise objections should be able to be exercised

online by contacting a specific person who is charged with examining complaints or dealing with the list of objections and whose status could be defined.

The user's right to terminal devices whose operation prevents illicit actions and is transparent

This right will be exercised by users vis-à-vis companies not necessarily covered by the traditional data protection provisions if they are not at all responsible for processing data – for example, the suppliers of terminal equipment and various software products, especially navigation programs, likely to be incorporated in the terminal to facilitate the receipt, processing or transmission of electronic communications.

In addition, this right is directed at public and private standardisation bodies concerned with the configuration of this equipment.

The main idea is that it should not be possible for the products made available to the users of electronic communications services to permit illicit actions – whether by third parties or the manufacturer itself – by virtue of their very configuration. A number of examples will illustrate the importance of this point:

- a comparison of the browsers on the market shows that “chattering” goes far beyond what is strictly necessary for setting up the communication.
- browsers differ in the way they handle the receipt, suppression and blocking the transmission of cookies. Accordingly, unfair processing will be more or less easy to carry out depending on the browser used.
- attention also has to be drawn to the use of unique identifiers or spyware by the suppliers of navigation tools or communication software.

Beyond this initial concern, the idea is put forward of terminal equipment that is transparent in its operation and enables the user to have full control over the data sent and received. Accordingly, the user should be able find out in a user-friendly way the precise extent of the “chattering” carried out by his or her computer, the files received, their purpose and their sender.

The right of the internet user and consumer to enjoy the benefits of consumer protection measures, in particular collective action

The trivialisation of the use of the information and communication technologies, which used to be reserved for companies, and the spread of their use in the development of E-commerce, leading to an increase in the number of online services, results in a more consumer based approach to privacy. It is as a consumer of these new services that the web surfer experiences breaches of his or her privacy (spamming, surfer profiling, adaptive pricing policies, refusal of access to certain services, etc).

This convergence of the consumers' interests in economic protection with the citizens' freedoms opens up some interesting prospects. It calls for the recognition of a right to exercise a collective legal remedy in the case of breaches of privacy, a right already recognised in connection with consumer protection. Apart from this, an entire range of provisions of consumer law would be advantageously applied. For example an obligation to provide information and advice could be imposed on operators that offer services that mainly involve the management or provision of personal data (eg, internet access providers or nominal database servers [databases containing legal data, search engines]), or it would be possible to apply the law relating to the standard terms and conditions of contracts (applicable in the case of a privacy policy) or to unfair commercial practices.

Another avenue of enquiry is the question of extending consumer product liability (terminals and software) not only to physical or financial damage but also to infringements of data protection. To what extent could a supplier of browser software the standard operation of which leads to violations of data protection not be made strictly liable for infringements by third parties?

3. Is there a necessity for specific legal instruments that go beyond Convention No. 108 in order to regulate the specific risks of attacks on freedom through the use of the information and communication technologies?

We are concerned here with answering a key question: do we need specific legislation on data protection in the information society that differs from Convention No. 108 or is it sufficient to develop the principles of this Convention in order properly to cover the data protection issues associated with the development of the information and communication technologies?

In order to answer this question, we shall run through the provisions of European Directive 2002/58/CE concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The most important provisions concern:

- the limitations relating to the processing of traffic and location data;
- unsolicited communications;
- confidentiality;
- the technical features of terminals;
- the identification of the calling line.

Mention may also be made of:

- the extension of the protection to legal persons in respect of certain provisions;

- the distinction between the subscriber and the user.

These provisions call for the following comments:

- With regard to location and traffic data, their special status in the directive can be put down to their purpose, which is limited from the outset: the conveyance of messages to or from the users of electronic communications services and the dangerous nature of the systematic processing of such data, which reveal these people's movements, consumption habits and lifestyle. In addition, is the requirement that consent be obtained for the use of these data to supply added-value services not explained in particular by the fact that, since the consent can easily be given by simply using the technologies, it may be assumed that it becomes the sole basis for the legitimacy of processings relating to these additional services?
- The explanation relating to the ease of obtaining the consent through the technologies used may similarly justify the European Union's rejection of the opt-out system, which would ultimately be based on the balance of interests traditionally employed in the context of direct marketing. Another argument is the intrusive nature of the communication, which directly penetrates the virtual home of the person concerned, as well as the ease with which such messages can be sent and the fact that the sender does not incur any costs.
- The requirements regarding the confidentiality of communications can be attributable to the fact that interactive network technology now enables its user to communicate with other people connected to it and to do so for personal purposes. This explains why the principle of the confidentiality of correspondence and the ban on eavesdropping must henceforth be extended to all electronic communications, both with respect to their content and their existences. There also arises the question of the status of the companies that convey the messages or intervene in this process: should the example of the regulations concerning the postal services and the traditional operators of telephone networks be followed by imposing on these companies regulations that would guarantee such confidentiality?
- The two last points mentioned are more novel. They affirm the right of the person using the services to have terminal facilities available that are "constructed in a way that is compatible with the right of users to pro-

tect and control the use of their personal data” and the communications network operators’ obligation to devise an infrastructure that makes it possible for them to exercise their right not to be identified.

- As regards the scope “*ratione personae*” of the new directive, it may be noted that the reasons for extending the protection to legal persons with respect to some, but not all, the provisions should be analysed to establish whether this extension actually represents a new principle or whether its *ratio legis* could be achieved in other ways, for example through a broader definition of the concept of identifiable natural persons. The distinction that may exist between the subscribers to a service and its actual users is frequently made. Examples that have been mentioned are the cases of the Adsl family subscription and a company that provides its employees with a mobile telephone. This distinction raises delicate questions since it leads to more possibilities for the subscriber to monitor the user’s employment of the services covered by the subscription. The person to be protected is no longer only the subscriber vis-à-vis the communications service provider but also the user vis-à-vis the subscriber. These issues are already addressed in connection with the surveillance of employees by their employers. As regards surveillance within the family, the notion of intra-family privacy has to be considered.

In conclusion, it is not clear that the development of electronic communications devices makes it necessary to adopt a specific sectoral convention since most of the solutions incorporated in national legislation or the European Directive only constitute a development of the general principles of data protection. However, this assertion calls at first sight for two reservations: the necessity for the regulation of products, especially terminals, and the establishment of rules or special obligations concerning the operators of networks that are necessarily involved in the conveyance of messages. This twofold concern proves necessary since the person concerned, by using electronic communication devices, is confronted by a double interface over which he or she has no control: on the one hand, the terminals that make it possible to connect to the network, and on the other the technical intermediaries between him or her and the recipient of the communication or those that intervene on his or her account.

Francesco Vatalaro⁽¹⁾

Grazie signor Presidente, e grazie all'Autorità per avermi invitato ad intervenire su questo argomento per il quale – se stamattina si parlava di Giano Bifronte – aggiungendo l'ingrediente della tecnologia *wireless*, potremo coniare un inusuale Giano Trifronte. La privacy, la sicurezza e il *wireless*, sono tre soggetti in qualche misura interallacciati, alcune volte in una unione che si rivela positiva e benefica per il cittadino, mentre in altri casi, indubbiamente, questa sovrapposizione può determinare preoccupazioni più o meno fondate. Data la limitazione di tempo e considerato che diversi argomenti sono stati già trattati a fondo, in particolare nella pregevole presentazione di stamattina del prof. Dècina, cercherò di procedere rapidamente, soffermandomi solo su alcuni degli aspetti che avevo in origine previsto.

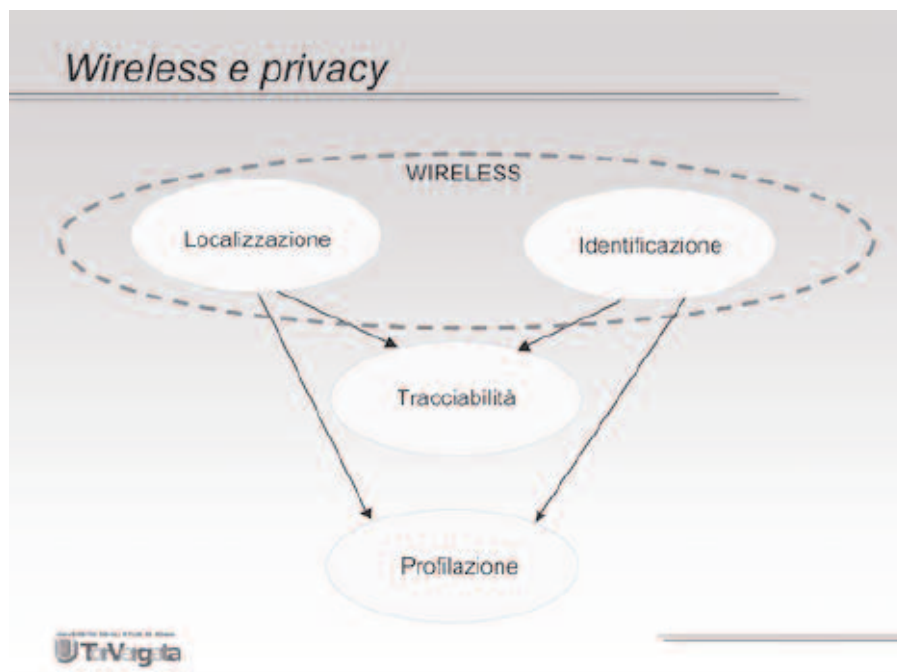


Figura 1 – Wireless e privacy.

(1) Ordinario di Radiocomunicazioni – Facoltà di Ingegneria dell'Università di Roma "Tor Vergata"

Sorvolerò pertanto sulla prima parte prevista per questo intervento, che troverete comunque disponibile nelle diapositive, e che è relativa proprio all'esame di questi tre soggetti. Vorrei passare, invece, a esaminare un po' più in dettaglio le peculiarità proprio delle tecnologie *wireless*, quando interagiscono con gli aspetti di sicurezza e di privacy.

Innanzitutto questi due ultimi elementi che oggi sono stati portati all'attenzione di tutti noi, sono legati alle due funzioni mostrate nell'ovale tratteggiato in Figura 1: gli aspetti di identificazione e di localizzazione, sono sostanzialmente i due tasselli fondamentali in cui il *wireless* viene a interagire con i problemi di privacy e di sicurezza. L'aspetto dell'identificazione ubiqua è stato assai trattato nelle relazioni di oggi perché è divenuto un punto all'ordine del giorno nel discutere sulla liceità e sulle modalità di attuazione dei servizi forniti dalle etichette *wireless*, gli identificatori a radiofrequenza chiamati in gergo Rfid (*Radio frequency identifiers*). Meno trattata mi è parsa invece l'interazione fra *wireless* e localizzazione. Non c'è dubbio che il servizio ubiquo di localizzazione con mezzi *wireless* sorge – come sempre avviene nelle buone intenzioni dei ricercatori – per risolvere il problema delle comunicazioni nelle emergenze, e ovviamente anche quello delle comunicazioni per rendere più tempestiva l'assistenza stradale. Negli Stati Uniti il problema delle emergenze è stato affrontato da molto tempo, estendendo alle reti mobili quanto già attuato nelle reti fisse, e la *Federal Communication Commission* è stata innovatrice in questo senso, avendo imposto ai gestori radiomobili, fin dal 1996, di assicurare un servizio di localizzazione, con l'obbligo di fornire l'identificazione automatica della posizione fisica del chiamante. Questo impegno è evidentemente stato dettato da fondamentali esigenze di sicurezza dei cittadini. È d'altra parte evidente che questo aspetto, poi, va valutato con attenzione in relazione alle implicazioni sulla privacy, ma non c'è dubbio che l'elemento trainante fondamentale di questa scelta favorisce anche l'inevitabile evoluzione e penetrazione della tecnologia in questo settore. A queste esigenze di base, infatti, si sono aggiunti poi altri elementi di natura commerciale, e cito qui i cosiddetti “*Location Based Services*”, servizi attuabili sia con i sistemi radiomobili di seconda generazione avanzata, sia ancor più con quelli di terza generazione. Ma se questi servizi commerciali promettono un sensibile sviluppo, non dobbiamo dimenticare che la motivazione fondamentale per assicurare la funzionalità di localizzazione in ambito *wireless* è stata l'incremento di sicurezza del cittadino.

Ed è sulla base delle due suddette funzionalità, rese ubiqua dal *wireless*, di identificazione e di localizzazione, che si forniscono i servizi di tracciabilità (inseguimento in rete dell'utente) e di profilazione (memorizzazione in rete degli attributivi parametri caratteristici dell'utente). Sia la tracciabilità che la profilazione pongono potenziali problemi di privacy.

Vorrei tornare brevemente a considerare anch'io l'aspetto di identificazione con

gli Rfid, per una considerazione. Queste etichette, che stanno suscitando molto interesse, a me che sono un ricercatore di radiocomunicazioni interessano qui fondamentalmente da un punto di vista specifico. Pertanto non entrerà nel merito delle questioni molto interessanti trattate stamattina, mentre a me queste etichette interessano in questa sede in quanto rappresentano un “laboratorio” di ciò che avverrà negli anni prossimi. In qualche misura queste etichette ci stanno mettendo, per la prima volta, di fronte a una problematica di rispetto della privacy in presenza di sistemi di telecomunicazione *wireless* diffusi nell’ambiente (fra l’altro estremamente semplici, devo dire, come sono appunto questi Rfid) a cui, tutto sommato, ancora non eravamo preparati. Non vi dico che cosa sono gli Rfid perché vi è già stato spiegato molto bene, ma faccio soltanto una piccola aggiunta a quanto già detto. Si parla molto di Rfid ma in effetti oggi sono già disponibili anche altri chip di basso costo e molto più potenti. Quello richiamato con la Figura 2 è un chip della Intel: si chiama “*Radio Free*” e la differenza sta nel fatto che questa classe di chip presenta già una notevole capacità di integrare sistemi di elaborazione e circuiti radio ricetrasmittenti. Chi conosce la legge di Moore non ha difficoltà a seguire quello che sta succedendo: l’integrazione delle funzionalità nel chip arriva già a livelli talmente spinti che oggi si riesce a fare coesistere molte funzioni in un solo chip, e questo è un primo esempio di una tecnologia, che già fa molto di più della Rfid, perché l’Rfid come dispositivo remoto è puramente passivo.

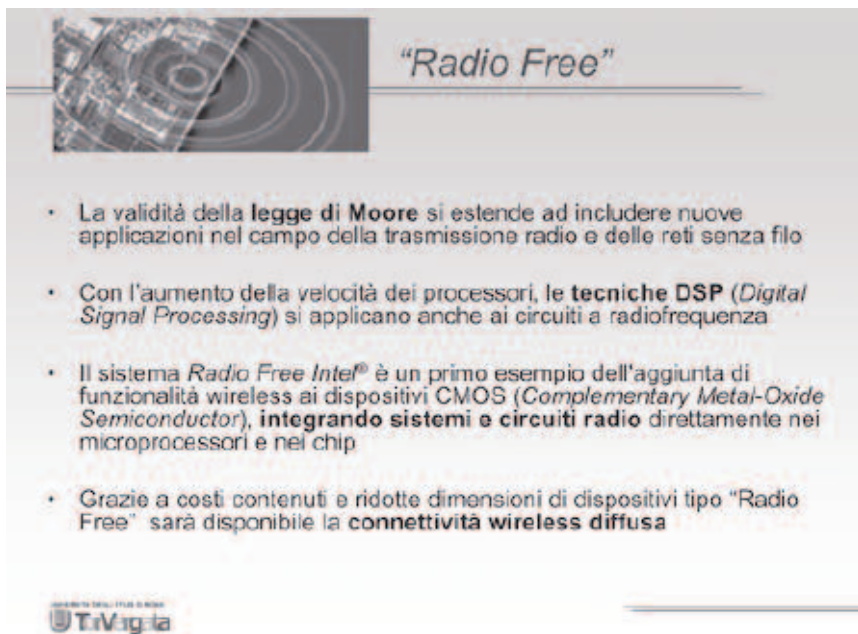


Figura 2 - Il chip “Radio Free”

Quindi si va a grandi passi verso una situazione in cui la connettività *wireless* diventa crescente, sostanzialmente perché le funzionalità integrate nel singolo chip sono sempre più spinte, e se è evidente che l'Rfid pone problemi di privacy, ciò sarà sempre più vero già con i chip dell'immediato futuro. Esaminiamoli rapidamente, questi problemi, per poi illustrare alcune delle reazioni che sono già emerse nel mondo nei riguardi di queste tecnologie:

- l'individuazione di etichette e lettori può essere resa difficile, cioè sia le une che gli altri possono essere nascosti, e quindi il consumatore può persino non essere consapevole della loro presenza;
- se non sono rimosse, le etichette *wireless* rendono continuamente identificabili gli oggetti e poi, in qualche modo, rendono identificabile chi li porta, e quindi possono essere collegate a dati sensibili, e alla fine sono soggette ad essere uno strumento utile per chi voglia fare profilazioni, lecite o illecite, dell'utente stesso.

Quindi in realtà questo dispositivo nella sua estrema semplicità, rappresenta un esempio di una possibilità – a fianco di tutte le funzionalità benefiche che offre – di portare attacchi alla privacy del cittadino. Tanto è vero che vediamo già apparire reazioni pubbliche a tutto questo. Negli Stati Uniti per esempio, esiste un'Associazione che si chiama Caspian che ha indotto Benetton a rinunciare all'uso che iniziava a fare degli Rfid sui vestiti, ed è anche responsabile di una campagna contro la Gillette che faceva ben di peggio di Benetton, associando web-cam agli Rfid per identificare visivamente l'acquirente nel supermercato.

Teniamo ben presente, tuttavia, che anche nel caso più eclatante dell'esempio della Gillette, non è “malvagia” la tecnologia in sé ma può esserlo l'uso che ne viene fatto. Ecco, allora notiamo questi punti che ho estratto proprio dal sito Internet di questa Associazione, la quale: 1) si esprime contro la caratteristica degli Rfid di fornire un codice identificativo unico, per il timore di associazioni del codice a dati personali e sensibili; 2) si oppone alla funzionalità di lettura a distanza, definendo questi componenti “*Spy Chip*”; 3) infine, è contraria comunque al loro uso poiché il sistema genera emissioni radio, ritenute potenzialmente dannose per la salute. E allora la conclusione di questi gruppi di cittadini associati negli Stati Uniti (che spesso sono all'avanguardia nell'esprimere sensibilità circa la tutela dei diritti dei cittadini) è addirittura una richiesta di interrompere le ricerche nel settore tecnologico degli Rfid.

Allora qui si può fare una prima osservazione, anche senza entrare nel merito dell'esame puntuale dei rilievi elevati nei riguardi della tecnologia Rfid. Alcune contestazioni mosse da queste Associazioni sono, forse, condivisibili altre sono certamente assai discutibili, ma rimane comunque il fatto fondamentale che è indispensabile promuovere la diffusione della conoscenza delle tecnologie, anche fra l'opinione pubblica, per evitare l'insorgere di forme di rigetto che possono essere anche

molto pericolose, per lo sviluppo prima delle conoscenze ma, poi, anche per lo sviluppo dell'economia e dei mercati. Da questo punto di vista, devo dire, è molto importante (e ritengo che l'occasione odierna sia molto utile in tal senso) l'incontro fra l'Autorità della Privacy e il mondo Universitario che è disponibile a supportare nel trasferimento di conoscenze "super partes" delle tecnologie, per mettere a fuoco quali sono i rischi reali, e quali sono invece i problemi facilmente risolvibili, nell'ottica di una corretta informazione dell'opinione pubblica.

Ecco perché, dicevo, l'Rfid è interessante. Perché ci fa vedere che cominciano ad apparire reazioni alle nuove tecnologie *wireless*, ma in una situazione in cui – dobbiamo essere molto aperti e molto franchi nell'ammetterlo – le telecomunicazioni pervasive nei prossimi anni troveranno applicazione comunque dappertutto. Si tratta infatti di tecnologie in nessun modo frenabili: si possono rallentare localmente, se ne può frenare lo sviluppo in un paese (che ne patirà conseguenze, anche serie, in termini di sviluppo e competitività internazionale), ma esse non possono essere fermate perché in realtà rispondono a esigenze profonde del cittadino, e dietro la loro diffusione ci sono non soltanto interventi di grandi multinazionali, ma anche finanziamenti pubblici, per esempio attraverso la Commissione Europea che stimola ricerche estremamente rilevanti in questo settore.

Quindi quello verso cui ci stiamo muovendo è un mondo in cui si realizzano sostanzialmente due paradigmi, come diciamo noi addetti ai lavori. Il primo è il paradigma della visione centrata sull'utente, o paradigma "*User-centered*" come si dice in lingua inglese, in cui sostanzialmente i sistemi e i servizi di telecomunicazione mettono al centro l'utente in modo da fornirgli con semplicità tutti i servizi di cui questi può avere bisogno, sempre e ovunque. Il secondo paradigma, è quello della tecnologia pervasiva e nascosta, o paradigma "*Device-less*", cosa che può far piacere o no ma è inevitabile, che discende dal fatto che evidentemente per effetto della legge di Moore possiamo avere, a costo irrisorio, potenze di calcolo, di memorizzazione e di comunicazione, estremamente vicine alle persone, diffuse e concentrate in elementi molto piccoli. La tecnologia, da questo punto di vista, è collaborativa, ubiqua, nomadica, eterna ed immanente: uso questi termini prendendoli a prestito dalla definizione di sistemi pervasivi data da ricercatori del *Massachusetts Institute of Technology*, per quanto per la nostra cultura cattolica, possa essere un modo di esprimerci non da tutti condiviso. Ma l'Mit usa forse in modo persino provocatorio questo tipo di terminologia, in quanto l'essenza di queste tecnologie è proprio l'essere dovunque e persino auto-riparabili e quindi sostanzialmente eterne. Ora ad esempio è in corso un progetto dell' Mit sulle tecnologie pervasive che, non a caso, si chiama *Oxygen*.

Le tecnologie pervasive, stanno in qualche modo seguendo un'evoluzione, da una fase che nella Figura 3 ho chiamato Fase 1, quella ancora attuale, diciamo, con

un rischio di invasività basso, livelli bassi di integrazione tra tecnologie eterogenee, e caratterizzata da tecnologie ancora ben visibili e abilitate dall'utente, con scarsa o nulla capacità di autoriorganizzazione, e con possibilità di inseguimento ancora limitate, ad una fase intermedia, che ho indicato come Fase 2, che è quella in cui stiamo entrando, nella quale l'RFid è solo uno degli esempi, in cui queste caratteristiche diventano più spinte, fino a una fase successiva, la Fase 3 che qui indicativamente ho collocato intorno al 2020 – ma la tecnologia ci ha insegnato molte volte che queste previsioni temporali possono sbagliare per eccesso – in cui il livello di integrazione fra le tecnologie è alto, e le tecnologie ormai sono divenute invisibili.

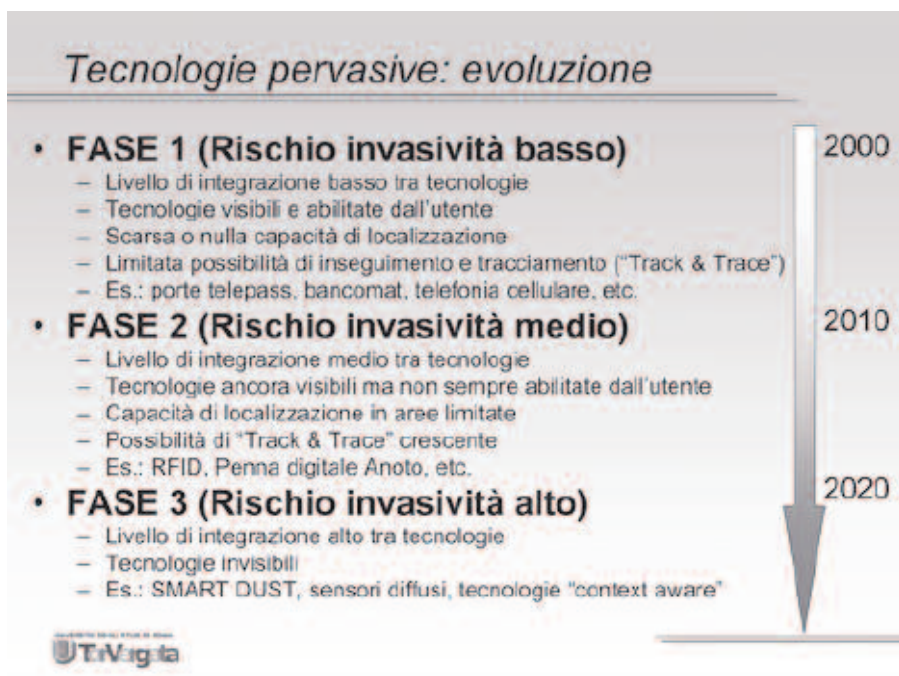


Figura 3 – Tecnologie pervasive

Un esempio di questo è il cosiddetto "*Smart dust*", su cui si sta lavorando da qualche tempo. Vediamo di cosa si tratta: questa "polvere intelligente" è un progetto dell'Università di Berkeley, in cui si integrano tutte le funzionalità che possono interessare i servizi di comunicazione, dalla memorizzazione alla sensoristica, dai sistemi di controllo a quelli di display, e perfino ai sistemi di locomozione. Si tratta quindi di una tecnologia non soltanto di telecomunicazioni, ma che mette insieme tutta una serie di altre funzionalità: è quella "polvere" cui faceva cenno stamattina il

prof. Dècina, che evidentemente può essere utilizzata per una serie di funzioni benefiche (polvere che fra l'altro finiremo per respirare), con molte possibilità di impiego, essendo equipaggiata da molteplici sensori (e finiremo persino con venirne in qualche modo anche monitorati nella nostra salute). Ma *Smart dust*, non è solo una tecnologia del domani, perché c'è già chi negli Stati Uniti ha realizzato uno *spin-off* industriale, che si chiama Dust Incorporated (www.dust-inc.com), con l'ambizione di iniziare a portare sul mercato questa tecnologia.

Polvere Intelligente



Febbraio 2002



Febbraio 2003



- **Obiettivo del progetto Smart Dust di Berkeley:**
 - Dimostrare che un completo sistema (sensore e trasmettitore) può essere integrato in un "package" della dimensione di un millimetro cubo
 - Ottenere sensibili progressi nella miniaturizzazione, integrazione e gestione dell'energia.
- **Sensori integrati:**
 - posizione, orientamento, accelerazione, magnetismo, luce, suono, temperatura, pressione, umidità, velocità dell'aria, video a bassa risoluzione, visione all'infrarosso, presenza di gas, agenti biologici, neutroni...
- **Attuatori:**
 - Sistemi di controllo, trasduttori, display, sistemi di locomozione...
- **Radiocomunicazioni:**
 - Raggio di copertura di decine di metri, cosicché per alcune applicazioni saranno necessarie matrici dense di sensori "smart dust".
- **Energia:**
 - Celle solari, generatori piezoelettrici, generatori alimentati da microscopici motori a combustione.

Figura 4 – Polvere intelligente



Figura 5 – Scenario di realtà aumentata.

Vorrei fare un'ultima considerazione, prima di andare verso leali conclusioni. Noi progrediamo anche verso un mondo di realtà aumentata, come si usa dire. Realtà aumentata vuol dire realizzare effettivamente questa fusione fra il mondo reale e il mondo virtuale: nel mondo della realtà aumentata non possiamo più staccare quella “spina” di cui parlava il prof. Dècina, e disconnetterci da Internet, perché Internet è tutto intorno a noi. Questo che vedete è, per esempio, un famoso scenario che mostra cosa si può fare proprio in questo ambiente di realtà aumentata (Figura 5). In un tale ambiente, noi veniamo un qualche modo accompagnati, attraverso opportune forme di display, da un agente sintetico, detto Avatar (quel pupazzetto che vedete in figura, sovrainpresso all'immagine reale), che realizza l'interfaccia fra noi e il mondo di Internet, e in qualche modo riesce a renderci tutte le informazioni che ci servono in qualunque luogo, in qualunque momento, per risolvere un problema specifico.

Quello qui illustrato è un problema banalissimo banale di scelta del ristorante, ma è evidente l'ampiezza delle potenziali applicazioni delle tecnologie immersive.



Figura 6 – Mobilità in ambienti immersivi.

Infine vorrei accennare sia pure rapidamente a ciò che facciamo oggi in Italia, perché in effetti anche noi operiamo, con i mezzi che abbiamo a disposizione, in questo settore scientifico della cosiddetta realtà aumentata, attraverso una collaborazione amplissima a livello universitario, in un progetto che si chiama Vicom (*Virtual Immersive Communications*), che sostanzialmente si ripromette di sviluppare sia le tecnologie di comunicazioni a banda larga, che le tecnologie pervasive di cui si parla oggi, che infine le tecnologie di contenuti virtuali e multimediali, proprio nell'ottica della imminente Società della Conoscenza.

In pratica l'obiettivo è integrare le comunicazioni ubique con varie tecnologie audio, video e di sensoristica, per aumentare sensibilmente il senso di presenza nelle comunicazioni. Vi illustro soltanto, e questa è l'ultima immagine che presento sperando di non aver rubato troppo tempo, uno dei dimostratori che sono previsti nel progetto Vicom (Figura 6). È un dimostratore che abbiamo chiamato "*Mobility in Immersive Environments*", con lo scopo di provare tecnologie avanzate di mobilità, in un unico "campus virtuale", in cui sostanzialmente, oltre a essere presenti le figure fisiche reali, sono associati anche elementi virtuali, che vengono trasportati dalla rete da locazioni fisiche anche molto distanti. Un obiettivo di questa parte del progetto è dimostrare nuove tecnologie di guida virtuale. Nella figura vedete due

esempi: quello in alto è l'esempio di un terminale portatile che consente al possessore di spostarsi raggiungendo un posto o una persona che a priori per lui possono essere persino ignoti, ma viene guidato dalla rete, che mostra sullo schermo l'immagine di ciò che effettivamente lui/lei sta vedendo, come conferma di ciò che sta facendo; nell'immagine in basso si vede un navigatore immersivo, basato su tecniche che imprinono le direzioni di guida direttamente sullo schermo di un veicolo. Queste sono solo alcune delle tecnologie immersive del domani sulle quali oggi si sta lavorando e sarebbe molto interessante poterle approfondire, anche sulla base delle valutazioni degli impatti sul cittadino, tra cui evidentemente molto rilevanti sono proprio gli impatti sulla privacy.

Quindi concludo dicendo semplicemente che nei futuri scenari tecnologici, queste funzionalità saranno comunque sviluppate ed è molto importante che queste tecnologie pervasive e immersive, godano di un'attenzione speciale data la forte caratteristica di innovatività e il forte impatto sociale che è ad esse connesso, ma senza imporre norme e regole discriminatorie. In particolare, ritengo che sarebbe opportuno fin d'ora approfondire, non solo tale impatto, ma anche quali sono le possibilità che queste stesse tecnologie offrono per dare un contributo al miglioramento della protezione della privacy del cittadino.

Grazie.

Dario Di Zenobio⁽¹⁾

A proposito di reti wi-fi geografiche, non vorrei che in questo clima di innovazione qualcuno pensasse a qualche nuovo standard di rete, o a una evoluzione del, credo ben noto, wi-fi; più semplicemente questo titolo criptico sta ad indicare particolari applicazioni dalla tecnologia wi-fi in aree, aree geografiche, che tipicamente soffrono il digital divide.

Io in questo mio intervento però, vorrei procedere in qualche modo più liberamente rispetto alla presentazione programmata, perché cogliendo qualche punto qua e là dagli interventi del pomeriggio, mi sorge spontanea qualche riflessione.

Ho sentito molto parlare di innovazione, di servizi, di applicazione; in qualche modo tutto questo mi stimola, ci stimola tutti, però vorrei ricordare che da una parte il successo di queste cose, quindi degli applicativi, delle applicazioni, dei servizi innovativi, è determinato soprattutto dalla infrastruttura di rete, ovvero, dalla capacità di avere una rete, scusate il bisticcio, capace e potente, e dall'altra dall'educazione all'uso del mezzo tecnologico.

Io mi riconosco perfettamente ignorante, tuttora, nell'utilizzo del telecomando del video registratore o del monitor al plasma e così via, quindi se noi vogliamo veramente avere successo, con le nuove tecnologie, con tutto quello che si propone di nuovo, dobbiamo in qualche modo educare e dare la possibilità di una infrastruttura capace. Per quanto riguarda l'educazione, non è compito nostro, mio, cioè di gente tipicamente abituata alle reti per telecomunicazioni, accrescerne il livello, ma sicuramente per la infrastruttura di rete, qualcosa possiamo fare.

Vorrei richiamare un attimino, e vado velocemente, il concetto di Digital Divide, che è notissimo, però spesso viene confuso con il fatto che parliamo di aree che sono in qualche modo svantaggiate, penalizzate economicamente. Questo è vero, però non ci dimentichiamo che il Digital Divide può essere presente in aree "ricche"; per esempio Courmayeur soffre il Digital Divide e così Capri. Cito Capri in particolare, perché voglio fare un collegamento con problemi di privacy in applicazioni wi-fi. Mi viene così immediato perché ho sentito questa notizia: a Capri c'è una rete di monitoraggio, basata su tecnologia wi-fi e web cam distribuite nella parte principale della cittadina (la stessa cosa avviene, questo lo so per certo, perché mi scontro spesso con il Sindaco, a San Benedetto Belbo, e così in altri piccoli paesi distribuiti nelle Alpi).

Risultato: giustificandosi col Digital Divide e con reti di monitoraggio, i co-

(1) Dirigente di ricerca - Fondazione Ugo Bordoni

muni danno dei servizi ai cittadini, lodevoli servizi per carità, ma sostituendosi agli operatori telco. D'accordo con il telemonitoraggio, "per la sicurezza" (purché si rispetti la privacy) ma poi si finisce col dare accesso a internet in modo libero, gratis, sostituendosi quindi agli operatori, utilizzando denaro pubblico, e creando una concorrenza sleale.

Tutti questi sono aspetti veramente importanti da trattare, che, per quello ho voluto richiamare il concetto di Digital Divide, vanno inquadrati nel giusto quadro di riferimento. Non ci dimentichiamo però che noi dobbiamo potenziare la rete, migliorare in qualche modo l'infrastruttura, facilitare l'accesso a internet, ed educare anche il cittadino.

Ma per fare questo la tecnologia, vado avanti velocemente, la tecnologia wireless può aiutare, aiuta senz'altro. La tecnologia wi-fi è una tecnologia che può aiutare lo sviluppo delle reti, soprattutto in queste aree svantaggiate, dove sicuramente la fibra ottica, o altri mezzi, che sono dei mezzi impegnativi, non possono arrivare.

Però, non ci dimentichiamo che nel potenziare l'infrastruttura, vanno potenziati due parti, una che riguarda la linea "feeder", questo è un termine tecnico, diciamo per telecomunicazionisti, ovvero il broadband verso la rete, la dorsale verso la rete: se il paesino sta in montagna, e io faccio una rete wi-fi locale che lo copre tutto, una rete wireless lan, come quella che esiste in questa sala, dove i vari computer sono collegati senza filo, c'è una rete di tipo cellulare, per intenderci. Riesco così a risolvere il problema del cablaggio del paesino, però a questo paesino poi, la condotta principale, gliela devo portare, quindi, devo in qualche modo potenziare la linea di dorsale, la linea di alimentazione.

E a tal riguardo, in questa presentazione, ho riportato (ci sono sforzi comuni da parte del Governo, del Ministro, del Ministero, degli operatori) anche un comunicato del Ministro Gasparri, che credo verrà più tardi, un comunicato del 1° agosto 2003, nel quale appunto "si autorizza la sperimentazione del wi-fi, per collegamenti punto-punto". Collegamenti punto punto significa dare anche la possibilità di potenziare la linea di alimentazione, però non ci dimentichiamo, e qui lo dico perché voglio essere preciso, che "sperimentazione" significa dire che uno fa un esperimento, viene autorizzato per l'esperimento; chiede l'autorizzazione, rende pubblici i risultati e non ne fa un uso economico, non ne fa un business, quello che invece sta avvenendo in molti casi. Cito un esempio: Video Bank a Catania ha annunciato di aver realizzato 500 hot-spots, collegati lungo l'autostrada e lungo la valle dell'Etna, chiamiamo Valle ma diciamo Etna, senza, per quanto io ne sappia, (fra l'altro voglio dire che i dati per le autorizzazioni circolano da noi, diciamo tra il Ministero delle Comunicazioni e Fondazione Ugo Bordoni) alcuna autorizzazione (lo stesso caso è pubblicizzato nel sito Intel a proposito di wi-fi). Quindi, se effettivamente, ci dev'essere sviluppo, lo sviluppo dev'essere pilotato e deve rispettare le re-

gole. C'è stata una regolamentazione, ci abbiamo lavorato: le regole possono pilotare. Ma soprattutto ci dobbiamo calare nelle realtà del nostro territorio, del nostro paese. Quando siamo andati insieme a Telespazio a San Giuliano di Puglia (un caso veramente triste), per dare un minimo conforto creando un accesso a internet veloce, portando anche un terminale satellitare, una bambina mi ha chiesto: “ma come mai tutte queste cose quando prima non avevamo nemmeno un gessetto?” cioè non ci dimentichiamo la realtà nazionale, d'accordo l'innovazione, d'accordo il tizio con il video della vita nel taschino, ma nella comunità montana della Majella, questo col video già immagino che dica: “ma la vita mia già fa tanto schifo, che fa? Me la rivedo pure?”.

Insomma voglio dire, ci sono dei concetti che vanno in qualche modo rivisti, affinché le tecnologie possano evolvere.

Per ultimo, dico, visto che parliamo di innovazione, che sono i contenuti, i servizi a determinare la novità, non tanto le tecnologie, che si possono consumare da sole, come per esempio il wi-fi, vi ricordate la diatriba Umts/wi-fi? Questo sconfigge, quello vince? No, qui non vince nessuno e tutto può avere successo se c'è preparazione e se l'utente viene preparato a queste evoluzioni. Con questo ho concluso, spero di essere stato veloce.



Tavola rotonda

**SESSIONE II
LE GARANZIE
NELLE COMUNICAZIONI**

COORDINATA DA ALESSANDRO CECCHI PAONE

Sessione II - Tavola rotonda

Le garanzie nelle comunicazioni

Coordinata da Alessandro Cecchi Paone⁽¹⁾

Interventi di: 1. Maurizio Gasparri; 2. Silvio Traversa; 3. David Banisar; 4. Guido Salerno.

1. Maurizio Gasparri⁽²⁾

Nel marzo 2000 il Consiglio Europeo ha definito a Lisbona una strategia per intraprendere un profondo rinnovamento del tessuto economico e sociale dei Paesi dell'Unione basato sullo sviluppo delle tecnologie digitali e delle Società dell'Informazione.

Questa strategia è poi confluita nel *Piano eEurope* 2002 per lo sviluppo della Società dell'Informazione in Europa con tutta una serie di obiettivi specifici per la diffusione delle tecnologie digitali nelle famiglie, nelle imprese e nelle amministrazioni pubbliche.

Grazie a questo piano negli anni successivi l'economia legata alle connessioni telematiche ha avuto una crescita rapida, è aumentata la concorrenza, i prezzi delle telecomunicazioni sono diminuiti ed è stato adottato a livello europeo un quadro normativo armonico per le comunicazioni elettroniche. Tanto che nel maggio 2002 *eEurope* ha avuto un seguito nel *Piano d'azione eEurope* 2005 che, capitalizzando gli sforzi del biennio precedente, ha spinto il piede sull'acceleratore della banda larga e dell'Internet veloce, dello sviluppo di moderni servizi pubblici on-line per pubblica amministrazione, istruzione e sanità, della creazione di nuovi modelli di *ebusiness* per le imprese e del potenziamento di un più evoluto sistema di sicurezza delle informazioni in rete.

Con *eEurope* 2005, quindi, in particolare, la sicurezza delle reti assume una posizione centrale nelle politiche di sviluppo dell'economia digitale in Europa.

Il Piano evidenzia, in maniera esplicita, il legame esistente tra la crescita economica derivante dall'aumento delle interconnessioni telematiche e l'attenzione ai profili della sicurezza delle telecomunicazioni. Solo la certezza che ci siano regole precise e applicazioni tecnologiche che garantiscano la sicurezza delle comunicazio-

(1) Giornalista

(2) Ministro delle Comunicazioni

ni elettroniche può fare in modo che consumatori e imprese siano incoraggiati a utilizzare la rete per le loro transazioni economiche, creando le condizioni per lo sviluppo dei mercati. La sicurezza ha assunto, pertanto, un'importanza critica tale da farne un presupposto indispensabile per la crescita delle imprese di commercio elettronico e per il funzionamento dell'economia nel suo complesso.

I governi sono ormai consapevoli che non solo le loro economie, ma anche tutto il sistema di organizzazione sociale dipende fortemente da un efficace funzionamento delle reti di comunicazione.

Le tecnologie dell'informazione e delle comunicazione elettronica hanno ormai assunto un ruolo fondamentale nelle nostre società: servizi e apparati informatici e di telecomunicazione da semplici strumenti di lavoro stanno sempre più diventando elementi pervasivi della vita quotidiana di ciascuno di noi. E le preoccupazioni in materia di sicurezza delle comunicazioni elettroniche e dei sistemi di informazione sono aumentate parallelamente al rapido incremento, anche grazie ai sistemi di trasmissione a larga banda, del numero di utenti e del valore economico e sociale delle transazioni e degli scambi che avvengono attraverso le reti.

Le reti e i sistemi di informazione veicolano un volume e una pluralità di servizi e dati inconcepibili fino a pochi anni fa. La loro disponibilità è essenziale per infrastrutture quali la rete idrica e la rete elettrica e per l'erogazione dei servizi pubblici essenziali.

Lo scenario è cambiato in maniera radicale rispetto a solo un decennio fa. Fino a pochi anni addietro la sicurezza dei sistemi di comunicazione elettronica era una questione che riguardava essenzialmente le imprese monopolistiche che fornivano i servizi di telecomunicazione sulle reti pubbliche, in particolare sulla rete telefonica.

La situazione è notevolmente cambiata con la liberalizzazione dei servizi di telecomunicazione e la concorrenza di più operatori privati nel mercato, con l'introduzione di sempre più innovative e sofisticate tecnologie della comunicazione, con lo sviluppo della convergenza delle reti e con la globalizzazione dei mercati a livello mondiale.

Tutto ciò fa sì che gli Stati in quanto autorità preposte alla regolamentazione e alla vigilanza dei mercati e dei sistemi di organizzazione sociale debbano assumere un ruolo attivo per garantire la sicurezza delle reti di comunicazione elettronica. E la dimensione mondiale della interconnessione delle reti esige che questa funzione di garanzia si svolga anche attraverso un'attività di cooperazione internazionale tra gli Stati.

Sicurezza delle informazioni in rete è innanzitutto protezione dei dati personali che passano sulle reti di comunicazione elettronica, e su questo aspetto gli autorevoli relatori di questo convegno hanno già esposto e forniranno domani le loro interessanti analisi sia con riferimento al recepimento della direttiva n. 2002/58/CE, relativa al-

la tutela della vita privata nel settore delle comunicazioni elettroniche, sia al nuovo Codice in materia di dati personali di cui al d.lg. 30 giugno 2003, n. 196.

Ma sicurezza delle informazioni in rete è anche sicurezza delle comunicazioni dagli attacchi del crimine informatico, sicurezza delle transazioni commerciali e dei patrimoni finanziari on-line, sicurezza dei know-how aziendali che utilizzano modelli di *ebusiness* aperti alla rete, sicurezza dei soggetti deboli sempre più privi di difese di fronte alla pervasività delle reti.

Su questi aspetti il Ministero da me guidato ha svolto la sua parte sia nel contesto nazionale sia in quello internazionale ed europeo in particolare.

Voglio ricordare al riguardo la creazione dell' *Osservatorio sulla sicurezza delle reti e la tutela delle comunicazioni*, operante dal 16 giugno 2003 presso il Ministero delle comunicazioni con la collaborazione di rappresentanti di altri Ministeri (Giustizia, Interno, Difesa, Attività produttive, Dipartimento della Funzione Pubblica, Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri).

Tra i compiti dell'Osservatorio ci sono la predisposizione degli atti normativi in materia di sicurezza delle reti, di tutela delle comunicazioni e di attività investigative a fini di giustizia (compresa la rete Internet anche a tutela dei minori), la tenuta dei rapporti con gli organismi nazionali ed internazionali, il monitoraggio dell'attività degli operatori assoggettati ad obblighi verso l'Autorità giudiziaria ed altri organismi di garanzia, il monitoraggio dello sviluppo tecnologico del settore delle telecomunicazioni con specifico riguardo alla sicurezza.

Per quel che riguarda poi i servizi della pubblica amministrazione con decreto interministeriale (Comunicazioni, Innovazione e Tecnologie) del luglio 2002 è stato costituito un *Comitato tecnico nazionale per la sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni* per indirizzare e coordinare le diverse iniziative connesse con il Piano Nazionale della sicurezza Ict e definire gli standard di sicurezza nella pubblica amministrazione.

Sicurezza delle reti di comunicazione nell'ottica delle politiche messe in atto dal mio Ministero è anche sicurezza delle informazioni fruibili in rete da parte dei soggetti in età evolutiva.

Sulla scia del successo del codice di autoregolamentazione "Tv e minori", al Ministero delle Comunicazioni ci siamo posti il problema di come tutelare questi soggetti deboli di fronte all'anarchia della rete Internet ed alle minacce che da essa possono venire al corretto svolgimento del processo di formazione della loro personalità.

Il 19 novembre 2003 Federcomin, le associazioni degli internet provider e gli altri soggetti rappresentativi del settore hanno firmato presso la nostra sede ministeriale il Codice di autoregolamentazione "Internet e minori".

Il Codice, sulla cui applicazione vigila un comitato di garanzia appositamente costituito, impegna i provider a rendere più sicura la navigazione dei minori nella

rete, contribuendo tra l'altro alla lotta a reati come la pedo-pornografia *on line*.

Internet, del resto, è uno dei settori più difficili da regolamentare. Sfugge ai confini nazionali e si trasforma con una tale velocità che il Legislatore difficilmente riesce a seguirne in tempo reale le evoluzioni. Un codice di autoregolamentazione ci sembrava essere uno strumento più snello che ci poteva permettere di definire in maniera efficace modalità operative di facile attuazione per perseguire comportamenti illeciti che spesso rimangono impuniti.

Con esso i provider che forniscono spazi web per la realizzazione dei siti Internet si impegnano a mantenere le informazioni necessarie a identificare gli autori dei contenuti, nel rispetto della normativa sulla tutela dei dati personali. In questo modo si rafforza una prassi già realizzata dagli operatori del settore, che favorisce la lotta al crimine e mette le forze dell'ordine, come il Servizio della Polizia Postale e delle Comunicazioni, nelle condizioni di consegnare alla giustizia i criminali identificati.

Per concludere questa panoramica sulle linee d'azione del Ministero delle Comunicazioni in materia di sicurezza delle reti di telecomunicazione vorrei fare un cenno alle iniziative promosse a livello europeo.

Un aspetto fondamentale da tenere in considerazione per un'efficace tutela della sicurezza delle comunicazioni elettroniche è la loro dimensione transfrontaliera. Per poter avere un sistema di norme dotate di effettività non si può quindi prescindere da una cooperazione sistematica a livello internazionale e da un coordinamento stabile a livello europeo in particolare.

In questa direzione va l'istituzione dell'Agenzia europea per la sicurezza delle reti e dell'informazione (Enisa, definitivamente approvata dal Consiglio dei Ministri europei per le Telecomunicazioni nella riunione del 20 novembre 2003), per la cui creazione fondamentale è stato l'impulso dato dal mio Dicastero nel periodo del Semestre di Presidenza dell'Unione Europea.

L'Agenzia servirà a realizzare quella cooperazione che si rendeva necessaria a livello europeo con l'obiettivo di diffondere la cultura della sicurezza e della prevenzione nel campo delle nuove tecnologie della Società dell'Informazione e di coordinare le iniziative degli Stati membri volte a contrastare il fenomeno della criminalità informatica.

Il nuovo organismo avrà compiti consultivi, costituendosi come centro di studio, raccolta e scambio di informazioni e documentazione in materia di rischi e sicurezza dei sistemi informatici, con funzioni di sensibilizzazione e consulenza nei confronti della Commissione e degli Stati membri. Ma avrà anche un ruolo operativo, in quanto attivamente coinvolta nell'applicazione delle norme relative agli *standard* che garantiscono i livelli di sicurezza opportuni per i prodotti e i servizi creati dalle aziende ed introdotti sul mercato.

2. Silvio Traversa⁽³⁾

Desidero in primo luogo ringraziare il presidente Rodotà ed i colleghi del Garante per la protezione dei dati personali, per l'invito che mi hanno rivolto a partecipare a questo convegno, considerato che il tema oggi dibattuto, ovvero "Le innovazioni tecnologiche e la privacy", è di grande momento.

Devo dire che sono rimasto favorevolmente impressionato dagli interventi che mi hanno preceduto, attraverso i quali ho avuto modo di apprendere molte cose nuove.

Il tema di questa tavola rotonda riguarda "Le garanzie nelle comunicazioni" un tema che interessa in modo particolare l'Autorità, alla quale mi onorò di appartenere, che il legislatore italiano, seppur in ritardo rispetto agli altri legislatori europei ha istituito con legge 31 luglio 1997, n.249.

L'Autorità per le garanzie nelle comunicazioni ha peraltro iniziato la sua attività solo nel 1998, più esattamente nella prima metà del 1998, (gli otto commissari erano stati eletti dal Parlamento il 12 febbraio) in quanto i primi mesi servirono a definire le procedure organizzative, come previsto dalla legge, con l'adozione di tre regolamenti: quello relativo all'organizzazione ed al funzionamento dell'Autorità, quello concernente la gestione amministrativa e la contabilità ed infine quello relativo al trattamento giuridico ed economico del personale. Da allora abbiamo fissato molte regole, procedendo spediti verso la liberalizzazione del mercato delle telecomunicazioni grazie all'adozione di un numero rilevante di delibere che, oggi lo possiamo dire, hanno inciso profondamente sul mondo delle telecomunicazioni e dei mass-media.

Una significativa caratteristica di questa Autorità è costituita dal fatto di essere un'Autorità della "convergenza". La scelta operata dal legislatore nel '97, che all'epoca poteva sembrare una scommessa e che oggi appare cosa scontata, è stata quella di creare un'unica Autorità, fenomeno raro nel contesto europeo se non addirittura mondiale, che si occupasse sia del settore dell'editoria e della televisione, sia delle telecomunicazioni, con una Commissione per i Servizi ed i Prodotti ed una Commissione per le Infrastrutture e le Reti che insieme formano il Consiglio dell'Autorità.

Quella che allora poteva apparire una anticipazione discutibile è oggi diventata realtà: la convergenza si è infatti realizzata ed è davanti agli occhi di tutti noi.

Sono sensibilmente migliorate sia le condizioni concorrenziali, sia le prospettive di crescita dell'intero comparto delle telecomunicazioni; sul fronte dei prezzi, aspetto che più interessa i cittadini-utenti, si sono inoltre registrati negli ultimi cinque anni diminuzioni consistenti che hanno favorito lo sviluppo di nuove applicazioni e di nuovi servizi.

(3) Commissario Autorità per le garanzie nelle comunicazioni

Vero è che, a fronte di queste luci dobbiamo registrare anche qualche ombra. Il solo fatto che abbiamo assistito ad una crescita generalizzata del settore, non è sufficiente a farci ritenere pienamente soddisfatti: c'è ancora molto da fare soprattutto relativamente alla qualità dei servizi forniti all'utenza.

In ogni caso è indubbio che – al di là delle oscillazioni di tipo congiunturale – il settore delle Tlc ha conquistato un ruolo strutturale nei modelli di sviluppo dei paesi avanzati, favorito altresì dalle profonde trasformazioni del quadro regolamentare europeo, soprattutto alla luce delle recenti Direttive per le reti di comunicazione elettronica che l'Italia ha prontamente recepito, grazie anche alle sollecitazioni ed all'impegno del ministro Gasparri, che saluto.

I punti dai quali non possiamo prescindere nel parlare di garanzie nelle comunicazioni sono quelli che emergono dalla stessa Costituzione, ed in particolare gli articoli 15 e 21.

L'articolo 15 si sofferma sulla libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione, definendole inviolabili – è questa la forma di comunicazione che comunemente definiamo interpersonale ed intersoggettiva – l'altro pone invece l'accento sulla libera manifestazione del pensiero con la parola, lo scritto e ogni altro mezzo di diffusione dando luogo a quella che viene comunemente definita, comunicazione di massa.

Questi modi di tutela di due diverse manifestazioni della libertà di espressione della comunicazione, nel corso degli anni, soprattutto di quest'ultimi anni, hanno subito una vera e propria evoluzione, collegata all'avvento delle nuove tecnologie che rende oggi certamente meno agevole lo stabilire dove cessa la comunicazione interpersonale, libera e segreta e dove inizia invece, quella cosiddetta di massa, per sua natura palese e destinata ad un numero non precisamente determinabile di destinatari.

Ormai grazie all'evoluzione tecnologica, si pensi ad internet, e ai nostri ripetuti interventi che, hanno certamente favorito il processo di liberalizzazione è oggi possibile avere, anche dentro casa, una sorta di "laboratorio convergente", dove computer e televisione dialogano tra loro, aprendo le porte a nuove forme di sfruttamento dei contenuti e dei programmi tv.

Tutto questo ha trasformato anche il modo di operare dei diversi soggetti attivi sul fronte della comunicazione.

Se prima infatti esisteva un solo imprenditore, un solo operatore che gestiva, ad un tempo, la rete ed i contenuti, adesso distinguiamo tra operatori di rete che hanno il regime giuridico proprio dei licenziatari ed i fornitori di contenuti e servizi che invece operano in regime di mera autorizzazione.

Ma non è tutto. Il processo di convergenza prospetta un percorso diretto alla fissazione di regole comuni a tutti i paesi europei; e non è un caso che si sia già opportunamente evocata (mi riferisco alle lucide riflessioni dell'amico Cassese) la co-

stituzione, sia pure ancora in nuce, di un diritto amministrativo europeo.

Il nuovo quadro regolamentare europeo, ad esempio in tema di posizioni dominanti, ha indicato puntuali procedimenti, articolati e complessi, ai fini della determinazione del possesso, da parte degli operatori, della significativa forza di mercato, sulla base della regolazione tipica antitrust, la quale stabilisce ex post e non più ex ante, le misure riequilibratrici per una corretta competizione.

Tale complesso di nuove regole ha previsto altresì sempre più efficaci strumenti di raccordo tra le varie Autorità nazionali competenti per le comunicazioni e le Autorità Antitrust, e tra il complesso delle Autorità nazionali e la Commissione europea attraverso l'azione del Gruppo dei Regolatori Europei (Erg).

Per quanto concerne il mercato della Televisione occorre sottolineare l'importante svolta, di carattere strutturale, rappresentata dall'introduzione della televisione digitale e dall'adozione della Legge Gasparri che, nonostante le polemiche ed i conflitti politici cui ha dato luogo per talune sue scelte, ritenute non conformi al sistema costituzionale della comunicazione, ha avuto il merito di porre ordine in un sistema sviluppatosi spontaneamente in assenza di regole puntuali, dando vita ad una vera e propria legge di sistema.

L'art. 13 c.1 di questa legge, in particolare, recita che "L'Agcom nell'esercizio dei compiti ad essa affidati dalla legge, assicura il rispetto dei diritti fondamentali della persona nel settore delle comunicazioni elettroniche, anche radiotelevisive". "Le funzioni di cui al comma 1, precisa la legge, sono svolte anche attraverso i Co.re.com" - i Comitati regionali per le comunicazioni istituiti con legge regionale ma funzionalmente "organi dell'autorità" - che, da quest'anno hanno iniziato finalmente a svolgere i compiti loro assegnati dalla legge e parte di quelli delegatigli dall'Autorità. Ad oggi sono state sottoscritte convenzioni tra l'Autorità e buona parte delle regioni, l'ultima delle quali è stata siglata proprio ieri con la Regione Piemonte. Ancora non tutto il quadro è stato completato anche se in buona sostanza già oltre 10 Regioni hanno sottoscritto questa convenzione con l'Autorità che ha delegato loro, dopo una lunga serie di incontri e tavoli tecnici, alcune rilevanti competenze nel territorio di riferimento, che concorrono certamente ad avvicinare i cittadini alle istituzioni.

Per quanto riguarda altri settori che interessano direttamente il tema delle garanzie, dobbiamo osservare che molto è stato fatto sul versante del diritto d'autore e della pirateria informatica, così come nel settore della tutela dei minori dove l'Autorità svolge un'attenta attività di vigilanza (nel periodo aprile 2003/2004 relativamente alle segnalazioni provenienti da privati ed associazioni, l'Autorità ha vagliato circa 50 nuove presunte ipotesi di violazione relative a film e a programmi vari). Altro importante strumento per garantire parità di trattamento ed imparzialità a tutti i soggetti politici è costituito dalla cosiddetta "par condicio". Nel periodo 1 aprile 2003 -

30 aprile 2004 l'Autorità ha emanato 87 provvedimenti; ed anche per quanto riguarda la "tutela del pluralismo dell'informazione" è intervenuta in più occasioni.

Non volendo ulteriormente abusare della vostra attenzione, desidero in conclusione, osservare che la globalizzazione e la convergenza, insieme ai mutamenti nei processi produttivi avvenuti in questi ultimi anni, hanno modificato i contenuti e gli obiettivi delle imprese che operano nella comunicazione, rimodellando altresì il ruolo stesso dei "fruitori" del prodotto, allettati da una gamma mutevole e diversificata di prodotti e servizi: cellulari di terza generazione – Umts - per quanto riguarda la telefonia mobile, la banda larga nella telefonia fissa, una vasta gamma di programmi, grazie all'introduzione della televisione digitale terrestre, che certamente migliorerà la qualità delle immagini e, ci auguriamo, anche quella dei contenuti delle trasmissioni.

3. David Banisar⁽⁴⁾

Introduzione

Generalmente, nel classificare le nuove minacce per la privacy si distingue fra quelle dovute agli sviluppi tecnologici e quelle derivanti da iniziative dei governi. Tuttavia, è sorta una nuova minaccia che deriva dalla combinazione delle due categorie, cosicché sono le norme a spingere la tecnologia verso il potenziamento delle capacità di sorveglianza. Questo nuovo approccio, cosiddetto di “conservazione indiscriminata dei dati”, comporta l’adozione da parte dei governi di norme di legge che impongono ai fornitori di telecomunicazioni di conservare informazioni sulle attività svolte dai rispettivi utenti. Ciò avviene entro un contesto giuridico in cui alle informazioni in oggetto, che possono riguardare opinioni politiche, dati sanitari, informazioni di carattere finanziario, ed altri dati di tipo sensibile, viene riconosciuta una tutela giuridica inferiore rispetto alle comunicazioni effettuate attraverso le reti telefoniche tradizionali.

Convergenza e neutralità delle tecnologie

Forme diverse di comunicazione e tecnologie informatiche stanno rapidamente convergendo ed espandendosi in tutti i settori della vita quotidiana. Nuove tecnologie sono in grado di raccogliere su base routinaria dati personali sinora mai contemplati (un elenco di tutti gli articoli letti, l’ubicazione di una determinata persona in qualsiasi momento) in modi sinora inimmaginabili (il tracciamento come situazione standard).

In primo luogo, è essenziale stabilire le differenze. Venti anni or sono, quando esisteva soltanto la telefonia tradizionale, una persona sollevava la cornetta e chiamava un’altra persona ad un altro telefono, e tutto ciò che era noto al sistema era che un determinato telefono in una determinata abitazione veniva utilizzato per comporre il numero di un altro telefono in un’altra abitazione e stabilire una connessione che aveva una certa durata – nessun’altra informazione era raccolta. La società telefonica in genere sapeva chi fosse il proprietario del telefono; magari poteva trattarsi di un’azienda, oppure di una persona fisica, ma non sapeva chi fosse l’utilizzatore effettivo del telefono.

Oggi, invece, le tecnologie della comunicazione permettono di raccogliere una massa di informazioni molto più consistente. La posta elettronica consente di registrare chi abbia utilizzato un certo computer, a che ora, dove – e non deve trattarsi necessariamente di una sede fissa in un determinato momento –, per comunicare con un’altra persona, di cui in genere conosciamo l’identità specifica oltre all’oggetto della comunicazione e, naturalmente, quello che i due interlocutori si sono detti.

⁽⁴⁾ Vice Direttore di Privacy International

Con i cellulari, anziché avere un telefono fisso in una determinata località con cui chiamare un altro telefono fisso, in genere si verifica che una persona identificabile chiama un'altra persona identificabile da una località specifica ad un'ora specifica e per un certo periodo – ma sempre senza che ciò comporti necessariamente la registrazione dei contenuti di tale comunicazione. Tuttavia, quando si comincia ad utilizzare Sms, Mms ed altre tecnologie, di fatto si ha la raccolta dei contenuti di una comunicazione.

Dal punto di vista giuridico, tutto ciò presenta interessanti risvolti. In genere si afferma che la legge dovrebbe essere tecnologicamente neutrale, che non dovrebbe riservare alle informazioni raccolte in un certo modo un trattamento diverso da quello utilizzato per le informazioni raccolte in un altro modo. Le legislazioni nazionali in materia di intercettazioni prevedono da tempo regole sulle intercettazioni telefoniche e sul trattamento da applicare alle informazioni raccolte attraverso di esse. Altre disposizioni, contenute per esempio nella Direttiva Ue sulla protezione dei dati e nella Convenzione del Consiglio d'Europa sui trattamenti automatizzati di dati, hanno fissato da tempo norme sulla raccolta e l'utilizzazione dei dati personali.

Tuttavia, la raccolta di queste informazioni attraverso le reti telematiche comporta, di fatto, un abbassamento della tutela della privacy. In molti Paesi, come gli Usa ed il Regno Unito, i dati relativi alle comunicazioni, compresi i dati sensibili, vengono considerati alla stregua dei dati di traffico telefonico puro e semplice di vent'anni or sono, anziché secondo gli standard più elevati applicabili alle intercettazioni.

In realtà, io credo che questi dati dovrebbero godere dello stesso livello di tutela; che le informazioni relative, per esempio, ai siti web visitati – supponiamo che un soggetto visiti un sito che tratti di Aids, o di tossicodipendenze, o di materie sindacali, oppure i siti web di alcuni giornalisti che hanno una specifica opinione politica – forniscono quasi le stesse informazioni privatissime che si possono trovare nella propria cartella clinica. Forse si tratta di informazioni ancora più intime, perché quando si parla con un medico talvolta si pratica una forma di autocensura, non fidandosi di quanto avverrà delle informazioni contenute in una cartella clinica elettronica. Invece, quando si usa la Rete, non sempre si riflette sul livello delle informazioni raccolte e sull'ampiezza di tali informazioni.

Il problema è reso ancora più grave dalle nuove normative in materia di conservazione dei dati, che prevedono la sorveglianza routinaria degli utenti – cosa che mai sarebbe accettabile per le comunicazioni verbali.

Conservazione dei dati, protezione dei dati e Convenzione europea dei diritti umani

In passato, per le intercettazioni riferite a comunicazioni telefoniche valevano i principi fissati nell'Articolo 8 della Convenzione europea dei diritti umani e richiamati dalla Corte europea dei diritti umani in casi quali *Klass c. Germania*, *Malone c. Regno Unito*, ecc. : doveva trattarsi di attività conformi alla legge, e la sorveglianza doveva essere prevedibile ed accessibile, e finalizzata ad uno o più scopi legittimi previsti dall'Articolo 8(2) (sicurezza nazionale, sicurezza pubblica, stabilità economica del Paese, prevenzione della criminalità, tutela della salute o della morale, ovvero tutela dei diritti e delle libertà altrui); infine, doveva trattarsi di attività necessarie per una società democratica, il che significa, fra l'altro, che l'ingerenza nella vita privata delle persone doveva essere proporzionata.

La conservazione dei dati comporta, invece, un sistema in cui i fornitori di telecomunicazioni (Isp, società telefoniche, servizi di televisione interattiva, radio interattiva, ecc.) sono obbligati a tenere traccia di tutti i dati in transito nei rispettivi sistemi. Bene, volendo considerare questi dati alla stregua, per esempio, di quelli relativi agli acquisti effettuati con carta di credito (ed in molti casi, di fatto, ciò si verifica), la protezione accordata a queste informazioni risulta assai inferiore, ed il periodo di conservazione è molto lungo. Stiamo parlando di un periodo di cinque anni, mentre il quadro proposto a livello dell'Ue, ad esempio dal Governo belga, prevede un periodo di 1-2 anni. Le informazioni raccolte riguardano tutti i soggetti in causa. Ai sensi della Convenzione europea dei diritti umani, la sorveglianza doveva basarsi su sospetti relativi a individui specifici, sospettati di un reato o comunque, se non di avere commesso un reato, di essere implicati in circostanze poco chiare; viceversa, oggi si è creata una situazione per cui i dati raccolti dai servizi di comunicazione riguardano chiunque: donna, uomo, bambino, cane, gatto. E questi dati sono conservati.

Dunque, oggi esistono database con informazioni risalenti a vari anni fa, il che suscita un interrogativo importante: perché costituire questi database se una persona non è sospettata di nulla di preciso? La risposta che spesso si fornisce a questa domanda è che se uno non ha niente da nascondere, non ha neppure niente da temere. Ma una società democratica dovrebbe guardare alle cose secondo un'ottica esattamente inversa. Bisognerebbe chiedersi, semmai, perché siamo sorvegliati. L'ultimo governo a tentare un'attività di sorveglianza di questo tipo è stato quello della Germania Est, e sono certo che tutti abbiamo giubilato quando il Muro è stato abbattuto ed il Patto di Varsavia si è sciolto, cosicché oggi possiamo accogliere tutti (o molti) di questi Paesi nell'Unione Europea. E allora, perché queste idee ormai screditate devono essere fatte proprie dall'Unione Europea? Non è un'immagine edificante, ed il fatto che Commissione e Consiglio dell'Ue avanzino proposte del genere è veramente assai dubbio, e forse anche illegittimo alla luce della Convenzione europea dei diritti umani.

Un modello alternativo

Invece della conservazione indiscriminata dei dati, ci farebbe piacere tornare ad un modello al contempo vecchio e nuovo, ad un approccio un po' diverso – al concetto di conservazione mirata, che è poi quello adottato negli Stati Uniti. Anziché avere un database contenente informazioni su tutti e su ogni attività compiuta negli ultimi cinque anni, che è qualcosa di decisamente non democratico, è preferibile un sistema in cui persone ragionevolmente sospettate siano le sole ad essere oggetto di sorveglianza; un sistema in cui le informazioni siano raccolte per il tempo necessario, e non oltre. Se una persona risulta non essere responsabile di quanto si sospettava nei suoi confronti, allora queste attività dovrebbero cessare. Un sistema in cui la sorveglianza sia autorizzata esclusivamente dalle autorità competenti, e preferibilmente da giudici indipendenti. Un sistema, per concludere, che rispetti la privacy e non tratti le persone come dei sospettati prima ancora di avere dimostrato che esse hanno compiuto, o anche solo pensato di compiere, un atto illegale.

La risposta di Privacy International all'Unione Europea

Privacy International [un'associazione inglese per la tutela dei diritti civili, per la quale opera anche David Banisar] ha elaborato un documento in cui illustra alla Commissione Europea le ragioni che impongono di abbandonare la proposta di conservazione indiscriminata. Nel documento, Privacy International afferma che la conservazione indiscriminata delle informazioni è una scelta invasiva, illusoria in termini di benefici, illecita quanto agli scopi, ed illegittima rispetto alle procedure seguite per la conservazione stessa. Il documento è stato sottoscritto da oltre 90 organizzazioni non governative e da 80 aziende.

La sintesi del documento di Privacy International, è disponibile (in lingua inglese) al seguente indirizzo:

<http://www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.htm>

3. David Banisar⁽⁵⁾

Introduction

Typically, new threats to privacy are categorized as either being from technological developments or from government initiatives. However, a new threat has emerged that comes from a combination of the two where the law is driving technology to be more surveillance capable. This new policy, called data retention, involves governments adopting legal requirements that telecommunications providers must retain information on the activities of their users. This is being adopted in a legal environment where this information which can include political opinions, health data, financial information and other sensitive information is given less legal protections than communications using traditional telephone networks.

Convergence and technology neutrality

Disparate communications and computer technologies are rapidly converging and this combination is expanding into all areas of life. New technologies can routinely collect personal information of types never before conceived (a list of all articles read, the location of a person at all times) in ways never envisioned before (routine tracking as a default).

First, it is important to set out the differences. Twenty years ago, when all there was standard telephones, a person picked up the telephone and called somebody else on a different telephone, and all the system knew was that a particular phone in a particular house was used to dial another phone in another house for a particular period of time – nothing else was collected. The phone company generally knew who owned the phone: maybe it was a company or maybe an individual, but didn't know who actually used the phone.

Whereas today, a much greater quantity of information is being collected by communications technologies. With electronic mail you have the collection of who used a particular computer, at what time, in which location which is not necessarily a particular fixed location at any one time, to communicate with another person in respect of whom we generally know who the exact person is, what the subject of the communication was, and – obviously – what was said between the two.

With mobile phones, rather than it being a fixed telephone in a location calling another fixed telephone, generally now you have an identifiable individual calling another identifiable individual from a particular location at a particular time, for a particular duration – still no content necessarily being collected. But when you start using Sms, Mms and other technologies: and so on, you do have the collection of content communications, what is actually said.

(5) Deputy Director, Privacy International

From a legal perspective this has an interesting aspect. Usually it is presented that law should be technologically neutral, that it should not deal with information collected one way differently from how it is being treated in another way. The national laws on wiretapping and interception of communications have long set rules on how telephones are to be intercepted and what is to be done with the information. And laws such as the Eu Data Protection Directive and the Coe Convention on automated data processing have for a long time set rules on the collection and use of personal information.

However, in practice the collection of this information by computer networks has the effect of actually lowering privacy protections. In many countries, such as the Us and Uk, communications data with all of the sensitive data is being treated with the same standards as the simple telephone data was from 20 years ago, not the higher wiretapping standard.

Whereas I would argue that it should be given that level of protection, that information about what websites you are browsing, for instance, if you are visiting a website related to Aids or to drug abuse or to labour unions, or to particular journalists' websites of a particular political trend, give almost necessarily almost as much intimate information as can be found in one's medical record. And perhaps even more, because when you talk to a doctor perhaps you do censor yourself, because you don't trust what is being done with electronic medical records. But when you use the Net you don't necessarily think about the level of information that is being collected and the range of it.

This problem is being made worse by the new rules on data retention which call for the routine surveillance of users which would never be acceptable for voice communications.

Data retention, data protection and the ECHR

In past decades, when you had a telephone talking to another telephone, the standards under Article 8 defined by the European Court of Human Rights under cases such as *Klass v Germany*, *Malone v. Uk* and others, set rules that every interception of communications had to follow: it had to be in accordance with the law and the surveillance had to be foreseeable and accessible; and pursue one or more legitimate aims set out in Article 8(2) (national security, public safety, economic well being of the country, prevention of disorder or crime, protection of health or morals, or protection of the rights and freedoms of others); and finally it had to be necessary for a democratic society which includes it being proportional to the intrusion into privacy.

With data retention, we have a system where telecommunications providers—whether they be Internet service providers, phone companies, interactive television services, interactive radio: any number of different technologies, these communica-

tions providers are being required to keep track of all of the data that is passing through their systems. Now, if you want to consider that data to be the same as for instance credit card purchases, which in a lot of cases it is being treated as, it is being protected at a much lower level, and it is being kept for a very long period of time: we are talking here of five years, while the Eu framework that was proposed by the Belgian Government is proposing one to two years. It is being collected on everybody. Unlike under the Echr and surveillance, where it had to be individualised suspicion, where a person had to be a suspect in a crime, or maybe not necessarily the direct suspects, but somebody whom the police believed was up to something; whereas it is now morphed into something where it is everybody: every man, women, child, dog, cat, whatever - the information being collected by the communications service refers to; and it is being kept.

So that now you have these data bases going back years, and in this connection a significant question arises: Why are these data bases being collected, if the individual is not suspected of something? The response we often hear is: if you have nothing to hide, you have nothing to fear. But a democratic society should be looking at things the other way round. It should be asking the question: why are we being surveilled? The last government that undertook this level of surveillance was East Germany – and I am sure that we all cheered when the Wall came down and when the Warsaw Pact dissolved, and we now welcome them all, or many of those countries, into the European Union. So why are these kind of discredited ideas about how to treat a populace now being adopted by the European Union? It is not a very favourable description and, for the Eu, that the Commission and the Council should be proposing this, is really quite dubious and likely unlawful under the Echr.

A different paradigm

So, instead of data retention, we would like to go back perhaps to both an old and a new paradigm, something that looks a bit different – and that is the idea of data preservation, which is the way they do it in the United States. Where, rather than having a data base of all individuals, and every activity they have undertaken in the past five years, which is frankly undemocratic, a system where individuals who are reasonably under suspicion of doing something are the only ones placed under surveillance; where the information is collected for as long as it is necessary and not any longer. If the person is found not to be doing what he or she was suspected of, then they shouldn't do it. A system where surveillance is only authorised by legal authority, and preferably by independent judges. And, finally, a system that respects privacy, not that treats people as to be suspected before they have been proved, or even thought of doing anything wrong.

PI's Response to the EU

The following is a response by Privacy International to the European Commission to abandon the proposed retention regime. In this response, PI argues that data retention is invasive, illusory in its gains, illegal in its goals, and that the policy process surrounding retention is illegitimate. Over 90 non-governmental organizations and 80 companies have endorsed it.

The response is also archived at

<http://www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html>.

4. Guido Salerno⁽⁶⁾

Ricordo che alcuni anni or sono, quando studiavo all'Università, esercitò su di me una forte impressione il libro di Natalino Irti "L'età della decodificazione". Quel testo descriveva in maniera esauriente la frantumazione del sistema normativo, per effetto della approvazione di una miriade di leggi e leggine, che non erano in grado di inserirsi nel tessuto normativo preesistente e di armonizzarsi con i codici. L'incapacità del Parlamento di darsi un coerente indirizzo politico faceva sì che il sistema normativo perdesse le sue caratteristiche unitarie.

In senso sostanziale, la perdita dei caratteri di esaustività e di unitarietà della normazione codicistica era dovuta al fatto che le nuove leggi non rispecchiavano più l'assetto istituzionale dell'epoca delle grandi codificazioni. Dal punto di vista della tecnica normativa, si doveva registrare che ogni nuova legge fissava dei principi ed adoperava una terminologia nettamente diversi rispetto a quelli della normativa precedente, cosicché era ben difficile arrivare a stabilire poi, in sede interpretativa, quale rapporto intercorresse tra la normativa precedente e la nuova legge e quali disposizioni dovessero intendersi abrogate. In Italia, comunemente definita la culla del diritto, in molti casi la certezza del diritto diveniva quasi impossibile.

Da allora, molti progressi sono stati compiuti e si delineano ormai chiaramente le strutture portanti di un nuovo sistema normativo ed istituzionale, grazie ad una vigorosa opera di sfondamento di disposizioni normative ormai superate e grazie anche alla affermazione di una tecnica normativa che determina una maggiore semplicità del linguaggio delle leggi ed un più coerente assetto delle fonti.

Con il consolidamento del sistema delle Autorità indipendenti, il tradizionale sistema dei tre poteri statali – legislativo, esecutivo e giudiziario – ereditato dall'Ottocento, si è arricchito di un nuovo protagonista. La modernizzazione del sistema si persegue anche e soprattutto mediante l'incentivazione della concorrenza e del pluralismo, che per loro natura esigono Autorità indipendenti, che controllino dall'esterno il rispetto delle regole del mercato da parte di tutti i soggetti coinvolti, così come il monopolio pubblico di un settore economico poteva rimandare solo ad un Ministero vigilante. Oggi, in Italia, Autorità come quella per le garanzie nelle comunicazioni o quella per la privacy o quella per la concorrenza, con le sue competenze che tipicamente incidono in maniera trasversale su numerosi settori, svolgono un ruolo indispensabile e da tutti riconosciuto. Si sta finalmente procedendo a passo spedito sulla strada di un riassetto completo ed organico della normazione, ristrutturando in molti settori la normativa precedente e ponendo le premesse per una evoluzione ordinata del sistema normativo.

Lo dimostrano i numerosi testi unici e codici di quest'ultimo periodo, tra cui

(6) Presidente Fondazione Ugo Bordoni

vanno menzionati il codice delle comunicazioni elettroniche, il codice per la tutela della privacy e l'emanando codice della televisione. I nuovi testi registrano i valori fondamentali dell'ordinamento, anche quelli che l'opera di revisione costituzionale va delineando con maggiore incisività, come la tutela della concorrenza, del pluralismo, della riservatezza dei dati personali. Accanto al diritto di proprietà – che alcuni anni addietro il presidente Rodotà definì, in una sua opera, “il terribile diritto” – si delineano nuovi diritti, in concomitanza con lo sviluppo di processi sociali, che talora risultano persino difficili da definire esattamente. E proprio tale difficoltà spiega quali problemi incontri spesso il legislatore nel disciplinare i nuovi fenomeni sociali. Si pensi ad un fenomeno come Internet: sarebbe ingeneroso criticare il legislatore per non averne dato una precisa definizione giuridica, poiché è proprio Internet in quanto tale che sembra sfuggire a definizioni troppo stringenti. E d'altra parte risulta anche teoricamente affascinante operare all'interno di un sistema in continua evoluzione, se si riesce a percepire le novità, a nominarle e adeguare ad esse le istituzioni, rinunciando ad impossibili pianificazioni ultimative e ad astratte volontà classificatorie. Se Carl Schmitt fosse ancora vivo, probabilmente aggiungerebbe un altro capitolo a “Il Nomos della Terra”, scriverebbe “Il Nomos della Rete”.

L'andamento dei lavori di questo Convegno – che è stato così mirabilmente organizzato e che ha visto un così gran numero di pregevoli interventi – dimostra che l'Italia, grazie alla attività delle Autorità indipendenti, ha ormai superato un ritardo che fino a poco tempo addietro era preoccupante e si pone oggi all'avanguardia nella gestione di nuovi processi economici e sociali, che devono essere potenziati e regolati, per far fronte alle sfide della modernizzazione.



Interventi

SESSIONE III
INNOVAZIONI TECNOLOGICHE
E NUOVI DIRITTI

PRESIEDUTA DA GAETANO RASI

Sessione III – Innovazioni tecnologiche e nuovi diritti

Innovazione e progresso civile

Gaetano Rasi⁽¹⁾

Questa 3^a sessione è la conclusiva di questo Convegno su “Innovazioni tecnologiche e nuovi diritti”.

Alcune brevi riflessioni di introduzione. Le innovazioni tecnologiche costituiscono nuove ed ulteriori opportunità per l'uomo. Quindi la possibilità di esercitare nuovi diritti. Naturalmente ai nuovi diritti corrispondono nuovi doveri (“ai diritti miei corrispondono doveri degli altri e ai diritti degli altri corrispondono doveri miei”). Dunque, quando noi parliamo di nuovi diritti implicitamente prevediamo anche nuovi doveri. Ambedue nascono proprio dalle innovazioni che, incalzanti e diffuse, caratterizzano questa nostra epoca.

Ieri abbiamo sentito da tutti gli intervenuti ripetere un concetto fondamentale: *le innovazioni sono per se stesse eticamente e socialmente neutre, tuttavia debbono essere rivolte solo al miglioramento della vita di ciascuno e della società*. Ogni volta che l'uomo migliora il suo benessere e la sua cultura non può non tener presente che le nuove potenzialità sono abbinate non solo ai diritti, ma anche ai doveri.

Sappiamo dalla storia delle società umane, che le invenzioni scientifiche, la scienza applicata, le innovazioni di processo, di prodotto e di organizzazione, hanno quasi sempre rotto gli equilibri precedenti e, naturalmente, in questa rottura vi è stato un momento in cui si è perduto qualcosa che era il progresso della società fino a quel momento. Tuttavia la coscienza civile, insieme con le nuove potenzialità tecniche, ha ricomposto gli equilibri infranti ad un livello superiore. Quindi le innovazioni tecnologiche che hanno potenziato l'uomo, lo hanno però anche costretto ad essere più responsabile. Se questa responsabilità individuale e collettiva non viene espressa automaticamente, prima o poi nelle società della democrazia rappresentativa la esprimono i parlamenti con le leggi.

È questa una visione ottimistica della storia? Può essere, ma non si può negare che la problematica retrostante è ineludibile

Con il Codice entrato in vigore il primo gennaio di quest'anno sono previste norme particolarmente ampie di carattere tendenzialmente generale, perché agli

(1) Componente Garante per la protezione dei dati personali

aspetti particolari provvederà di volta in volta il Garante. Inoltre è prevista un'auto-regolamentazione, una legislazione partecipata dagli operatori e dai fornitori: i codici deontologici relativi ai vari comportamenti promossi ed elaborati da una rappresentanza significativa delle categorie interessate, insieme col Garante che ne ha poi la sorveglianza per l'applicazione *erga omnes*.

E appunto il Codice in materia di tutela dei dati personali è stato varato su una delega del Parlamento.

Un'altra riflessione per porre i termini di una problematica incombente: quella della innovazione come progresso e non come regresso, ossia innovazione per la crescita e lo sviluppo. Quest'ultimo aspetto comprende anzitutto la sicurezza. Senza sicurezza sociale, pubblica e infrastrutturale non vi è progresso. Se una innovazione diminuisce la sicurezza individuale e sociale e di conseguenza determina anche incertezza, non può ovviamente essere considerata progresso.

Parimenti, se una innovazione soddisfa in maniera più personalizzata i bisogni dell'uomo, dobbiamo considerarla un progresso, cioè una elevazione civile. Se invece una innovazione determina una menomazione di autonomia nelle scelte oppure condiziona i comportamenti, oppure consente di penetrare, senza consenso, nell'intimità delle persone oppure, ancora, menoma la identità e la dignità, allora, non c'è dubbio, ci troviamo di fronte ad un regresso civile.

Mi sembra dunque che si possa convenire su una tesi: in realtà le innovazioni tecnologiche *non sono neutre* se la loro introduzione deve tenere conto dei fondamentali valori etici e sociali dell'uomo, perché devono fare i conti con i diritti di libertà, di rispetto della dignità e della riservatezza, di tutela della personalità dell'individuo. A fronte dei diritti del progresso tecnologico vanno considerati dunque anche i doveri di chi si occupa di avanzamento della scienza e della sua applicazione. Anche per questo aspetto l'esistenza dei diritti implica l'esistenza dei doveri.

Paolo Vigeveno⁽¹⁾

Grazie Presidente, grazie al Garante per questa iniziativa perché viene a conclusione di una parte di anno che ha visto momenti molteplici d'incontro, di collaborazione, di cooperazione tra il Ministro per l'Innovazione e le Tecnologie e il Garante per la Privacy. Ed un'occasione di riflessione a questo punto dell'anno, direi che è estremamente utile ed importante.

Il tema che affronterò è l' "e-government e i diritti della personalità", uno degli argomenti più critici della nostra società in quanto non rappresenta più il semplice problema del confronto fra il cittadino e le tecnologie della rete, quanto quello del cittadino con la pubblica amministrazione presente sulla rete. Tutto ciò comporta una serie di responsabilità di funzioni da parte della pubblica amministrazione, estremamente delicata, poiché lo scenario che si sta disegnando rappresenta l'insieme dei livelli di sicurezza per i cittadini e quindi dei gradi di libertà e di opportunità per le generazioni del futuro. Un aspetto particolarmente importante è quello della funzione che la pubblica amministrazione può avere in questo senso anche nei confronti del settore privato, come termine di paragone e di competizione. Quando parliamo di e-government intendiamo fornire una possibilità di accesso sostanzialmente illimitato ai cittadini. A questo accesso corrisponde da parte della pubblica amministrazione una automazione e una integrazione di processi burocratici in cui però non è più il cittadino che si integra come avviene nel mondo reale tra le diverse funzioni della pubblica amministrazione spostandosi da uno sportello all'altro; è la pubblica amministrazione che si presenta come un unico soggetto attraverso un'unica porta di accesso. È questo in sostanza il vantaggio e il beneficio per il cittadino al quale la pubblica amministrazione deve adeguarsi con una serie di operazioni e funzioni che sono quelle su cui intendiamo puntare la nostra attenzione.

L'effetto che dovrebbe scaturire da questo nuovo modo di intendere il rapporto cittadini-P.A. è quello di avvicinare l'utente finale alle istituzioni, alle loro funzioni di servizio; il che implica sia una maggiore efficienza della macchina statale sia una maggiore efficacia nei confronti dei cittadini e delle imprese. Si tratta cioè di una vera e propria rivoluzione copernicana nel rapporto tra il cittadino e le istituzioni. Nel modello tradizionale è il cittadino che si rivolge alle istituzioni, che fornisce le informazioni all'istituzione. Nell'e-government il rapporto s'inverte: le informazioni sono contenute nel sistema e il cittadino non è tenuto a fornire più di una volta dette informazioni. L'e-government opera attraverso una serie di operazio-

(1) Capo segreteria tecnica – Ministero per l'Innovazione e le Tecnologie

ni complesse, invisibili al cittadino, riuscendo tuttavia a garantire la riservatezza dei dati. Per rendere operativo questo sistema, quindi, occorre di fatto realizzare un progetto che trasformi gli elementi che definiscono la personalità dei cittadini mediante l'uso di tecnologie informatiche e di comunicazione, creare cioè una vera e propria identità elettronica.

L'identità elettronica ha creato inevitabilmente problemi di privacy in considerazione degli innumerevoli dati, principalmente di carattere personale, che devono essere comunicati per poter essere inseriti in database. Al riguardo, l'Autorità per la privacy, nell'esercizio della funzione consultiva di cui è titolare, ha più volte segnalato, negli anni precedenti, la necessità di individuare con maggiore attenzione e proporzionalità la tipologia dei dati da inserire nei documenti elettronici, i soggetti che possono eventualmente accedere alle varie categorie di dati e le garanzie per gli interessati, con particolare attenzione per le informazioni più delicate, quali i dati sanitari o biometrici.

Comportamenti lesivi nei confronti dei cittadini e dei soggetti che forniscono dati si verificano oramai frequentemente, basta pensare ai reati maggiormente diffusi: spamming, furti d'identità, ecc. In merito cito solo alcuni dati del mercato americano rilevati dalla Federal Trade Commission: 9,9 milioni di vittime, circa il 4,6% della popolazione adulta, per furto di personalità, tra furti di carte di credito, utilizzo improprio di conti correnti altrui, apertura di nuovi conti bancari.

Sono tutti fatti che, oltre a ledere i diritti dei cittadini, ostacolano la diffusione e l'uso della rete, alimentando la diffidenza degli utenti nei confronti delle nuove tecnologie.

La risposta che abbiamo dato noi (ne parleremo più approfonditamente in seguito) è quella di far sì che il cittadino sia identificabile in rete, evitando in questo modo il furto d'identità. Una delle innovazioni più importanti introdotte dal governo è quella della carta nazionale dei servizi, strumento di riconoscimento e di identificazione in rete.

Rispetto ai rischi connessi ad un ambiente non sicuro, rispetto a questo tipo di aggressione derivata da una mancanza di regole o di strumenti in grado di arginare le violazioni dei diritti della persona, l'e-government, in quanto presenza delle istituzioni nella rete può e deve assumere un ruolo di riferimento fondamentale per la salvaguardia dei diritti della personalità nel nuovo contesto informatico. I servizi di e-government possono funzionare da modello per altri servizi nel settore privato, generando quindi una concorrenza virtuosa nel campo della fiducia da parte dei cittadini.

I servizi di e-government, quindi, devono fornire garanzie intrinseche di difesa dei diritti della personalità e allo stesso tempo servire da riferimento per il settore privato. Esempio, lo dicevo prima, quello della carta nazionale di servizi è un'iniziativa senz'altro più innovativa ed efficace. Adesso è stata presentata a Bologna, di

recente, una serie di servizi di e-government che offrono la possibilità di effettuare transazioni bancarie effettuate con la Cns, seppur limitate ai pagamenti nei confronti della pubblica amministrazione. Il grado di sicurezza raggiunto è estremamente significativo.

Dalla progettazione e dalla determinazione del livello di sicurezza si misura la capacità sia dell'imprenditore privato, sia del politico, nel senso che in entrambi i casi occorre avere la capacità di bilanciare e di valutare il grado di rischio tollerabile a fronte dei costi da sostenere, in funzione dell'obiettivo da conseguire. Se l'operatore privato deve conseguire un fine di lucro, deve riuscire ad equilibrare questi due elementi. Altro è l'obiettivo dell'operatore pubblico, il cui scopo precipuo è quello di tutelare i diritti delle persone ed ottenere consenso, adesione e cooperazione da parte dei cittadini.

È indispensabile, a tal fine, un'opera di formazione diffusa che crei una cultura informatica adeguata, in grado, cioè, sia di far comprendere l'utilità e l'importanza che oramai la tecnologia ha assunto nel terzo millennio, sia di istruire gli utenti alla conoscenza del mezzo; oggi usare un computer è rischioso, per certi aspetti, quasi quanto guidare un'automobile ed il rischi non investe solo i minori ma anche gli adulti. Il processo tecnologico di cambiamento è diventato così radicato da diventare irreversibile. È quindi inutile porre divieti a bambini, meglio insegnare loro ad utilizzare correttamente i mezzi tecnologici. Altrettanto vale per gli adulti: occorre conoscere lo strumento per adoperarlo al meglio e soprattutto, come afferma anche l'Ocse, creare una vera e propria cultura della sicurezza informatica.

In questo senso si sta muovendo anche il governo, cito un'iniziativa per tutte, quella del centro dell'informazione per la sicurezza (Icd) nella Pubblica Amministrazione. Vanno attivati inoltre tutti gli strumenti normativi per i diversi ambiti di applicazione, quali il codice per la tutela dei dati personali, la firma digitale, la carta nazionale dei servizi, la posta certificata, il protocollo informatico. Sono tutte soluzioni normative che hanno l'obiettivo di assicurare una funzionalità dei servizi in un ambiente sicuro.

Bisogna poi adottare delle adeguate scelte tecnologiche. A tal fine si sono create una serie di Comitati (interministeriali) di lavoro, sulla larga banda, sul digitale terrestre, sulle biometrie; si sono creati Comitati di garanzia, come quello per Internet e minori.

Tutte queste iniziative vedono coinvolte sia le altre amministrazioni, sia i rappresentanti della cosiddetta società civile.

Un problema però esiste. Se si vogliono rendere fruibili al maggior numero di persone i servizi della pubblica amministrazione attraverso l'e-government, raggiungendo il massimo livello di fruibilità del servizio, necessariamente ci si deve confrontare con il problema di Internet. Si devono, quindi, affrontare tutti i proble-

mi connessi alla sicurezza su Internet, capire quali sono le vie praticabili.

Esse sono sostanzialmente tre: la prima è di intervenire sulla Governance di Internet, che comporta un confronto con un ambiente nuovo, virtuale, ma soprattutto con il problema della giurisdizione nazionale, ancora inadeguata, non sufficientemente matura. Occorrono, pertanto, norme di diritto di carattere transnazionale che siano efficaci; tale processo, va seguito attentamente, e lo stiamo facendo, perché richiede tempi estremamente lunghi e operazioni particolarmente complesse.

La seconda via è quella di realizzare reti sicure parallele a quelle di Internet come il sistema bancario; tuttavia è evidente che questo limita il numero di accessi a Internet possibili.

La terza strada è quella di creare su Internet un ambiente sicuro, tramite il sistema pubblico di connettività (Spc).

La possibilità di sviluppare servizi fra le diverse pubbliche amministrazioni permette di ottenere maggior efficienza nei procedimenti interamministrativi e di raggiungere l'obiettivo di presentare le diverse pubbliche amministrazioni al cittadino e all'impresa, in modo unitario. In tale ottica questo strumento potrà permettere un'erogazione di servizi secondo modalità diverse di integrazione, che realizzano una maggiore sinergia, utilizzando diversi strumenti di accesso tra i quali i Portali nazionali e locali della Pubblica Amministrazione.

Obiettivi primari del Spc sono quelli di fornire un insieme di servizi di connettività condivisi dagli Enti interconnessi, definiti negli aspetti di omogeneità, qualità e sicurezza, ampiamente graduabili in maniera tale da poter essere ritagliati al meglio sulle esigenze delle diverse amministrazioni, di garantire l'interazione della pubblica amministrazione centrale e locale con tutti gli altri soggetti connessi ad Internet, nonché con le reti di altri Enti che debbano interagire con la Pa. Realizzare insomma una rete che abbia la pervasività e la raggiungibilità tipica di Internet ma che fornisca garanzie di qualità e sicurezza che la rete pubblica non può offrire.

Per ottenere questo obiettivo il sistema pubblico di connettività (Spc), sarà gestito dagli stessi operatori che gestiscono la rete, cioè gli Internet Service Provider, tenuti però a rispettare regole e standard di qualità e sicurezza definiti nel progetto. Nella fase iniziale non sarà possibile accedere al sistema pubblico di connettività da parte diretta dei cittadini perché ovviamente questo comporterebbe un abbassamento del livello di sicurezza. Quindi la prima fase interesserà solo la pubblica amministrazione. In una fase successiva, verranno gradualmente coinvolti anche cittadini o soggetti che offriranno adeguate garanzie di sicurezza perché utilizzano sistemi di riconoscimento in rete come la carta nazionale di servizi o la carta d'identità elettronica. Il percorso adottato ha permesso di seguire un plafond comune di misure di sicurezza che assicurerà a tutti i partecipanti al sistema pubblico di connettività adeguate garanzie di protezione alle informazioni scambiate. C'è anche un sistema di

organizzazione che assicura una corretta gestione e un livello di sicurezza nei confronti di attacchi esterni attraverso la utilizzazione di Cert, centri di pronto intervento contro hackers o simili.

Ma uno degli aspetti più importanti, direi, come acquisizione e livello di sicurezza istituzionale che deve essere garantito è quello della cooperazione applicativa. Si tratta di una metodologia importante perché basata sul principio di conservazione della responsabilità di gestione dei dati in capo alle amministrazioni detentrici, anche quando questi dati devono essere comunicati ai fruitori, ai cittadini o alle imprese. Ad esempio, se devo accedere ai miei dati sanitari e fiscali, devo potere accedere con un'unica transazione, con un unico accesso; manca a tutt'oggi l'interoperabilità tra le varie amministrazioni: i progetti di e-government, attualmente in corso, realizzati con il bando dello scorso anno, si riferiscono soltanto a singole amministrazioni. Si vengono a creare in questo modo delle amministrazioni-guida, responsabili dei cosiddetti "domini di cooperazione", per i quali vengono definite politiche di sicurezza dove potranno essere utilizzate, nel rispetto di standard definiti, misure tecnologiche adeguate per il tipo di dominio che verrà creato.

Ciascuna amministrazione aderente sarà responsabile per i propri sistemi che contengono dati, sarà autonoma nella gestione dei propri sistemi, nella definizione ed attuazione delle politiche di sicurezza del proprio sistema informativo. Inoltre l'autorizzazione all'erogazione del servizio di cooperazione sarà di responsabilità di ciascuna amministrazione e le eventuali informazioni necessarie per concedere l'autorizzazione saranno costituite dalle sole organizzazioni istituzionalmente preposte a questo. Quindi viene mantenuto anche nell'e-government il principio di responsabilità dell'amministrazione rispetto ai dati che detiene. Il modello di cooperazione quindi definisce anche le modalità di scambio tra i diversi sistemi secondo il principio di trasmettere la minor quantità d'informazione relative, come peraltro prescritto dal codice per la privacy. In molti casi l'unico dato che viene trasmesso è il codice fiscale; e quindi viene lasciata a ciascuna singola amministrazione la responsabilità dei dati trattati. Questo è un modo per facilitare la tutela dei diritti della personalità. Vediamo che sono proprio le tecnologie stesse che possono fornire soluzioni ai problemi che le tecnologie pongono; e con gli attuali strumenti informatici è possibile ottenere un'efficienza maggiore delle transazioni on line mantenendo le informazioni relative alla personalità in poche banche dati opportunamente protette, e comunque separate tra di loro.

La cooperazione applicativa non prevede affatto la creazione di banche dati centrali; le informazioni anagrafiche restano di competenza dei Comuni e quello che viene scambiato è soltanto l'indice e non i contenuti delle informazioni. La separazione dei processi è una delle regole principali di sicurezza perché evita che uno stesso soggetto possa agire indebitamente all'interno dell'intero processo. Ricordo

comunque che la infrastruttura base della garanzia della sicurezza è proprio lo strumento di identificazione in rete che abbiamo creato. La carta d'identità elettronica è stata inserita nella carta nazionale dei servizi che peraltro assicura un adeguato livello di sicurezza. Per concludere voglio solo ricordare che quando ci si inoltra in territori come questi, del tutto nuovi, occorre da una parte un gran senso di responsabilità e di consapevolezza da parte della pubblica amministrazione per il ruolo che sta svolgendo in termini di novità e di riflessi che questi comportamenti possono determinare in futuro e sul futuro delle prossime generazioni e d'altra parte far sì che i cardini delle amministrazioni operino al massimo livello di capacità e di qualità. Questo si può realizzare soltanto attraverso una strettissima cooperazione tra le diverse competenze della pubblica amministrazione, con la consapevolezza che il miglior assetto di lavoro è quello che dà, che può dare, il miglior livello di garanzia per il conseguimento della tutela, della sicurezza e della personalità dei cittadini sulla rete, attraverso i servizi di e-government. Ci siamo trovati, e concludo, grazie allo sviluppo delle tecnologie e del loro uso, ad un'inversione di marcia che comporta una serie di responsabilità e di potenzialità e che rappresenta una sfida che intendiamo continuare a perseguire al massimo delle nostre capacità pur nella consapevolezza della difficoltà degli obiettivi da raggiungere.

E-government e diritti della personalità



Paolo Vigevano ⁽¹⁾

(1) Ministero per l'Innovazione e le Tecnologie

I benefici dell'e-government



- Informazioni "senza confini"



- piena partecipazione dei cittadini alla vita democratica

- Automazione ed integrazione dei processi burocratici



- accorciamento delle distanze tra cittadini ed istituzioni
- maggiore efficienza della macchina statale
- benefici economici e sociali per cittadini ed imprese

La trasformazione del modello di interazione



- **Modello tradizionale**
 - le informazioni sono detenute dal soggetto che interagisce con le istituzioni
 - il soggetto deve farsi carico di fornire le informazioni agli enti che partecipano al processo
- **Modello di e-government**
 - le informazioni sono detenute dal sistema di e-government (l'utente non deve avere l'onere di comunicare ogni volta informazioni che lo stato già conosce)
 - il soggetto effettua un'unica interazione con il sistema che maschera la complessità interna e realizza in modo automatico gli scambi informativi necessari per erogare il servizio

La personalità virtuale



- **L'attuazione del modello di e-government comporta la progressiva astrazione degli elementi che definiscono la personalità:**
 - identità → sistema di autenticazione
 - dati personali → banche dati
 - comportamenti → transazioni informatiche
 - atti → documenti elettronici
- **I sistemi di e-government trattano immagini virtuali delle personalità dei soggetti**

I rischi per lo sviluppo dell'e-government



- Le informazioni acquisite o elaborate dai sistemi informatizzati possono essere raccolte, memorizzate, analizzate, relazionate ed utilizzate in diversi modi, in posti geograficamente dispersi, senza che i soggetti interessati ne siano consci
- Lo sviluppo dell'e-government è accompagnato dal sorgere di nuovi problemi che ledono i diritti della personalità
 - furto d'identità
 - spamming
 - prodotti di pubblicità indesiderati (adware)
- Dopo una fase di entusiasmo per le nuove tecnologie, si rischia di assistere ad un fenomeno di "rigetto" per l'assenza di garanzie nella navigazione in Rete

Incidenza del furto d'identità (fonte

Federal trade commission¹⁾



Source: Identity Theft Survey Report, conducted by Innovate for the FTC (March-April 2007).
Based on the U.S. population age 18 and over (115.47 million as of July 1, 2007) (Source: Population Division, U.S. Census Bureau, Table NC-100-000A001-01).

Le prospettive dell'e-government



- Le istituzioni possono assumere un ruolo fondamentale per la salvaguardia dei diritti della personalità nel nuovo contesto informatico
- Occorre che, al pari del mondo reale, nella Rete esistano riferimenti certi rispetto a cui i soggetti possano orientarsi: le istituzioni hanno la possibilità ed il dovere di costruire questi riferimenti
- I modelli dei servizi di e-government possono diventare il riferimento per altri servizi "fidati" caratterizzati da garanzie di tutela dei diritti individuali

Le leve per lo sviluppo dei servizi di e-government



- Coscienza collettiva e nuova cultura informatica
 - formazione
 - campagne promozionali
 - coinvolgimento delle scuole
- Comportamento corretto di tutti gli attori coinvolti
 - normativa di settore
 - codici di autoregolamentazione
 - comitati di garanzia
- Scelte tecnologiche adeguate

E-government = Internet ?



- Internet è il mezzo naturale per promuovere lo sviluppo dell'e-government
 - raggiunge un numero elevatissimo di soggetti
 - ha costi ridotti
 - è di semplice utilizzo
- In una fase matura, probabilmente i sistemi di e-government saranno isolati rispetto ad Internet
- L'isolamento può attuarsi con diverse soluzioni tecniche ed organizzative
 - utilizzando media diversi
 - con isolamento logico rispetto alla rete Internet

Il Sistema Pubblico di Connettività



- E' l'infrastruttura comunicativa che supporterà i servizi di e-government
- Sfrutta le risorse e gli standard di Internet, ma costituisce un sistema logicamente isolato
- E' stato progettato per consentire lo scambio informativo sia tra le amministrazioni, sia tra queste e soggetti terzi (cittadini ed imprese) dotati di sufficienti credenziali
- Le regole base di sicurezza garantiscono la riservatezza delle informazioni scambiate
- E' protetto nei confronti di accessi indebiti da Internet con opportune contromisure passive ed attive (CERT)

Le regole per la cooperazione applicativa



- E' attivo un gruppo di lavoro per il perfezionamento delle regole con cui le amministrazioni realizzeranno i servizi di e-government
- Il modello definito si basa sulla cooperazione di amministrazioni che sono autonome nella gestione delle informazioni di competenza
- I servizi sono realizzati nell'ambito di aggregazioni tra amministrazioni istituzionalmente preposte al trattamento delle informazioni (domini di cooperazione)
- Ciascun dominio è autonomo nelle scelte di carattere tecnico ed organizzativo, ma deve rispettare regole comuni che garantiscono la tutela delle informazioni trattate

I criteri per lo sviluppo dei servizi di e-government



- Le informazioni inerenti i soggetti destinatari dei servizi sono custodite esclusivamente dalle organizzazioni istituzionalmente competenti
- Le funzioni utente forniscono al sistema il minimo insieme di informazioni necessario per dimostrare la titolarità ad usufruire del servizio, per fare ciò si basano sugli strumenti di autenticazione nazionali (Carta d'Identità Elettronica, Carta Nazionale dei Servizi)
- Le eventuali informazioni aggiuntive necessarie per l'autorizzazione (ruolo, funzione, ecc.) sono ottenute mediante accessi "sicuri" verso gli enti competenti
- Ciascun ente mantiene traccia delle sole operazioni di propria competenza

Tecnologia informatica e diritti della personalità



- Con gli attuali strumenti informatici è possibile ottenere l'efficienza delle transazioni "in linea" mantenendo le informazioni relative alla personalità in poche banche dati opportunamente protette
- Il modello italiano di e-government asseconda l'organizzazione decentrata della pubblica amministrazione ed evita l'accentramento – o la facile correlazione – dei dati inerenti la personalità
- I servizi di e-government corrispondono a processi cooperanti che accedono con regole condivise a domini protetti ed autonomi
- Le carte per l'accesso ai servizi in rete sono lo strumento nazionale per l'utilizzo sicuro dei servizi di e-government

Roberto Galimberti⁽¹⁾

Parlerò su che cosa s'intende per innovazione sostenibile, poi su alcuni temi relativi al ruolo della tecnologia e infine dell'impatto che il testo unico della privacy ha sull'industria.

In questa prima slide mostro l'innovazione come fattore che guida la crescita. Oggi i problemi che s'incontrano a livello industriale sono stati molto bene illustrati dal nostro presidente Luca Cordero di Montezemolo nella sua conferenza di insediamento in Confindustria, ove la parola innovazione è stata più volte ripetuta. È il fattore innovazione che guida la crescita, soprattutto in un momento così difficile si deve proprio cercare di cambiare qualche cosa (prodotto/processo/catena del valore...) per poter crescere.

Nella slide successiva ho sintetizzato le caratteristiche di un imprenditore: passione per la risoluzione dei problemi, forte capacità di trasformare le idee in realtà, propensione al rischio. Un imprenditore riesce a esprimersi soprattutto in fase di crescita, ma è in fase di compressione (momento molto, molto delicato e difficile) che deve sforzarsi per dare il meglio di sé stesso: e questo è proprio il caso attuale. Le aziende orientate all'innovazione, sono aziende che creano e reinventano nuovi mercati, nuovi prodotti/servizi, e soprattutto nuovi modelli di business che ampliano la catena del valore.

Un punto voglio sottolineare, l'ultimo: i nuovi modelli di business che ampliano la catena del valore. Questo è un problema che oggi l'industria italiana si trova ad affrontare in maniera pesantissima. Il contenuto di lavoro nella fase di produzione del prodotto è in forte calo, stiamo andando verso una società, lasciatemi dire, di produzione di servizi. Il problema è quello di ampliare la catena del valore nella singola impresa in maniera tale da poter sopperire al calo di necessità di forza lavoro per la produzione dei prodotti con un adeguato incremento per la parte di generazione dei servizi. Questo è un grosso problema, anche di portata politica, per un fatto: i servizi sono locali, sono nazionali: è estremamente difficile esportare dei servizi. Questo è uno dei motivi per cui la nostra industria sta perdendo quote di mercato sull'esportazione: ce ne sono altri, ma indubbiamente questo è uno dei più importanti, soprattutto nel settore che stiamo trattando qui, quello dell'Ict.

Vediamo ora la nuova slide: cosa vuol dire innovazione sostenibile. Innovazione sostenibile vuol dire sostanzialmente centrare a livello di top management una guida e una strategia verso l'innovazione. Innovazione vuol dire continuamente am-

(1) Presidente di Etnoteam, E.TREE e I.NET

piare la propria gamma di prodotti/servizi e dei mercati; vuol dire saper utilizzare la tecnologia come strumento a sostegno dell'innovazione. Diverse società italiane hanno dato un grandissimo contributo allo sviluppo della tecnologia nel settore dell'Ict; oggi purtroppo di significative ne rimane una: la Stm di cui Pasquale Pistorio è presidente.

Nella prossima slide mostro che oggi l'industria italiana è più orientata verso l'utilizzo delle tecnologie piuttosto che lo sviluppo delle tecnologie di base. Usare una tecnologia è una cosa che può essere fatta in diversi modi: la nostra situazione attuale è quella di utilizzare tecnologie già stabili. Per la situazione in cui noi ci troviamo, parlo sempre dell'Ict, le grandi tecnologie, che sono queste che ho elencato qui, sono già chiare. Sono state sviluppate, parte in Europa, parte fuori dall'Europa e sostanzialmente sono due: l'Internet Protocol ed il web. Queste sono le due tecnologie vincenti che hanno caratterizzato gli ultimi dieci anni e che come vedrete nelle slides successive, caratterizzeranno i prossimi anni dello sviluppo di questo settore. L'Internet Protocol è una tecnologia che è nata più di 30 anni fa, ormai è stabile, ormai è in mano ai grandi operatori. Abbiamo sentito prima Vigeveno che è stato uno dei primi a introdurre Internet in Italia, allora era una tecnologia innovativa, come sempre gestita da piccole imprese. Oggi l'Internet Protocol è l'unico modo con il quale le grandi società di telecomunicazioni stanno costruendo le loro reti.

Poi c'è il web. Il web è un'altra tecnologia nata in Europa, sviluppata negli Stati Uniti che ha solo 10 anni. È giovane, anzi giovanissima. Ancora oggi è difficile utilizzare in maniera industriale commercialmente valida il wweb. Non è una cosa che deve preoccupare perché è già successo a tante altre tecnologie, pensate alla radio che ha impiegato parecchi anni per diventare l'unica tecnologia di successo per il broadcasting.

Con questo ho accennato, brevemente agli effetti che le tecnologie porteranno nelle innovazioni. L'effetto che queste tecnologie così pervasive provocheranno sulla nostra industria deve essere chiaro se si vuole impostare un concetto di innovazione.

Due parole sul nuovo testo unico sulla privacy.

Una grossa benvenuta opportunità per tutti e in particolare per l'industria italiana; molto simile a quello che è successo con la qualità l'Iso 9000 circa 25 anni fa: anche allora all'inizio si sono avute reazioni tiepide, se non addirittura negative, poi abbiamo capito e abbiamo trasformato un apparente vincolo in una buona opportunità.

Oggi le aziende vivono sempre più di informazioni. Proteggere le informazioni, vuol dire difendere l'impresa. E le informazioni serie vanno trattate seriamente.

Queste cose prima del 28 settembre 2003 non si dicevano così chiaramente. Il 28 settembre 2003 è caduto un alberello in Svizzera e c'è stato in Italia un black-out

anche di qualche ora. Allora tutti noi ci siamo repentinamente accorti di quanto sia vitale la Business Continuity e di conseguenza la necessità di avere dei Data Recovery Centre molto affidabili.

Nella nuova slide vi illustro i nuovi obblighi che il nuovo codice impone.

In estrema sintesi:

- cifratura dei dati sensibili
- sistemi antivirus
- autenticazione
- controlli perimetrali
- backup e restore
- un documento (Dos) con l'analisi dei rischi
- misure organizzative
-

Le reazioni davanti a tutti questi impegni possono essere due:

1° atteggiamento

§ Lo faccio perché me lo impone la legge

§ Lo faccio ma non ci credo

§ DEVO quindi Sicurezza = seccatura

2° atteggiamento

§ abilita il mio business

§ da adempimento a disciplina

§ VOGLIO quindi Sicurezza = vantaggio competitivo

La sicurezza deve diventare un vantaggio competitivo.

E c'è un fatto molto importante: in generale, il danno non è molto rilevante da un punto di vista economico. È molto più rilevante da un punto di vista psicologico.

Imporre la sicurezza è un fenomeno che serve soprattutto per dare sicurezza.

Oggi cominciano ad esserci delle assicurazioni abbastanza ben organizzate per parare il danno economico dovuto ad un attacco alla sicurezza.

E qui per sicurezza intendo la sostenibilità di tutto il sistema informativo.

Il problema fondamentale è quello che la sicurezza è un fenomeno che altera notevolmente la tranquillità del cliente e di chi fa business.

Infine è molto importante impostare una politica di sicurezza partendo dal concetto: quanto sono debole.

Infatti nessuno sta bene: tutti stanno male. Si tratta di capire quanto sto male, e di pensare a come migliorare.

E questa è una politica ormai, lasciatemi dire, possibile, non difficile: basta volerlo.



Il ruolo dell'impresa per una innovazione sostenibile

18 Giugno 2004

Roberto Galimberti

Presidente di Etnoteam, E.TREE e I.NET

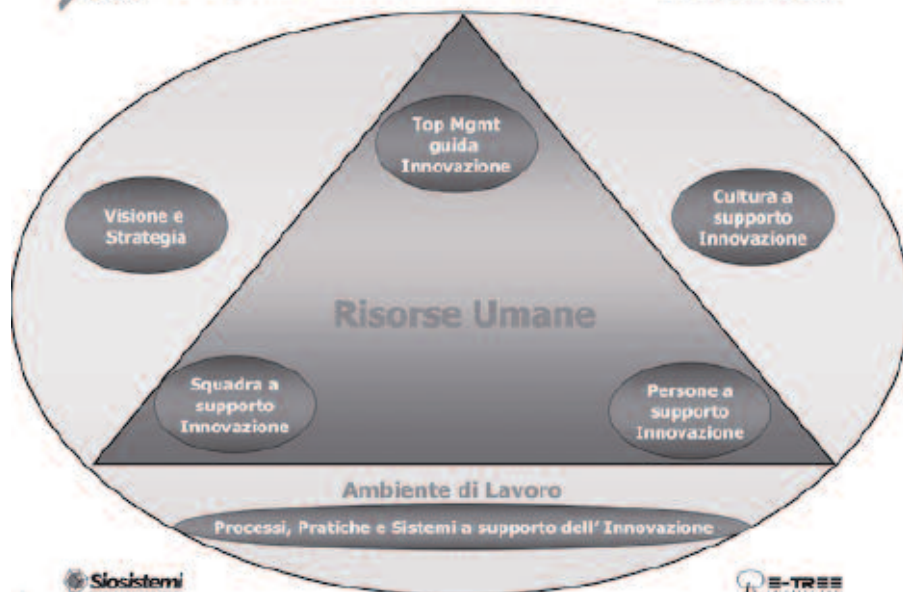
- L'innovazione sostenibile
- Il ruolo della tecnologia
- Il nuovo Testo Unico sulla Privacy

Innovazione : la chiave per il Successo

- L'innovazione è il fattore che guida la crescita
- L'innovazione viene costruita da persone che hanno
 - **passione** per la risoluzione dei problemi
 - una forte capacità di **trasformare le idee in realtà**
 - propensione al **rischio**

Innovazione : la chiave per il Successo

- Le aziende orientate all' innovazione creano e reinventano continuamente
 - nuovi mercati
 - nuovi prodotti/servizi
 - modelli di business che ampliano la catena del valore
- La cosa migliore per garantire la crescita è la costruzione di una organizzazione orientata alla **"innovazione sostenibile"**.

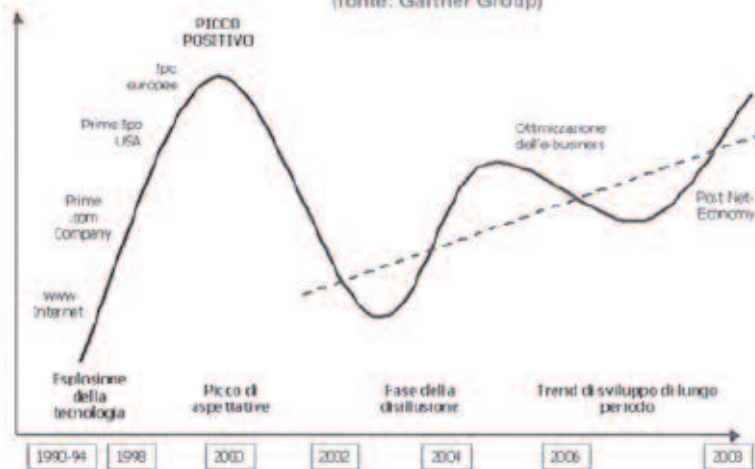


- Le risorse umane di qualità sono al centro del processo di innovazione
 - Passione per l'innovazione
 - Cultura dell'innovazione
 - Formazione continua
 - Condivisione delle conoscenze
 - Volontà di creare una squadra

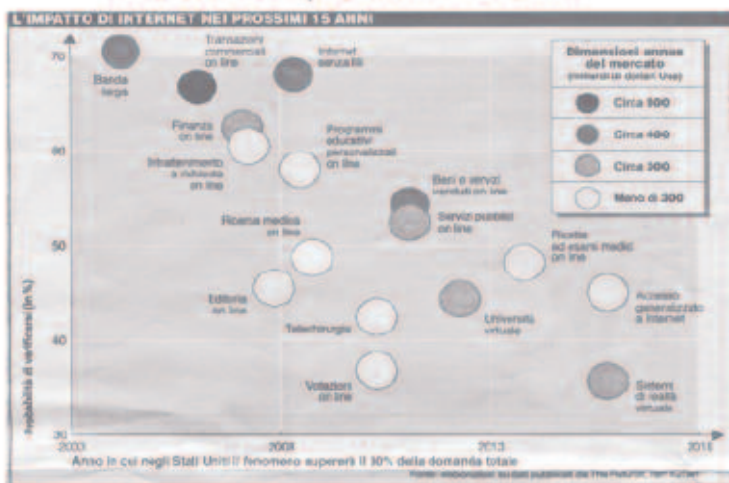
- Il ruolo della tecnologia come strumento effettivo a sostegno dell'innovazione
- Quali tecnologie
 - Internet Protocol
 - WEB
 - Wireless Lan/Wan/Man
 - Grid Computing
 - Radio Frequency Identification
 - ...

La curva della disillusione

(fonte: Gartner Group)



Internet nei prossimi 15 anni



Il nuovo Testo Unico sulla Privacy

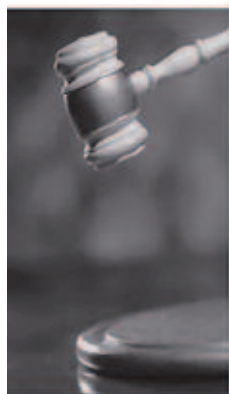
Una grossa benvenuta opportunità

Il valore per l'azienda



- Le aziende vivono di informazioni
- Proteggere le informazioni vuol dire proteggere l'impresa
- L'informazione seria va trattata seriamente

Nuovi obblighi



- Il codice **IMPONE**
 - cifratura dei dati sensibili
 - sistemi antivirus
 - autenticazione
 - controlli perimetrali
 - backup e restore
 - un documento (DPS) con l'analisi dei rischi
 - misure minime e organizzative
 -

Subire o agire?



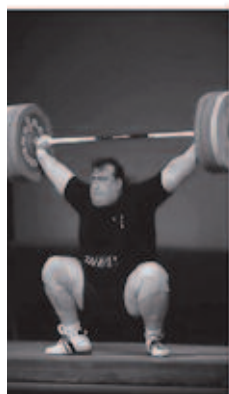
- Lo faccio perché me lo impone la legge
- Lo faccio ma non ci credo
- **DEVO**
 - Sicurezza = seccatura
- abilita il mio business
- da adempimento a disciplina
- **VOGLIO**
 - Sicurezza = vantaggio competitivo

Auditing



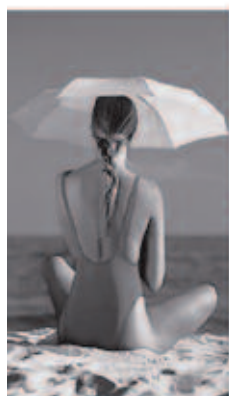
- **QUANTO
SONO
DEBOLE?**

Rafforzamento



■ COME POSSO ESSERE PIU' FORTE?

Competenza



- L'ombrello che ripara dalle scottature
- La necessità di usare al meglio le funzioni dei prodotti migliori
- La garanzia di efficacia nei progetti in outsourcing
- La sicurezza nella traduzione delle policies aziendali nelle implementazioni sul campo

Quindi.....



- Sicurezza non per paura
- Sicurezza per non perdere
- **SICUREZZA PER DARE SICUREZZA**

Giovanni Buttarelli⁽¹⁾

Vorrei partire da una confidenza. Nei giorni antecedenti questo evento, un mio amico, nostro interlocutore istituzionale, ha declinato l'invito a venire qui, oggi; ironizzando, ma non tanto, mi ha detto che da interlocutore istituzionale è divenuto un "oppositore istituzionale" perché dopo una serie di nostri interventi e di asseriti protagonismi della autorità, saremmo divenuti insopportabilmente invasivi per cui, fermo restando l'apprezzamento personale per i suoi rappresentanti, sarebbe giunto il momento di introdurre una "distanza istituzionale" con questa autorità.

Questo episodio mi induce a porvi il quesito, anche in questo caso ironicamente, se siano più invasive le nuove tecnologie o invece la legge che le insegue o le autorità che la fanno applicare. È un interrogativo che si somma a quello che ieri Danilo Bruschi poneva a tutti noi quando si chiedeva se l'imposizione di regole, almeno per quanto riguarda la sicurezza, rallentasse o meno il processo di apprendimento degli utenti. Bruschi ci diceva il *bit* non va trattato come l'atomo. Anche su questo ho riflettuto e a me sembra che sia abbastanza certo a tutti che il diritto si occupa, molto, di moneta elettronica, di commercio elettronico, di vendite *on-line*, della validità giuridica dei documenti informatici, della firma elettronica, della firma digitale. Perché fa tutto questo? Non per snobismo normativo, ma per l'esigenza ineliminabile di assicurare certezza ai rapporti giuridici che intercorrono con la pubblica amministrazione e con le imprese.

Ora, come è possibile ipotizzare che si lascino questi aspetti che ora ho citato agli equilibri che possono nascere, diciamo di fatto, nell'ambito dei rapporti intersoggettivi. E allora, se noi interveniamo con norme molto dettagliate (non parliamo poi della tutela del diritto d'autore) per non pregiudicare l'attività contrattuale, per dare certezze agli operatori o per assicurare efficienza e sviluppo dell'impresa, perché mai dovremmo affidare soltanto all'autodisciplina, non sanzionata, un quadro di garanzie che invece riguarda quella che dovrebbe essere al centro di tutta la nuova area delle nuove tecnologie, cioè la persona, la sua sfera privata, la sua intimità, la persona con il suo diritto, diciamo, di essere sé stessa anche in differenti modi, con differenti persone.

Dico questo, perché da questi due giorni mi sembra emersa la conferma (se ve ne era bisogno), che diversamente da quanto noi pensiamo normalmente, la tecnologia ha già clonato il corpo umano. L'individuo è frammentato, lo abbiamo visto ieri da molti esempi, nella sua identità. Siamo divisi in mille rivoli, in mille

(1) Segretario Generale Autorità Garante per la protezione dei dati personali

data base. Abbiamo perso la nostra unitarietà. Migliaia, e milioni di flussi di dati, diventano la vera cifra di una persona. E questa cifra, purtroppo, non è sempre corrispondente con la realtà, con la nostra effettiva identità personale.

Pensiamo ad esempio al rapporto che c'è tra il diritto all'oblio, che il Codice citato da Galimberti assicura e il problema che pongono, invece, i motori di ricerca che implacabilmente, anche se il cittadino ha ottenuto giustizia rispetto ad una pubblicazione diffamatoria, ad un qualche cosa che dovrebbe essere oggetto di perdono dello Stato per una sanzione disciplinare, permettono per anni di reperire documenti attraverso i motori di ricerca, negli innumerevoli siti web nei quali all'epoca la notizia è stata pubblicata.

L'epoca dell'informazione totale mette in discussione la nozione giuridica di persona. Siamo dei nomadi, ci hanno detto ieri, in costante movimento, e diviene assolutamente difficile, se non impossibile, che oggi e ancor più nel domani si possa vivere *wireless*. I dati personali non sono più, quello che si diceva negli anni '70 e '80, solo una merce preziosa. Appare chiaro che essi sono ora la proiezione del nostro corpo, sono il nostro corpo virtuale. Quindi un pc invasivo non è più una secatura, ma è un'arma puntata contro la nostra persona.

Ecco, noi ieri abbiamo assistito a molte relazioni interessanti. Però, non è forse emersa a sufficienza una novità, che non è soltanto italiana, ed è una novità degli ultimi mesi: il diritto alla protezione dei dati personali. Un diritto che questo Codice ha inserito proprio nel suo apice. Cosa comporta questa etichetta, che non è solo un logo di lusso? Comporta che l'interessato, d'ora in poi, ha una signoria sul modo con cui le informazioni che lo riguardano sono trattate, anche quando queste informazioni sono blindate, cifrate, trasformate in un *template*, e alcuni dei diritti che questa normativa riconosce sono di fatto divenuti indisponibili anche se non toccano aspetti della fisicità della persona. Le misure di sicurezza che vengono viste come un peso nella prima parte della slide di Galimberti sono divenute oggetto di un diritto soggettivo dell'interessato il quale può attivare un contenzioso circa la loro inattuazione anche se non vi è alcun concreto pericolo di un utilizzo abusivo delle informazioni.

E, allora, è chiaro che di fronte a questo cambiamento di carattere culturale ci sembra di poter guardare con perplessità alle preoccupazioni di chi oggi pensa, oggi soltanto, alla questione se ci sarà o meno una proroga di questo o di quell'adempimento in scadenza al prossimo 30 giugno. La coscienza ci obbliga, considerati gli spunti che sono arrivati da ieri da tutti gli amici presenti, anche nel corso delle pause, a definire senza timore, come "vampiri dell'ansia" dei ritardatari, quei soggetti che in questo periodo stanno vessando una serie di aziende proponendo loro soluzioni costosissime e inutili, specie attraverso software in circolazione che non danno alcuna garanzia di adempiere bene a tutti gli obblighi di sicurezza e che andrebbero sottoposti ad un "sequestro morale per oltraggio all'intelligenza".

Di fronte a tutto questo scenario, come si è comportato il legislatore ? Possiamo dire che l'autorità garante abbia saputo svolgere il suo ruolo ? Sul primo aspetto, quello del legislatore, mi pare indubbio che c'è stata una discreta innovazione anche delle tecniche legislative. Alludo non solo alle semplificazioni legislative o alla razionalizzazione delle norme, o all'introduzione dei codici di deontologia, ma anche al principio di efficacia che, accanto agli altri che sono stati evidenziati ieri, ci dice oggi che gli operatori istituzionali, pubbliche amministrazioni e soggetti privati devono concentrarsi su ciò che è veramente efficace per assicurare un livello elevato di tutela delle persone, in un quadro, appunto, di semplicità. Quindi, noi abbiamo aperto, attraverso questo Codice, la possibilità di adattare subito alle nuove tecnologie, senza perdere nulla in termini di efficacia dell'attività, le modalità dell'informare gli interessati, attraverso un *call center* oppure attraverso, diciamo, siti web.

C'è una buona attenzione legislativa, nel Codice, alla teleassistenza e alla telemedicina. Questo stesso Codice, e solo questo Codice, ci tengo a ribadirlo, ha aperto la possibilità di svecchiare, una volta per tutte alcune forme di accesso alla giustizia da parte dei cittadini: disponibilità *on-line* di ruoli di udienza, maggiore disponibilità pubblica delle pronunce già pubblicate e delle notizie sullo stato dei procedimenti; ha risolto poi, una volta per tutte, l'annoso problema del mascheramento o meno dei nomi delle parti nei processi più delicati che toccano ad esempio i rapporti di famiglia.

Ma c'è di più: giudici e forze dell'ordine, per effetto di questo Codice, e ribadisco, per effetto di un Codice che dovrebbe intervenire nel campo più limitato della tutela dei diritti della personalità, piuttosto che sulle dinamiche processuali. Guarda caso, però, questo Codice dà la possibilità agli operatori di giustizia di svolgere *on-line*, più facilmente, quegli accertamenti che la legge già permette di fare, senza mandare necessariamente qualcuno di persona o affidarsi alla posta.

Il secondo quesito riguardava l'autorità garante. Anche qui, non per spirito di istituto, mi sembra che l'autorità abbia fatto la sua parte e che, magari dopo un reclamo o una segnalazione, abbia trovato caso per caso varie soluzioni *privacy oriented* che gli operatori interessati non avevano saputo o non avevano pensato di dover trovare. Questa mattina abbiamo parlato poi dell'*e-government*: qui, va detto che non è pensabile che il cittadino ripieghi sul piano di diritti della personalità in una condizione deteriore solo perché può fruire, diciamo, di alcuni servizi *on-line*. Quindi, occorrerà proseguire l'attività in questo senso, non a marcia indietro, stando attenti anche ad alcune delle problematiche che ieri sono state evidenziate.

Noi, questa attenzione l'abbiamo trovata nell'Ufficio del Ministro per l'innovazione e le tecnologie, ma non l'abbiamo trovata sempre, sinceramente parlando, in alcuni operatori. Se si guardano le pronunce del Garante su le attività dei comuni *on-line* ci si accorge che a volte era stato posto un inutile ostacolo alla diffusione, maga-

ri delle sedute dei consigli comunali, e c'era al contrario una deriva rischiosa per quanto riguardava l'ostentazione di colloqui privati, magari del Sindaco, o di riunioni riservate delle giunte comunali; se si guardano i nostri provvedimenti sul rischio che si è corso ad un certo punto di costituire un'anagrafe nazionale, un'anagrafe delle anagrafi; se si guarda alle soluzioni tecnologiche che abbiamo trovato per il nuovo stato civile, per evitare la distruzione di questi registri in caso di calamità naturale, ma soprattutto per favorirne la gestione, possiamo rilevare che un ruolo questa autorità l'ha svolto ed è stato, purtroppo, un ruolo di supplenza di ciò che alcuni operatori istituzionali non hanno fatto. A volte, questo ruolo ha dato risultati positivi; altre volte non siamo riusciti a scalfire l'ostinazione dei nostri interlocutori.

Una partita molto aperta a questo riguardo è sulla spesa sanitaria; perché un obiettivo sacrosanto, quello di monitorare parti della spesa pubblica sempre più consistenti, ha portato nei mesi scorsi a redigere alcune norme che non sono francamente accettabili in una società democratica e, cioè, a prevedere la costituzione di una mega banca dati che dovrebbe contenere tutti i dati relativi a tutte le prescrizioni mediche di vario tipo dei cittadini italiani. Per fortuna, il dialogo successivo con le autorità sta portando, almeno spero, a risultati nettamente diversi, forse perché si è capito che attraverso le tecnologie è possibile arrivare allo stesso risultato: permettere ad un'unità sanitaria locale di fare effettivamente un controllo, che oggi magari trascura di fare, senza costruire una enorme banca dati che non esiste in nessun paese del mondo.

Auspichiamo anche che questo stesso risultato possa essere perseguito per quanto riguarda una scelta più recente che si affaccia nell'ordinamento, quello della costituzione di una anagrafe nazionale degli studenti di cui non sono perfettamente chiare ancora le finalità e di cui speriamo che si possa chiarire meglio la portata. Poi, un cenno va fatto a chi normalmente vede la privacy (torno a parlare del mio interlocutore istituzionale), come un fattore seccatore: pensiamo spesso alla interoperabilità dei sistemi, e pensiamo poco al *back-office*, che rimane basato su un sistema ordinario di gestione. Quindi, quel risultato che si ritiene insoddisfacente e che spesso viene attribuito alle norme di protezione dei dati o alle preoccupazioni che derivano dalla privacy, a volte deriva invece dalla mancanza di coraggio di portare avanti l'automazione anche, appunto, nel *back office*.

Teniamo anche presente che questi problemi non possono essere risolti guardando soltanto al problema della sicurezza ed introducendo ad esempio la cifratura. Una citazione per tutti che deriva dalle cronache di questi giorni sulla psicanalisi *online*. Se si guarda a questi articoli di stampa, si vede che non c'è soltanto il problema dell'identificabilità del professionista; il problema, quindi del consenso informatico, della cifratura, della firma digitale: sull'essere certi, quindi, che ci siano due interlocutori riconosciuti e che non ci sia il rischio di una ingerenza da parte di soggetti

non autorizzati. C'è anche un problema che riguarda la persona. È un problema che non è soltanto di privacy. Ricordiamoci che questo Codice non tutela soltanto il diritto alla sfera privata. Alcuni osservano infatti, giustamente, che c'è un problema serio a considerare lecita la psicanalisi *on-line* rispetto a soggetti per i quali non si è mai stabilito un rapporto precedente con il paziente e che si deve prendere in considerazione il fatto che nella psicoterapia i corpi devono essere presenti. Quindi, si guarda alle problematiche che possono sorgere dal fatto che la *web-cam* non garantisce che nella stanza del soggetto che ti assiste ci sia qualcun altro o viceversa.

Potremmo fare molti altri esempi. Ieri abbiamo citato la pubblicità durante le conversazioni telefoniche. Ebbene, la società *GratisTel* che aveva deciso di iniziare in Italia questa attività aveva preso il software in Svezia, ovvero da un Paese che non aveva ancora recepito la direttiva comunitaria. La *GratisTel* (non quella italiana, ma la casa madre svedese) ha fallito *in toto* l'impostazione *privacy oriented* di questa tecnologia e ha speso molti soldi per adeguarla alla soluzione che noi cooperativamente abbiamo poi individuato.

Siamo stati visti nella fase iniziale della procedura contenziosa come dei pericolosi seccatori e si è pensato subito ad un contenzioso giudiziario contro l'autorità. Quando è invece terminato il procedimento dinanzi al Garante, il servizio non è poi decollato, forse per altre ragioni commerciali. Ma quando noi abbiamo individuato la prima informativa agli interessati in sette secondi di conversazione telefonica, e abbiamo individuato le modalità per integrarla in altro modo, la *Gratistel* a livello europeo ha preso atto con soddisfazione di questa soluzione ed ha potuto beneficiare del lavoro svolto dall'autorità italiana in molti altri contesti.

Non parlerò delle considerazioni che abbiamo fatto a proposito del riconoscimento facciale nella video-sorveglianza. C'è un nostro provvedimento che evidenzia chiaramente i rischi che si pongono in questi casi come in quelli della biometria. Non accennerò poi, per brevità di tempo, a tutte le altre considerazioni che abbiamo fatto in materia di *spamming*, di sms, e anche di tv interattiva su cui è prevista la possibilità di intervenire in un prossimo futuro: credo che l'esempio che ho appena fatto mi permetta di concludere positivamente all'interrogativo che avevo posto prima.

Certo, non possiamo nasconderci che c'è ancora una certa barriera culturale all'azione volta a orientare tutte queste innovazioni al principio di necessità.

L'intervento dell'autorità garante non è necessariamente sempre interdittivo, diciamo, o di cassazione. Se prendiamo due esempi, due soli, che vengono una volta tanto (se no parliamo troppo del garante italiano), dai nostri cugini francesi (che hanno peraltro ancora una legge legata del 1978), abbiamo due casi esaminati in aprile e quindi attualissimi, riguardanti l'uso della biometria. Ebbene, come si può notare, abbiamo due deliberazioni dello stesso giorno, l'8 di aprile, a proposito degli aeroporti di Orly e di Roissy. L'autorità francese riconosce che l'uso delle tecni-

che biometriche in particolarissime aree di sicurezza (da parte solo di alcuni addetti ed utilizzando una tecnica che non porta, come ci si diceva ieri, ad immagazzinare in una banca dati il complesso delle impronte, ma semplicemente a lavorare su un *badge*), sia proporzionato e ragionevole.

Allo stesso tempo, lo stesso giorno e per un diverso progetto che riguarda il invece centro ospedaliero di Yale si giunge alla esatta opposta conclusione. Perché, si dice, il sistema biometrico ipotizzato per questo ospedale, basato semplicemente sulla finalità di gestione migliore del rapporto di lavoro, non avrebbe avuto una finalità proporzionata e a nulla sarebbe valso il consenso eventuale dei lavoratori interessati.

Ora, penso che dovremmo fare di più la nostra parte per incrementare la consapevolezza degli utenti rispetto a molti mezzi di comunicazione. In questo senso, si apre tra pochi mesi una partita importante, forse la più importante da quando in Italia c'è una disciplina organica sulla privacy ed è quella che riguarda i nuovi elenchi telefonici *on-line*, ed anche cartacei.

Uno degli sforzi più importanti che l'autorità sta facendo in collaborazione con gli operatori, è quello non di individuare nuove regole sul consenso, sull'informativa o sui diritti di essere messi o non messi su questo elenco, ma di definire la brevità e la chiarezza dei moduli per spiegare anche agli utenti meno avveduti l'importanza delle scelte da fare sull'essere o meno in questi elenchi (che saranno molto più disponibili di prima, conterranno i dati relativi alle utenze mobili, ma, soprattutto, saranno sfruttabili attraverso nuove metodologie).

Le autorità di garanzia, non solo quella italiana, dovranno investire più risorse su queste tematiche, dovranno caratterizzarsi anch'esse come autorità di terza generazione cercando di trovare quegli spazi che spesso l'ordinario e pressante lavoro che deriva dal contenzioso, dalle ispezioni, dall'attività internazionale non sempre permette.

Noi abbiamo, e mi avvio alla conclusione, uno strumento formidabile per incrementare il dialogo con il mondo Ict, anche quando non c'è un contenzioso. Il Codice ha previsto questo nuovo istituto del *prior checking* che permette, per la biometria, per la genetica, per la localizzazione, prima di far partire una tecnologia, prima di programmarla, prima di implementarla, di chiedere l'orientamento di questa autorità ed essere confortati in scelte che possono avere poi una riproduzione su scala. E diciamo anche che occorrerà forse investire più risorse nel prossimo futuro per quanto riguarda le modalità semplici per esercitare i diritti da parte degli interessati, modalità *user friendly*, *plug and play*, anche per isolarsi, diciamo, nel quadro dei dispositivi di localizzazione o per governare la nostra privacy rispetto a tutti questi vari dispositivi che avremo nella interazione di pc, computer e televisione.

L'interessato dovrà avere diritto di cambiare le proprie scelte senza essere necessariamente legato ad una raccomandata postale. Quindi, una semplicità tecnologica anche nell'esercizio dei diritti. Altrimenti noi rischiamo, proprio su questo punto della

complicazione delle modalità di esercizio di diritti, di avere non un *digital divide*, ma un *right divide* che deriverebbe peraltro dalle norme, ma dalla complicata situazione di fatto. Il cittadino, sul tema degli elenchi telefonici come per molte altre cose più complicate, potrebbe non essere edotto e trascurare quindi le garanzie e i mezzi per tutelarsi con la stessa semplicità con cui potrà invece collegarsi, navigare ed effettuare scelte parimenti importanti. Insomma, abbiamo capito che la privacy degli anni 2000 non è di ostacolo ad uno sviluppo efficace delle nuove tecnologie.

Mi sembra che quindi sia da considerarsi superato l'interrogativo se il diritto debba intervenire solo dopo che determinate tecnologie sono mature o se debba invece normarle prima, indirizzandole. Sul piano delle norme, abbiamo già la garanzia che il mondo *on-line* non è una *right-less society*. La legge attribuisce a questa autorità, come ad altre istituzioni, un compito affascinante. E questo compito va esercitato con cura. Abbiamo bisogno, visto anche che abbiamo molte imprese oggi qui, di esportare questa etica delle nuove tecnologie al mondo della progettazione, al mondo dello sviluppo dei sistemi informativi; occorre risolvere preventivamente il problema delle *privacy enhancing technologies*.

Diceva ieri il prof. Rodotà: “*Il principio di necessità deve diventare regola*”; ci ricordava ieri il prof. Rasi: “*Abbiamo bisogno di un imprenditore innovativo*”. Ebbene, di questa inventiva pro-persona abbiamo un grande bisogno. Abbiamo bisogno, e concludo, di una creatività garante.



Tavola rotonda

SESSIONE III
QUALE FUTURO PER LA PRIVACY

COORDINATA DA **CARLO MASSARINI**

Sessione III - Tavola rotonda

Quale futuro per la privacy

Coordinata da Carlo Massarini

Interventi di: 1. Lucio Stanca, 2. Carlo Formenti, 3. Francesco Chirichigno, 4. Stefano Rodotà

Presentazione

Gaetano Rasi

Passiamo dunque alla Tavola Rotonda “Quale futuro per la privacy”. Tavola Rotonda che è il coronamento di questo Convegno che si è svolto tra ieri ed oggi in maniera così densa ed anche, mi sembra, produttiva, utile per il futuro.

La Tavola Rotonda è coordinata dal dott. Carlo Massarini, che tutti noi conosciamo perché autore e conduttore televisivo: ha curato per sette anni la trasmissione Rai “Mediamente”, interessandosi in particolare alle nuove tecnologie digitali, nonché agli sviluppi delle innovazioni in genere. Lo ringraziamo per aver accettato di partecipare a questo Convegno.

Della Tavola Rotonda fa parte il ministro Stanca, che tutti conosciamo come benemerito della modernizzazione del Sistema Italia, pubblico e privato. Fa parte poi il dott. Francesco Chirichigno, che è stato direttore generale, e poi amministratore delegato di Telecom Italia. Uno dei maggiori manager delle telecomunicazioni che possiede l'Italia. Attualmente è presidente di una Società che opera nel settore delle infrastrutture per la banda larga. E, ancora Carlo Formenti, giornalista, la cui firma è ben nota. Lavora, come voi sapete, al Corriere della Sera. È autore di molti libri tra cui un libro intrigante, molto interessante davvero: “Mercanti di futuro”. Insegna “Storia e Tecnica dei nuovi Media” all'Università degli Studi di Lecce. Il prof. Stefano Rodotà, non ha bisogno di essere presentato. Il nostro presidente è un capo scuola nel diritto della privacy insieme con il nostro vicepresidente, prof. Giuseppe Santaniello.

Spero che, come in tutte le Tavole Rotonde conclusive, non solo si tirino un pò le somme di questi due giorni di lavoro ma si provi anche a guardare oltre, a dopodomani. A quelli che possono essere gli sviluppi di una situazione che è oggettivamente interessante da un punto di vista tecnologico, ma forse da affrontare con cautela da un punto di vista della privacy.

Sicuramente chi di voi è stato qui da ieri avrà già sentito molti degli argomenti in ballo. Se posso tirare una sintesi, ma giusto per dare il la a questa nostra discussione - noi abbiamo un'ora per confrontarci- direi che il problema della privacy stia per fare un salto. Mi spiego: negli ultimi anni, con lo sviluppo di Internet, delle reti di comunicazione, delle reti mobili e quant'altro, abbiamo avuto una serie di problemi, che il prof. Rodotà, con il quale spesso ci siamo sentiti quando era in onda "Mediamente", ha sottolineato più volte. E sono i problemi che conoscete bene, i problemi relativi soprattutto alle leggi relative alla comunicazione, quindi a Internet, alla telefonia, alla telefonia mobile, quindi agli sms, più recentemente alle impronte digitali, alle banche dati. Le banche dati insieme ad Internet è stato uno degli argomenti sui quali ci si è focalizzati di più negli ultimi anni. Siamo però in un momento nel quale la tecnologia ci sta portando molto oltre. Alcune delle parole chiave dei prossimi anni potrebbero rappresentare una frontiera nuova e molto difficilmente controllabile, almeno per adesso. Credo che questo sia il tema dei prossimi anni. Il futuro prossimo vuol dire, come diceva il prof. Rodotà in questa interessante introduzione al suo documento poi inviato al Presidente della Repubblica, il momento in cui il corpo diventa una password, il momento in cui l'individuo non è più una persona che mette a disposizione o nega o a cui vengono chiesti determinati dati, ma è il suo corpo stesso ad essere messo in gioco. I chip da introdurre sotto la pelle, l'Rfid, questa sorta di nuovo codice a barre che in qualche maniera è in grado di localizzare la merce, e non solo la merce, a seconda di come si muove, i dati biometrici.

Ieri si parlava addirittura anche di smog dust, quindi di una polvere -siamo sulla frontiera delle nano tecnologie- la polvere intelligente, che può addirittura mandare dei segnali. È chiaro che noi stiamo passando da un momento di sorveglianza visibile, in fondo le telecamere le vediamo se ci stiamo attenti a un'altra fase. Sappiamo che su Internet in generale i dati digitali possono essere rintracciati, possono essere controllati, possono essere immagazzinati. Stiamo passando ad un momento in cui la persona deve essere consapevole che ci saranno degli altri rischi, per quanto riguarda la privacy. Dei rischi, tra virgolette, direi, invisibili. Quindi è un momento nel quale bisogna avere molta cautela. Bisogna un pò prevedere perché certe

(1) Giornalista

tecnologie nel tempo potranno esplodere, diventare importanti. Bisogna monitorarle fin dall'inizio per riuscire ad andare avanti alla velocità delle tecnologie.

Una cosa che negli anni è sempre stata abbastanza chiara è che, da un punto di vista giuridico e da un punto di vista etico, i tempi sono quelli umani, quindi sono più lenti. Le tecnologie corrono molto di più, anche perché ci sono centinaia di migliaia, milioni di persone in tutto il mondo che le fanno evolvere, grandi aziende o magari ragazzetti nei garage. Mentre invece le nazioni, i governi, da un punto di vista giuridico e da un punto di vista etico marciano più piano. È inevitabile che sia così. Però questa differenza di velocità può creare, e ha creato anche nel passato remoto, ma anche e soprattutto nel passato recente, una differenza di velocità. La conseguenza è che le due cose non possono procedere contemporaneamente. E questo può creare dei guai, può creare dei problemi. Allora, io chiederei ai quattro relatori che sono al tavolo, il ministro Stanca, il dott. Chirichigno, Carlo Formenti, il prof. Rodotà di fare, magari un primo esame, anche per farci conoscere, la loro posizione.

Se posso, vi chiederei una durata di sei, sette, minuti per un primo intervento prima di passare alla vera propria Tavola Rotonda, dove metteremo a confronto, e cercheremo di approfondire le singole situazioni.

Vuol cominciare Lei, Ministro:

Lucio Stanca⁽²⁾

Desidero innanzitutto esprimere un complimento sincero per l'organizzazione di questo incontro perché credo sia importante che in Italia si approfondiscano temi così attuali come la privacy e l'innovazione tecnologica. Il nostro Paese ha certamente accumulato ritardi sul fronte dell'innovazione tecnologica, in particolare digitale, soprattutto a causa di un gap culturale. Non siamo ai primi posti in Europa nelle varie classifiche di utilizzo e di penetrazione di queste tecnologie. Quindi ben vengano occasioni come queste per approfondire, dibattere e far accrescere la conoscenza e la diffusione delle nuove tecnologie nella nostra società.

Stiamo entrando a far parte, e ce ne accorgiamo ogni giorno, di una società molto diversa, basata sull'innovazione tecnologica. Quella che può essere definita come "l'economia dell'innovazione" è un edificio che poggia su tre pilastri: la conoscenza, che viene alimentata dalla formazione e dalla ricerca di base; la ricerca (in particolare quella applicata) con il suo obiettivo di realizzare l'innovazione tecnologica; ed infine la tecnologia (in particolare quella digitale) che promuovendo soprattutto l'innovazione di processo (a differenza della ricerca e lo sviluppo, che genera principalmente innovazione di prodotto), migliora la produttività, dunque la cresci-

(2) Ministro per l'Innovazione e le Tecnologie

ta, attraverso la diffusione di nuove applicazioni fra i cittadini, le imprese e le pubbliche amministrazioni.

Perché questa “economia dell’innovazione” si espanda in Europa e soprattutto nel nostro Paese bisogna dunque operare ed investire allo stesso tempo nell’istruzione e formazione, nella ricerca di base ed applicata, pubblica e privata, e sulla capacità di “assorbimento” delle tecnologie moderne (in particolare quelle digitali).

Siamo solo all’inizio di questa rivoluzione digitale verso la quale dimostriamo un limite: non riusciamo a comprendere fino in fondo l’evoluzione tecnologica in tutte le sue implicazioni fondamentali, dalle comunicazioni alla capacità di calcolo, alla memorizzazione. Quindi abbiamo davanti a noi, come in tutte le grandi ondate innovative, da una parte delle enormi opportunità e dall’altra anche dei rischi. È compito della politica massimizzare le opportunità e contenere il più possibile i rischi che possono diventare, invece, un reale motivo di rallentamento nell’uso di queste tecnologie. La sfida della politica è quindi quello di indirizzare e gestire i processi di diffusione tecnologica.

Non a caso, le Nazioni Unite, di fronte all’emergere di questa nuova società dell’informazione, alla cui base vi è una “terza rivoluzione industriale” che sta cambiando l’economia, gli stili di vita, i modelli sociali e pressoché tutti i nostri campi di attività, hanno ritenuto opportuno convocare il primo vertice sulla società della informazione, che si è tenuto a dicembre 2003 a Ginevra, e che vedrà una seconda fase a Tunisi nel novembre 2005. Nella “Dichiarazione dei Principi” firmata da 191 Paesi – che considero una “Magna Charta” istitutiva della società dell’informazione a livello planetario – vi è un punto molto interessante: il rafforzamento di un quadro di “trust”, di fiducia. In realtà il termine inglese “trust” significa più che fiducia: include sicurezza delle informazioni, delle infrastrutture di rete, l’autenticazione, la privacy e la protezione dei consumatori. Pilastri fondamentali, di cui la privacy è un prerequisito, per lo sviluppo della società della informazione, per costruire un reale clima favorevole tra gli utilizzatori delle nuove tecnologie. Da qui la mia prima conclusione: chi contrappone le tecnologie digitali alla privacy, piuttosto che porre l’accento sull’autenticazione, sulla sicurezza delle reti o delle informazioni, commette un errore grossolano, dimostrando di non comprendere a fondo l’argomento. In realtà non vi è contrapposizione, anzi la diffusione di queste tecnologie è direttamente proporzionata, lo si dice anche nella “Magna Charta” cui accennavo prima, all’aver risolto o perlomeno affrontato queste problematiche. Perché alla base di questa moderna società dell’informazione non vi siano le tecnologie, ma proprio i grandi valori di libertà, di democrazia, di espressione, di sviluppo economico, di partecipazione.

In genere riusciamo a rimuovere i timori, le preoccupazioni che molte persone possono provare di fronte alla diffusione di nuove tecnologie se ci sentiamo più

sicuri, più protetti. In altre parole se vi è un ambiente che ci permette di mettere a frutto le prospettive e le opportunità offerte da queste tecnologie. Si stanno affermando una serie di nuovi diritti della società dell'informazione. Parlo, ad esempio, del diritto all'accesso in rete. Dieci anni fa non si poteva neanche parlare di diritto all'accesso, perché non avevamo la rete! Credo fermamente che oggi tutte le persone, tutti gli uomini e tutte le donne, debbano avere il diritto all'accesso. Penso ad esempio alla legge di grande progresso e civiltà che abbiamo promosso in Italia, la prima in Europa, per affermare il diritto all'accesso dei disabili alle tecnologie informatiche. Penso al diritto alla trasparenza: a poter conoscere, cioè, chi memorizza i miei dati, chi li conserva; a sapere, come semplice cittadino, di quali dati e informazioni si tratti. Penso al diritto alla privacy: per una società moderna basata sull'uso delle nuove tecnologie, è un diritto emergente molto forte, assolutamente necessario, da difendere se si vuole garantire uno sviluppo corretto della "civiltà digitale". Stiamo assistendo a un progresso tecnologico che nessuno pensa, ovviamente, di poter rallentare o fermare.

Non sto affermando, però, che le grandi opportunità che ci offre la tecnologia siano soltanto positive e che debbano essere accettate acriticamente, senza un'approfondita analisi dei rischi e dei pericoli che possono implicare. Sta alla politica, come ho già detto, massimizzare opportunità e ridurre i rischi, ma poi anche promuovere lo sviluppo di questa società. A meno che qualcuno non intenda sostenere che l'adozione delle tecnologie digitali comporti molti più rischi che opportunità: in tal caso dovremmo avere tutt'altro tipo di dibattito. È questo il quadro generale di riferimento. Ovviamente in una società complessa come la nostra talvolta emergono diritti fondamentali in contrasto l'uno con l'altro. Ogni diritto anche costituzionalmente garantito (ad esempio quello alla sicurezza), trova il limite in un altro diritto, anch'esso costituzionalmente garantito (come quello alla riservatezza): il confine non è facile da definire. Allora il problema è definire il confine, il crinale, cioè il giusto l'equilibrio tra questi diritti fondamentali.

Per quanto riguarda il rapporto tra le nuove tecnologie digitali e la privacy, voglio innanzitutto porre l'accento su questo equilibrio, che è una sfida di "qualità della democrazia". E quindi di qualità anche nella capacità di produrre norme, per assicurare e gestire al meglio un conflitto che oggettivamente esiste. Lo sviluppo delle tecnologie dell'informazione e della comunicazione porrà sempre nuove sfide alla privacy. Privacy è, come accennavo, un termine anglosassone; nel contesto europeo e americano possiamo notare che l'approccio normativo alla privacy è differente. Quindi certamente si pone il problema di una produzione normativa che tenga conto di sensibilità culturali diverse: pensiamo al mondo emergente dell'Asia, ad esempio, relativamente a questi argomenti. Poi vi sono anche circostanze diverse. La stessa tecnologia, assolutamente positiva e accettabile in alcune circostanze, diventa

assolutamente negativa e da rigettare in altre. Man mano che acquisiamo più familiarità, abbiamo anche più fiducia del mezzo. Sintetizzando, dunque, la definizione del crinale non è una scelta ideologica. Non è rigida, ma influenzata da varie circostanze che devono essere tenute nella giusta considerazione.

Le nostre politiche di innovazione tecnologica si orientano verso tre punti cardinali. Il primo riguarda la *diffusione* delle tecnologie. Siamo indietro rispetto ad altri Paesi avanzati e oggi il personal computer rappresenta sicuramente un valido supporto sia nel lavoro che nello studio. Il secondo cardine è l'*inclusione*, perché dobbiamo assolutamente evitare nuova emarginazione, soprattutto tra le categorie deboli o svantaggiate come gli anziani, i disabili, le famiglie con un reddito inferiore, chi vive in aree remote. Qui abbiamo promosso iniziative come la nostra legge di disabilità, gli incentivi alle famiglie con basso reddito, le iniziative comunali per l'alfabetizzazione informatica degli anziani, la promozione di reti e contenuti digitali per le aree svantaggiate. Il terzo punto cardine è la *fiducia*. Che significa promuovere strumenti di autenticazione e di riconoscimento in rete, dunque privacy.

Proprio riguardo alla privacy voglio sottolineare che il primo avviso di e-Government attraverso il quale sono stati individuati e co-finanziati 134 progetti, conteneva in allegato le "Linee guida sul trattamento dei dati personali", relative alla tutela della privacy dei cittadini che usufruiscono dei servizi pubblici in rete. Un documento redatto in stretta collaborazione proprio con il Garante per la tutela dei dati personali, che colgo l'occasione per ringraziare pubblicamente. Lo sviluppo del governo elettronico, l'e-Government, è una straordinaria occasione per la Pubblica Amministrazione, passaggio fondamentale per un Paese moderno e per rispondere alla crescente domanda di servizi e di efficienza da parte dei cittadini e delle imprese e di una loro maggior partecipazione alla vita pubblica (quella che viene chiamata e-Democracy o democrazia elettronica). Il recente avviso di e-Democracy, che consente la partecipazione dei cittadini, in quanto elettori, alla vita e alle decisioni delle istituzioni, siano esse regionali, locali o di qualsiasi altro livello, è "costellato" da continui riferimenti alla protezione della privacy, alla necessità di conservare, in molti casi, l'anonimato. Si minerebbe alla base il concetto stesso di e-Democracy se non fosse garantita la partecipazione del cittadino nelle migliori condizioni di tutela dei propri dati personali. Una mancanza di privacy, in questo caso, potrebbe generare, ad esempio, una discriminazione in base alle opinioni politiche.

Ribadisco, ancora una volta, dunque, che è compito della politica massimizzare le opportunità, veramente interessanti, che ci offre la trasformazione digitale della nostra società, e nello stesso tempo affrontare i potenziali rischi proteggendo le persone attraverso una specifica normativa, in modo da poter creare un clima di maggiore fiducia nell'approccio e nell'uso delle nuove tecnologie.

Quel che mi preoccupa è, invece, l'allarmismo. Perché, come ho sottolineato proprio all'inizio del mio intervento, questo Paese è in ritardo nell'uso delle tecnologie dell'informazione e della comunicazione per un fattore culturale e non economico: si tratta, in ultima analisi, di una mancanza di comprensione. Abbiamo una maggiore diffidenza rispetto a questa onda innovativa. Quindi dobbiamo conseguire una corretta formazione di fronte al cambiamento della nostra società. È sicuramente importante rimuovere la diffidenza relativa alla sicurezza, alla privacy, all'autenticazione in rete. Ma è davvero preoccupante se problematiche di questo tipo vengono continuamente prospettate in termini di allarme. I grandi media, ad esempio la televisione, parla pochissimo di Internet, e quando ne parla lo fa spesso in termini negativi, in situazioni collegate alla pedofilia o con il terrorismo. In questo modo viene sempre accoppiato un valore negativo ad un validissimo strumento dalle grandi potenzialità, di promozione della libertà, della conoscenza, di informazione, quale è Internet. L'allarmismo è l'ultima cosa di cui abbiamo bisogno nel nostro Paese. Perché, infine, l'opportunità non è la tecnologia in sé, ma tutto quello che la tecnologia genera di positivo. Questa è la sfida con la quale dobbiamo confrontarci.

Carlo Massarini

Sono assolutamente d'accordo con Lei Ministro. Io mi ricordo dei primi tempi in "Mediamente", che cominciò nel '95: questi sono proprio gli echi. Ed ha ragione: Internet, i primi tempi che andò sulle prime pagine, - Formenti, che fa il giornalista, se lo ricorderà bene - era proprio legato ai casi "scandalo", quelli che facevano notizia, quindi inevitabilmente, quasi sempre negativi. Credo che forse Internet all'inizio era una terra virtuale popolata da persone di estrazione e tendenze diverse, e forse si è creato fin dall'inizio un equivoco sul fatto che Internet, essendo nata in maniera un po' anarchica, libera, spontanea, dovesse continuare ad essere così. Poi credo che il tempo abbia dimostrato che solo attraverso la sicurezza, solo attraverso delle regole che tutti quanti sono in qualche maniera tenuti a rispettare, si può creare una piattaforma, come diceva il Ministro, che dia fiducia, che quindi poi attragga la grande massa. Altrimenti potrebbe rimanere una cosa per pochi eletti. Quindi la funzionalità del sistema, la sicurezza del sistema, è assolutamente alla base di un *buon* sistema. Ora, chiamerei in causa Carlo Formenti: a proposito di ruoli comuni per quanto riguarda la privacy e lo sviluppo tecnologico, so che lui vuole sottolinearne alcuni. Partiamo da quelli per vedere un po' come negli anni si è sviluppato proprio il rapporto tra privacy e sicurezza e tra la tutela dei dati e lo sviluppo delle tecnologie.

Vorrei partire dal tema della comunicazione, sottolineata nell'ultima parte dell'intervento del ministro Stanca. Mettendomi nei panni di un non addetto ai lavori che ha seguito queste due giornate di convegno, ho la sensazione che abbia ricevuto due messaggi che vanno in direzioni opposte. Introducendo la Tavola Rotonda, tu hai rievocato le immagini da fiera delle meraviglie associate al concetto di *ubiquitous computing*, alla pervasività delle nuove tecnologie, alla potenza di elaborazione distribuita ovunque, all'intelligenza incorporata in un numero crescente di oggetti ecc.. Da quasi tutti gli interventi - che ieri ci hanno spiegato come stiano rapidamente progredendo questo tipo di tecnologie - emergeva un primo messaggio, che suona francamente inquietante, non molto lontano dalla tesi sostenuta da uno dei massimi esperti di sicurezza del gruppo Gartner, Richard Hunter, nel suo recente libro "Un mondo senza segreti": tutti noi stiamo andando verso un mondo di trasparenza assoluta, e non esiste alcuna possibilità di invertire questa tendenza. Come ha brutalmente sintetizzato Scott McNealy, il Ceo di Sun Microsystems, "You have zero privacy", rinunciate a ogni illusione di poter mantenere un minimo di privacy. Un altro messaggio è arrivato dal tavolo del Garante che, al contrario, ci ha detto: siamo ancora perfettamente in grado di tutelare la privacy, nella misura è la tecnica stessa a offrire le soluzioni per i problemi, i rischi e le sfide che il suo incessante cammino suscita continuamente.

Carlo Massarini

Perché qui il luogo comune è un pò "... se tu non hai niente da nascondere che problema è per te la privacy, che problema è per te la trasparenza?"

Carlo Formenti

La verità è che abbiamo tutti qualcosa da nascondere. A partire da coloro che detengono il potere i quali, com'è noto, non hanno mai molto amato la trasparenza: basti ricordare la recente decisione del Pentagono di vietare l'uso privato di telecamere digitali ai soldati americani che operano in Iraq, per evitare la diffusione di immagini sgradite. Al potere la trasparenza piace solo quando funziona dall'alto verso il basso, e non viceversa. Ma non sono solo i potenti, siamo anche tutti noi, persone normali, ad avere qualche cosa da nascondere: per esempio i nostri gusti sessuali, le nostre idee politiche-religiose, il nostro stato di salute, ecc. Esiste un diritto a essere la-

(3) Giornalista

sciati soli, così come esiste un diritto all'oblio, che hanno ottenuto un riconoscimento e sono stati codificati all'interno della tradizione giuridica anglosassone, ma che l'Europa ha il merito d'aver saputo ulteriormente ampliare, e oggi questi diritti sembrano essere minacciati. Così qualcuno ieri ha detto che ormai dovremmo rassegnarci a rinunciare al diritto ad essere lasciati soli – accontentandoci del diritto a non essere coinvolti - perché nessuno può più realisticamente sperare di essere lasciato solo in un mondo pervaso dalle nuove tecnologie. Ebbene, io sono convinto che il senso di ineluttabilità che viene in questo modo trasmesso sia sbagliato, soprattutto quando viene attribuito a effetti immanenti al progresso tecnologico in quanto tale. In ultima istanza è sempre la società a governare, consapevolmente o meno, lo sviluppo tecnologico, siamo noi che, a seconda del modo in cui ci appropriamo di determinate tecnologie, determiniamo la direzione di sviluppo che prendono tanto la ricerca tecnologica quanto il mercato che ne sfrutta i risultati. Ecco perché ritengo che i rischi maggiori arrivino dal clima di paura che oggi sembra pervadere la società. Qualcuno, giustamente, stamattina ha detto che la ricerca di sicurezza non deve essere ispirata dalla paura. Purtroppo il senso di paura è invece insidioso e diffuso, suscitando per esempio la tentazione di controllare i bambini attraverso le web-cam o, come vorrebbe il Ministro Sirchia, di iscrivere gli anziani in un "registro dei fragili". E mentre cresce l'allarmismo sociale nei confronti dei normali rischi statistici che riguardano i soggetti più deboli, letteralmente dilaga la paura suscitata dagli spettri del terrorismo e del cyber-terrorismo. Così finiremo per essere tutti disponibili a lasciarci sottoporre alle più diverse forme di sorveglianza permanente, una tendenza alimentata anche dalle sempre più diffuse pulsioni all'esibizionismo mediatico da parte della gente comune. Basti ricordare le cinquemila persone che ieri si sono presentate per partecipare alla trasmissione del Grande Fratello, lottando per conquistare l'opportunità di mettere in piazza la propria immagine attraverso i media elettronici.

Carlo Massarini

non in questa sala, però.

Carlo Formenti

Si spera di no. Ma vorrei concludere ricordando che a ispirare le tentazioni più insidiose a rinunciare alla nostra privacy è probabilmente il nostro amore per la vita facile. Ieri qualcuno diceva: perché rifiutare il passaporto biometrico, visto che

questa tecnologia promette di evitare noiose code in aeroporto? Per tacere delle mille altre comodità che ci vengono offerte dalle nuove tecnologie. Così sta succedendo una cosa curiosa: fino a ieri la condizione di anonimità sociale garantita dalla metropoli moderna ci era parsa come una liberazione dal controllo ossessivo della comunità sull'individuo – quello, per intenderci, del paesino dove tutti sapevano tutto di tutti. Oggi, mentre stiamo entrando in una sorta di ipermodernità tecnologica, molti sembrano disposti a regredire alla vecchia mentalità premoderna, accettando l'idea – che qualcuno ieri ha formulato esplicitamente – secondo cui l'autonomia individuale non può più essere conservata nell'era digitale. Per fortuna siamo ancora in grado d'impedire che questo punto di vista prevalga, e vorrei sottolineare che gli anticorpi più efficaci a tale scopo, si trovano paradossalmente proprio all'interno dello strato culturale più coinvolto nella rivoluzione tecnologica in corso: mi riferisco a quella cultura della rete che ha sempre cercato di autogestire la sicurezza senza rinunciare alla privacy, rifiutando di delegare le proprie scelte alla miriade di grandi e piccoli fratelli che oggi incarnano le nuove forme del potere politico ed economico.

Quanto al Garante, penso che, tenuto conto del contesto ideologico in cui è oggi costretto a operare, il suo ruolo sarà sempre più quello di difendere in modo intransigente quei diritti - anonimità, inosservabilità, intracciabilità, il diritto a essere lasciati soli, il diritto all'oblio – che alcuni vorrebbero far passare per vecchi e superati. Un esempio di queste vecchie-nuove battaglie ci è viene offerto dal caso del decreto-legge 354 che, senza l'intervento del Garante, avrebbe portato da 24 a 30 mesi il tempo massimo di registrazione dei dati del traffico telefonico e di rete. Ma per aiutare il Garante in questa difficile missione, dobbiamo soprattutto combattere ogni pedagogia della paura: la consapevolezza delle sfide che ci arrivano dal rapporto fra privacy e sicurezza non si ottiene agitando sotto il naso della gente lo spettro dei rischi che ognuno di noi corre connettendosi alla rete.

Carlo Massarini

Allora molte grazie a Carlo Formenti. Molti spunti li riprendiamo dopo. Vorrei chiudere questo primo giro. Il diritto alla irrintracciabilità, mi ricorda molto *Chi l'ha visto*, un programma televisivo che voi conoscete, perché uno avrà pure il diritto di sparire, se se ne vuole andare e vuole mollare tutto avrà il diritto di farlo senza essere inseguito da orde di cameramen e persone che si passano parola!

Ing. Chirichigno la Sua posizione, invece, in merito a questo sviluppo tecnologico e della privacy?

Dopo l'intervento del collega Formenti ritengo necessario rilevare, pur estremizzando, che vi sono due linee di tendenza che guardo entrambe con grande preoccupazione: c'è chi crede ancora di poter ripristinare un'epoca luddistica e quindi di rottamare tutte le macchine e chi, invece pensa che la privacy non abbia più scopo di essere perché tanto la tecnologia prevarica su tutto. Io credo che sia necessario raccogliere una considerazione che ha fatto il dott. Buttarelli al termine della sua relazione in merito alla collaborazione e sinergia fra privacy e sviluppo della tecnologia. Inoltre io aggiungo: possiamo permetterci il lusso di non avere uno sviluppo economico, di non avere una innovazione perché abbiamo la preoccupazione che la nostra privacy venga limitata? Io penso assolutamente di No. È necessario fare un salto di qualità.

Da un lato, c'è l'innovazione tecnologica, fenomeno non solo notoriamente inarrestabile ma anche dimostrabilmente alla base dello sviluppo economico dei Paesi che, più di altri, in esso credono ed investono. L'innovazione che si concretizza in un processo di sviluppo di applicazioni pratiche, che si trasforma in aumento del prodotto interno lordo, dei posti di lavoro e del benessere materiale dei cittadini.

Dall'altro, la possibilità di digitalizzare le informazioni, di conservarle in misura quantitativa e temporale quasi incredibile ed a costi accessibili, di scambiarsele in tempo reale, di elaborarle con modelli matematici sempre più sofisticati, associata ad una "permeabilità" evidente delle reti di computers e dei relativi sistemi di sicurezza, rende sgradevolmente concreta la possibilità che il "Grande Fratello" si concretizzi sul serio e, quel che per certi versi è peggio, che non si tratti solo di un occhiuto controllo riservato allo Stato-Padrone, ma che una miriade di soggetti possano essere in grado di "ficcare il naso" nelle nostre questioni più intime e delicate, costringendoci ad una non voluta "trasparenza", che ci renderebbe debolissimi, sempre meno padroni della nostra vita.

Ad oggi, non sembra essere stata imboccata di comune accordo una via di soluzione a questo non facile dilemma. C'è il rischio di contrapposizione fra posizioni ugualmente estremiste ed inconcludenti.

Torno a ripetere, veniva accennato, ma penso che come tutte le idee considerate semplici in realtà sono anche molto complesse, quelle di far andare in comune accordo le leggi con le innovazioni, cioè fare un salto che può sembrare semplice nel dirsi, ma difficile nel realizzarsi. Sappiamo perfettamente che le cose difficili sono quelle che devono portare ad una certa sfida il nostro Paese. Credo, che non ci si possa permettere il lusso di avere ulteriori blocchi nella ricerca e nella innovazione perché siamo un Paese che non facendo ricerca, corre il rischio di far diventare le nostre imprese delle

(4) Presidente Fondazione Italiana Nuove Comunicazioni

semplici officine. Dobbiamo avere l'ottimismo e la speranza che questa inversione di tendenza ci possa essere. Allora, non vorrei ingabbiarmi fra queste due grosse tematiche che sono in contrapposizione ma proprio per tale motivo credo che le stesse ci debbano aiutare a trovare un nuovo modello di pensare e organizzare questa privacy in modo tale da essere anziché un freno eventualmente uno stimolo ad un accordo a monte e non a valle. Io ho terminato questo primo intervento.

Stefano Rodotà⁽¹⁾

Honoré de Balzac, nel 1844, scrive un libro, *Modeste Mignon*, abbandonandosi ad un certo punto ad una vera e propria invettiva: “cercate di restare nascoste, povere donne di Francia, cercate di non intrecciare neppure la minima relazione sentimentale nel cuore di una civilizzazione che rende note sulle piazze pubbliche le ore di partenza e di arrivo delle carrozze, che conta le lettere, che le timbra nel momento in cui vengono impostate e nel momento in cui vengono distribuite, che dà un numero alle abitazioni e che crea un catasto degli immobili”. Oggi, a 160 anni di distanza, possiamo sorridere di queste cupe previsioni. Ma che cosa accadrà se, tra vent'anni, qualcuno leggerà taluni dei rilievi critici contenuti nelle Relazioni del Garante? Troverà sciocche le preoccupazioni manifestate da questa istituzione, perché perché tutto ciò che la inquietava è ormai divenuto dato di realtà?

Carlo Formenti ha già ricordato la frase di Scott Mc Neal: “Voi avete zero privacy, rassegnatevi”. Si può aggiungere, tra le mille citazioni possibili, quella tratta dal film *Nemico Pubblico*, dove ad un certo punto si dice: “Voi non avete più privacy, l'avete solo nella vostra testa e forse neppure in quella”. Ma, se questo è uno scenario che i dati e le riflessioni di questo convegno rendono realistico, quali sono le vie d'uscita?

Il 10 ottobre in quel luogo singolare che è la Camera dei Lords, si è discusso dello spamming. Uno dei Lords ha preso la parola ed ha raccomandato al Primo Ministro di combattere l'invasività della posta elettronica non desiderata favorendo “il ritorno alla corrispondenza epistolare, possibilmente manoscritta”. Questo vuol dire che solo la regressione tecnologica ci può salvare?

Evidentemente no. Tenendo sul mio comodino il libro di Balzac, e chiedendomi sempre chi sa che cosa diranno di noi tra qualche anno, credo tuttavia che il tema del futuro della privacy non sia un semplice problema di previsioni più o meno azzeccate su questo o quello strumento tecnologico, ma una questione culturale. In tutti i suoi documenti il Garante ha messo in evidenza che la forte protezione dei dati personali incarna, prima ancora di una decisione legislativa, una scelta sociale, una grande e impegnativa decisione politica.

(1) Presidente Garante per la protezione dei dati personali

Già prima dell'11 settembre, nel 1999 e nelle stesse settimane, due grandi settimanali, *Time* e *Der Spiegel*, riflettono sulle grandi raccolte di dati a fini commerciali e fanno due copertine identiche, parlando di "fine della privacy". La privacy, dunque, costituirebbe solo una parentesi della modernità, tra il villaggio tradizionale e il villaggio globale.

Una tesi suggestiva, ma poco fondata. È vero, e lo dico per esperienza diretta, che a metà del secolo passato, e oltre, nelle piccole città di provincia il controllo sociale era assoluto. Ma nella folla solitaria delle grandi città vi erano sicuramente indifferenza e abbandono sociale, però anche sottrazione all'occhio indiscreto, allo sguardo indesiderato. Ora sembra che si stia tornando alla situazione del villaggio, e tuttavia il paragone risulta improprio perché il controllo si estende ben oltre l'attenzione per le vicende minute, abbraccia un orizzonte che ci fa apparire inadeguata la stessa parola "privacy".

Siamo di fronte ad una dimensione fondamentale della libertà dei contemporanei, di cui dobbiamo cogliere il senso poiché essa investe il nostro modo d'essere e la nostra identità, fatti come ormai siamo di un doppio corpo, uno fisico ed uno virtuale. Questo convegno, fin dall'inizio, ha messo ben in evidenza come queste due dimensioni, che si pensavano del tutto separate, si stiano in questo momento congiungendo in una *mixed reality* che ci restituisce il vero corpo del cittadino.

È da qui che dobbiamo partire, perché siamo di fronte ad una mutazione antropologica e sociale. E, se riflettiamo su questi temi nell'ottica di una democrazia, sappiamo che la democrazia si è costruita anche su rinunce. La Magna Charta, nel 1225, contiene una promessa del Sovrano: "non metteremo né faremo mettere la mano". È la nascita dell'*Habeas Corpus* fondato, come ben si vede, su una rinuncia. La rappresentanza democratica nasce all'insegna della formula "No taxation without representation": la possibilità di continuare ad avere denaro dai cittadini è pagato dal Sovrano con la rinuncia ad un potere politico assoluto. E un altro dei grandi passaggi storici, strettamente legato all'*Habeas Corpus*, è la rinuncia alla tortura, che pure era (e purtroppo continua ad essere considerato) uno straordinario mezzo proprio per acquisire informazioni.

Da queste rinunce nascono la civiltà moderna e la democrazia. Ma questa riflessione non si chiude solo in uno sguardo sul passato. Obbliga a considerare il presente ed a guardare al futuro, poiché vi sono rinunce tecnologiche necessarie per salvaguardare i valori fondativi dei nostri sistemi; altrimenti, in nome di una trasparenza sempre più estesa, non sarà in pericolo soltanto la vita privata, ma la stessa libertà individuale e collettiva.

Ma continuiamo a sentir dire che il buon cittadino, chi non ha nulla da nascondere, non può temere le raccolte dei dati personali, per ampie che siano. Attenzione, "L'Uomo di vetro" è immagine nazista e dietro di essa si cela la pretesa dello Stato di

saper tutto su tutti. Se qualcuno chiede rispetto e riservatezza, immediatamente diviene colui che ha qualcosa da nascondere, si trasforma in cattivo cittadino, sul quale ogni investigazione è legittima. Al fondo di questa deriva s'incontra la Stato totalitario.

L'esperienza del Garante ci mostra quanto sia diffuso un bisogno dei cittadini di una sfera privata riservata, perché solo così è possibile salvaguardare la dignità, ottenere rispetto, non essere discriminati, esercitare in condizioni di libertà i diritti fondamentali. Siamo ben al di là del piccolo egoismo, della grettezza riuol tener nascosta qualcosa a qualsiasi costo. E vi è quasi un dato antropologico di cui dobbiamo tenere conto.

Il fatto che siamo in presenza di una dimensione della libertà è ormai riconosciuto dalla Carta dei Diritti fondamentali dell'Unione europea, ora parte del progetto di Trattato per una Costituzione europea, dove vengono fatte due operazioni. La protezione dei dati personali viene riconosciuta come diritto autonomo e distinto dalla tradizionale tutela della vita privata e familiare. La protezione dei dati personali viene menzionata per ben due volte, nella prima e nella seconda parte del Trattato, ed agganciata all'esistenza di una autorità indipendente di garanzia. Il programma politico e la scelta istituzionale sono nettissimi, riflettono una consolidata consapevolezza sociale, individuano un valore non eliminabile.

Attraverso la tutela della privacy si disegna così il modo in cui ciascuno sta in società, entra in rapporto con gli altri, con le istituzioni pubbliche, con il sistema delle imprese, senza che ciò pregiudichi i suoi spazi di libertà e di intimità. Tutto questo, inoltre, esige un pieno rispetto della dignità di ciascuno. Riflettiamo, ad esempio, sull'annunciato ricorso alla tecnologia Rfid, alle etichette "intelligenti", ai microchip impiantati sotto la pelle che, usati come carte di pagamento insieme alle etichette sulle merci, consentirebbero di passare nel giro di pochi secondi alla cassa di un supermercato con un carrello strapieno di prodotti. Ma possiamo ritenere socialmente accettabile, pur di non aspettare qualche minuto, addirittura una modifica del corpo che può poi essere seguita da interventi sempre più invasivi?

Diventa chiaro, allora, che dobbiamo costruire una cittadinanza che incorpori pienamente il valore della persona nella sua particolare proiezione rappresentata dal trattamento dei suoi dati. Questo è il punto essenziale, anche perché si arriva alle radici dell'eguaglianza, al diritto di non essere discriminato attraverso uno scrutinio continuo delle mie abitudini, attraverso profili individuali incessantemente prodotti. Si tratta, in definitiva, di determinare quali siano le condizioni di legittimità in base alle quali soggetti pubblici e soggetti privati possono raccogliere, trattare e scambiarsi i dati. E questo esige sottolineatura della necessità di una base legale rigorosa per il trattamento dei dati personali, che dia rilievo alla consapevolezza individuale e collettiva, a requisiti di legge rigorosi e ad un consenso effettivamente libero ed informato, alla possibilità di "chiamarsi fuori".

Devo mantenere il governo di me. Poter decidere liberamente a che ora esco di casa, come mi vesto, in che direzione mi muovo. Poter prendere decisioni sul mio corpo fisico ed elettronico. Poter stabilire, ad esempio, che alcuni dati sulla mia salute non debbano essere contenuti nella carta elettronica che mi viene rilasciata, assumendomi consapevolmente il rischio di tale scelta. Devo mantenere una capacità di governo.

Carlo Massarini

Allora, intanto apro e chiudo velocemente una parentesi con il prof. Rasi. Mentre il Prof. Rodotà parlava pensavamo che poi in fondo il villaggio, quello antico, quello in cui tutti sapevano di tutti aveva qualche vantaggio, però, in fondo, no ? Cioè ci si aiutava, si era solidali, ci si tenevano i figli, ci si raccontavano le cose. Ormai è roba del passato. Ma insomma, anch'io vengo da una città di provincia, qualche piccolo vantaggio insomma nel quartiere, ancora a Roma ce ne sono tante di zone del genere. Trovo molto interessante, molto affascinante, la sua considerazione sul corpo fisico e corpo virtuale, i diritti del primo e i diritti del secondo. Questa mi sembra veramente, forse in assoluto, la sintesi di quello a cui andiamo incontro. Però prima, poi di continuare a far girare la parola volevo far solo, visto che parlava di Magna Charta, in qualche maniera di Costituzioni europee che tornano indietro di diverse centinaia di anni. Siamo sempre in questa fase di scontro/confronto con gli Stati Uniti, per quanto riguarda la privacy? So, insomma, che questo negli ultimi anni è stato un tema molto forte. Gli Stati Uniti sono più aperti alla concessione dei dati, al far circolare questi dati, hanno una società basata sul outsourcing, quasi tutte le grandi aziende danno in outsourcing i propri dati da gestire. Si parlò molte volte anche di vendita di dati, no? Cioè di Società che chiudevano dando in eredità, oltre al loro bilancio, anche i dati dei loro abbonati ecc... Siamo sempre in questa fase di scontro?

Stefano Rodotà

Non voglio sdrammatizzare, ma dare qualche indicazione per mostrare come effettivamente si evolvano le situazioni. Alla fine dell'anno scorso, il Senato degli Stati Uniti, ha votato, 95 a favore e zero contro, un *Genetic Non-discrimination Act*, una legge fortemente protettiva delle informazioni genetiche. È importante che questo segnale venga dagli Stati Uniti, con un radicale divieto per datori di lavoro e assicuratori di ogni utilizzabilità dei dati genetici delle persone. Perché i dati genetici sono quelli più bisognosi di una tutela rigorosa e perché gli Stati Uniti hanno sempre manifestato forti riserve verso il ricorso allo strumento legislativo in queste materie. Te-

niamo conto del fatto che il mondo imprenditoriale era interessato all'utilizzazione dei dati genetici e che tuttavia il Senato ha scelto una via diversa partendo da una constatazione concreta. L'offerta gratuita di test di cancro al seno era rifiutata dal 30% delle donne. Perché? Perché temevano che le informazioni raccolte potessero finire nelle mani dei datori di lavoro, con rischi di licenziamento o di mancata assunzione, o degli assicuratori, con rischi di rifiuto di stipulare la polizza o di richiesta di premi esorbitanti. Poste di fronte ad una scelta "tragica", mantenere vantaggi economici o tutelare la salute, quelle donne hanno deciso drammaticamente di sacrificare quest'ultima. Una forte tutela dei dati personali restituisce ad esse una condizione di libertà e la pienezza di un diritto fondamentale come quello alla salute.

intervento esterno

È una correzione di rotta?

Stefano Rodotà

Non è una correzione di rotta in via generale, ma una correzione importante rispetto alle pretese del mondo imprenditoriale. Nelle materie legate alla sicurezza le limitazioni rimangono forti: basta pensare alle richieste riguardanti il trasferimento all'amministrazione americana dei dati dei passeggeri delle linee aeree che viaggiano verso gli Stati Uniti ed alla esclusione, per questi ultimi, della possibilità di ricorrere alle corti statunitensi contro eventuali abusi. Questo vuol dire che esiste una cultura della giurisdizione capace di intervenire severamente in specifici casi. Tuttavia, il modello legislativo europeo appare oggi più idoneo per fondare una tutela forte, generalizzata e preventiva per i dati personali. E poiché, parlando di dati personali, ci riferiamo a dati ormai destinati ad una circolazione planetaria, diventa sempre più chiaro che siamo di fronte ad una competizione tra modelli: il modello dell'Unione Europea e il modello americano. Quale dei due modelli si imporrà nei prossimi anni come regola planetaria della circolazione dei dati? Qui è la sostanza della questione.

Carlo Massarini

Ecco questa in sintesi la questione. Abbiamo ancora un 10/15 minuti a nostra disposizione. Quindi io provo a fare qualche domanda su quelle che mi sono sembrate alcune delle considerazioni più interessanti e vediamo, magari con delle rispo-

ste sintetiche, di toccare più punti possibili. Intanto chiamerei in causa il Ministro. Il Ministro in una sua vita precedente è stato anche presidente dell'Ibm che è una grande Azienda americana e mi aggancerei a una considerazione di Rodotà sui modelli diversi del mondo imprenditoriale e del mondo pubblico. Vorrei provare con Lei a vedere se si può fare un parallelo del genere in Italia: c'è in Italia una differenza fra aziende e pubbliche amministrazioni nei confronti della sicurezza, per quanto riguarda la privacy, secondo Lei?

Lucio Stanca

Certamente vi sono delle differenze nell'atteggiamento, come ho detto prima, a proposito delle norme. Anche se il valore della privacy è nato e si è sviluppato nella cultura anglosassone, credo che la società americana sia più avanzata nell'accettazione di queste tecnologie. Nella comprensione del loro valore. Negli Stati Uniti e in molti altri Paesi, è stato pienamente compreso che le tecnologie dell'informazione e della comunicazione sono lo spartiacque tra passato e futuro nel modo in cui lo sono state altre innovazioni come il vapore o l'elettricità. Sono tecnologie che rappresentano un elemento del vantaggio competitivo e, quindi, del processo di creazione e di distribuzione della ricchezza. Toccano tutti i settori economici, incidendo significativamente non solo sugli aspetti produttivi, ma anche su quelli sociali.

Quindi il discorso, ripeto, non può essere assoluto. La complessità della democrazia sta nel combinare vari bisogni, vari diritti, che in diverse circostanze sono in conflitto fra di loro. Quindi se impostassimo il discorso in termini assoluti potremmo magari mettere tutti d'accordo in questa sala. Poi però questo tema, impostato in termini assoluti e astratti, deve essere calato in un contesto reale, quotidiano, con esigenze diverse. E quindi è necessario trovare il migliore equilibrio, come accade nelle democrazie più avanzate. È stato fatto un riferimento all'outsourcing. Dobbiamo considerare che le nuove tecnologie modificano l'organizzazione del lavoro. Posso avere l'ufficio della contabilità al piano di sotto o a migliaia di chilometri di distanza, non fa alcuna differenza. Dunque i modelli organizzativi cambiano grazie alle nuove tecnologie: siamo più flessibili, abbiamo più opzioni. Chiaramente, allora, bisogna combinare lo sviluppo di un'economia mondiale, compresa l'esigenza di creare benessere, con specifiche necessità che ne costituiscono una risorsa, per esempio, quella del trasferimento dei dati e delle informazioni.

Queste sono le grandi scelte che non possono essere in alcun modo essere rigide. Nell'intervento del presidente Rodotà, che considero persona di grandissima esperienza e conoscenza, mi ha però colpito la parola "rinuncia". Si tratta di rinunciare alle opportunità delle nuove tecnologie o si tratta di introdurre delle garanzie?

Al termine “rinuncia”, mi è venuta in mente subito l’energia nucleare. Pur di fronte all’immane pericolo di usare l’energia atomica per costruire armi di distruzione di massa, comunque l’uomo ha deciso un suo uso per fini positivi, di produzione dell’energia. È difficile immaginare un cittadino che preferisca non entrare in una banca dotata di telecamere, se queste sono un deterrente per le rapine. Le persone non rimangono a casa per paura delle “registrazioni” della loro presenza sulle strade, ma perché temono per la loro incolumità. Del resto importanti successi nella lotta al terrorismo e alla criminalità sono stati conseguiti grazie anche ad un’attività di “intelligence” che ha fatto buon uso delle nuove tecnologie. Questi sono i problemi quotidiani. Se devo recarmi in banca, e ne sono personalmente convinto, scelgo una banca che ha delle telecamere, perché riduce eventuali rischi di rapina, ovviamente non in termini assoluti. Quindi è una protezione, la “pretendo” come protezione personale, anche se ciò implica una videoregistrazione.

Allora: dove sta il crinale, in questo caso? Il punto è: o rinunciamo ai benefici delle nuove tecnologie o garantiamo gli utenti. Il crinale sta, secondo me, nella garanzia sull’uso di alcune informazioni, che devono essere gestite solo da chi è garante della democrazia. Prima, per esempio, Lei ha fatto riferimento al traffico telefonico: credo che nessuno possa discutere sul fatto che bisognerebbe tenere registrati i dati di traffico telefonico. Il problema è: chi deve usare questi dati e in quali circostanze devono essere usati. Ripeto: non si tratta di rinunciare, ma di garantire.

Carlo Massarini

Ed altri in intervento esterno: Questo è quello che Lei diceva a noi in assoluto ma relativamente ai singoli casi.

Lucio Stanca

Per quanto riguarda la libertà personale come concetto assoluto, siamo tutti d’accordo che sia la più ampia possibile, ma dobbiamo tenere in considerazione l’autorità dello Stato. Dove finisce l’una, comincia l’altra. La libertà del cittadino e quella dell’autorità dello Stato: questo equilibrio definisce la democrazia. Mi ha colpito il dibattito in Italia sugli Sms inviati in occasione delle ultime elezioni amministrative. Apprezzo il riserbo espresso ieri dal presidente Rodotà, perché vi sono stati reclami che verranno valutati, ma personalmente, in quanto autorità politica, devo esprimere un’opinione. Un organo istituzionale ha inviato non un messaggio elettorale, ma un’informazione circa gli orari di apertura dei seggi. Nella cir-

costanza di una novità, perché i seggi anziché essere aperti solo di domenica, come di consueto, in questa occasione erano aperti anche il sabato, per poter esercitare, con più comodità, se mi è consentito il termine, il diritto di voto. Rivolgo una domanda: se avessimo ricevuto una lettera, anziché un messaggio Sms ci saremmo chiesti se fosse stata violata la privacy? Invece è stata usata un'altra tecnologia, anziché la carta, il telefono. E ciò ha provocato la reazione a cui abbiamo assistito, e non parlo qui di posizioni ideologiche, politiche o strumentali, che in questo caso non ci interessano. Perché siamo abituati a considerare il telefono come uno strumento per una comunicazione che i tecnici definiscono "one-to-one", da una singola persona a un'altra singola persona; uno strumento confidenziale e privato. Ma questo è il telefono, nel suo uso più tradizionale e "storico". A quel tipo di modello di conversazione telefonica vocale si è aggiunta oggi una piattaforma diversa: la tecnologia mobile. Che consente una sorta di "broadcasting", cioè la comunicazione da una persona a molte persone, "one-to-many".

In un futuro prossimo, molto vicino, i Comuni potranno usare, per esempio, questa tecnologia per informare sulla situazione del traffico di un rione, o per inviare un avviso di interesse per la collettività. Vi domando: ritenete che questo tipo di comunicazioni rappresentino un'invasione della sfera personale o la fornitura di un servizio di pubblica utilità ai cittadini? In situazioni di emergenza o di informazione su eventi di rilevanza istituzionale, come l'informazione su un orario di apertura di un seggio, stiamo parlando di violazione della privacy? Certo la nostra sensazione del telefono come uno strumento di uso personale, individuale, confidenziale ci porta a reagire anche negativamente, ad avere un riflesso condizionato. Ma oggi la tecnologia è cambiata, e quindi può essere utilizzata per avere informazioni di pubblica utilità o di emergenza. Penso che questo esempio illustri concretamente il relativismo di cui parlavo: condizioni storiche di maturazione, di percezione, di familiarità anche con le tecnologie, che vanno affrontate e gestite con estremo equilibrio e, ripeto, senza generare inutili e dannosi allarmismi.

Concludo: sono 34 anni che mi occupo di queste tecnologie e mi viene da "sorridere" quando purtroppo sento citare con preoccupazione, come è accaduto anche in questa sede, lo studio del "chip" sottopelle per evitare le code al supermercato. Credo che dobbiamo avere un minimo di rispetto per la nostra intelligenza, a meno che non vogliamo veramente disegnare un mondo in cui non ci riconosciamo, con ulteriori timori e preoccupazioni. Questo sarebbe davvero fuorviante e controproducente. Nessuno pensa "realmente" di impiantarsi un chip sottopelle per evitare le code: evidentemente non è questo il problema. Ma questo esempio segnala il ruolo centrale della comunicazione, che deve evitare di essere condizionata dalle interpretazioni estremizzanti e irrealistiche dell'innovazione tecnologica. Un ruolo, quello della comunicazione, estremamente importante proprio in que-

sto Paese che ha maggiore diffidenza verso le prospettive aperte dall'innovazione tecnologica. Il mio suggerimento è: non dobbiamo frenarla per paura, dobbiamo accelerarla per desiderio di conoscenza e di crescita. Grazie !

Francesco Chirichigno

Io torno al problema di come va l'economia italiana e che quindi il problema economico sovrasta sia l'Authority che la ricerca. Io ho la grande preoccupazione che freni in questo campo ci possano costringere ancora a rimanere fermi. Faccio un esempio e poi una considerazione. Per esempio la scia che noi lasciamo se abbiamo la macchina collegata al satellite, praticamente indica dove andiamo, cosa facciamo, però in cambio, ci dà la possibilità, se la macchina viene rubata, di poterla riprendere con maggiore facilità. Quindi c'è un problema di assicurazione in meno, c'è un problema di sicurezza in più, c'è un problema di un nuovo modo di concepire anche la nostra privacy. Sicuramente è una rinuncia a qualcosa per ottenere nel sistema paese di più. Allora, quindi rilancio l'idea, cercare di fare andare d'accordo ricerca e privacy, a monte e non a valle. Non fermiamo l'innovazione, non fermiamo la tecnologia, perché faremmo nient'altro che un piacere a tutti coloro che desiderano un'Italia piccola. Dobbiamo guardare avanti, adottare soluzioni innovative, ma progredire. Grazie per l'ascolto.

Carlo Massarini

Mancano pochi minuti alla chiusura dell'ora a nostra disposizione. Concluderei allora con una considerazione su questo tema, citato da Rodotà e ripreso dal Ministro: quali sono le rinunce da fare da parte della democrazia, e quanto vale la pena cedere in privacy per avere, in cambio, garanzie in sicurezza?

The background of the cover features a faint, light blue circuit board pattern. A prominent, darker blue diamond shape is centered on the left side, partially overlapping the circuit lines. The overall design is clean and modern, with a focus on technology and structure.

Conclusioni

**LA RINCORSA TRA REGOLE
E TECNOLOGIA**

DI CARLO RUBBIA

CONCLUSIONI

Gaetano Rasi

Credo che il successo di un Convegno stia soprattutto nell'aprire un dibattito per un altro Convegno. Ci siamo riusciti in pieno ed io ringrazio proprio tutte le voci che si sono confrontate così ad alto livello. Ringrazio inoltre tutti coloro che dall'interno del nostro Ente hanno contribuito a realizzare il programma del convegno sia nella fase preparatoria che nella logistica.

Qui ora abbiamo uno scienziato dello spessore del prof. Rubbia, vanto del nostro Paese, che ringraziamo per la sua presenza e per il suo contributo ai nostri lavori. Egli concluderà il Convegno.

La parola al prof. Rubbia. Grazie

La rincorsa tra regole e tecnologia

Carlo Rubbia⁽¹⁾

Vorrei concludere questa riunione molto rapidamente anche perché moltissimo è stato detto sul tema di oggi, e le discussioni sono state ampie, chiare e conclusive su tutta una serie di argomenti, quindi di fatto c'è poco da aggiungere su questo tema.

Quindi, soprattutto tenendo conto che non sono una persona esperta del campo, vorrei esporre rapidamente alcuni punti che mi sembrano importanti, e che vale la pena che siano considerati: non rappresentano un'analisi o un commento a quello che è stato detto, ma piuttosto un punto di vista su quello che si potrebbe dire e fare sul tema.

Vorrei far osservare che la tecnologia, che sta cambiando così rapidamente, con tutte le conseguenze che conosciamo, può sembrare sotto certi aspetti quasi un gioco, ma in realtà, in certi casi e in talune condizioni, può generare dei problemi per gli individui. Questa è un pò l'impressione che si ha. Talvolta ci presentano delle innovazioni tecnologiche con il sorriso di chi è convinto di proporre delle cose buo-

(1) Premio Nobel per la Fisica. Presidente Enea

ne, ma qualche volta questo sorriso si può anche tramutare in qualcos'altro e diventare problema, fatica, paura, sofferenza.

Essenzialmente ciò deriva dal fatto che noi ci troviamo di fronte ad un mondo che si evolve sempre più rapidamente, anche se i principi di base sono sempre gli stessi, un mondo nel quale le cose si realizzano sempre più velocemente e, avendo stabilito nuove regole del gioco, ci sono delle implicazioni sul modo in cui reagire e procedere.

A proposito della cosiddetta "privacy" dei dati personali vorrei richiamarmi all'immagine tradizionale delle *guardie e dei ladri*. Oggi abbiamo ancora delle guardie e dei ladri con le stesse regole, con gli stessi meccanismi di base, soltanto che il tipo di cassaforte è cambiato, ed anche il modo di vuotare la cassaforte è fundamentalmente cambiato. Ed evidentemente quello che rimane costante in tutto questo discorso è l'esigenza di proteggere i dati. I dati rappresentano sempre l'elemento di base del problema che si può riassumere in alcuni punti molto semplici.

Anzitutto va detto che l'informazione ha un valore specifico ben preciso. E l'alterazione dell'informazione può distruggere il valore contenuto nell'informazione stessa. Oggi, con i nuovi sistemi informatici è possibile l'accesso al dato e la sua copiatura senza lasciare traccia. Vi è quindi una situazione diversa rispetto al passato. E un altro punto importante della realtà di oggi, che è diverso dal passato, è che in effetti il valore di un oggetto può non essere associato al suo valore fisico. Cioè il valore della cosa non è l'oggetto, non è la cosa. In fondo ci eravamo abituati anche a questa situazione con l'introduzione delle banconote. Una banconota da 100 Euro non possiede un valore fisico di 100 Euro. Una volta l'attuale banconota da 100 Euro era fatta da un pezzo d'oro, del valore fisico di 100 Euro. Adesso le cose non funzionano più così. Lo stesso tipo di meccanismo si applica a tutta una serie di situazioni che sono associate a vari tipi di tecnologia di cui abbiamo bisogno. E quali sono le regole di base di questa nuova struttura logica, di questo nuovo approccio? Sono due. La prima è la necessità di fare ampio uso di sistemi di codifica: il biglietto di banca deve essere riconosciuto come valido; e poi la necessità di dotarsi di capacità di autenticare. E nella codifica bisogna tener conto che l'informazione che diventa confidenziale va protetta, e questo implica anche la necessità di evitare copie non autorizzate, e occorre limitare la diffusione dell'informazione - che ha un suo valore - con accessi che siano ristretti, limitati e codificati. E poi, evidentemente vi è la necessità di proteggere l'autenticazione, come dicevo, una volta fatta la codifica, in modo che l'autenticazione sia scritta all'interno di ciò che dobbiamo leggere.

A tale riguardo esistono molti aspetti diversi. Ci può essere un'autenticazione fisica, ad esempio per identificare una persona. Abbiamo la carta d'identità, con la fotografia, ci confrontiamo: questo è un atto di autenticazione. C'è la codifica scritta nel documento, diciamo del passaporto, e c'è l'autenticazione fisica. Que-

sta operazione può diventare molto più complessa: si può pensare ad una *card*; per esempio, l'autenticazione personale può essere effettuata in tanti casi, per consentire l'accesso ad un sistema, per firmare una transazione e così via. Quindi, essenzialmente l'autenticazione di una firma può essere utilizzata ad esempio per una transazione, per evitare la duplicazione della transazione, per identificare in maniera univoca l'autore di un messaggio, per limitare l'accesso all'informazione e per proteggere l'informazione contro le cose non autenticate. E nel convegno di oggi questo discorso "di guardie e ladri", che fundamentalmente si coprono attraverso tutta una serie di tecnologie, è già stato discusso abbondantemente: non vi è dubbio che la tecnologia attuale ci permette di fare delle cose estremamente innovative. In cinque anni si dice che, almeno nei Paesi sviluppati, la spesa al supermercato si farà senza avere una cassiera perché ci sarà un gran numero di oggetti che saranno dotati di dispositivi "smart". Ciascuno avrà il suo codice di trasmissione che è lo sviluppo del codice a barre, che conosciamo già oggi, sviluppato ultimamente, e questo codice a barre, controllerà tutto il vostro carrello con tutto quello che avete comprato, farà la somma e scriverà la somma totale andando a contare ciascuno degli elementi. Io personalmente non vedo un problema etico, morale in tutto questo. Vedo una grande semplificazione, e vedo un grande problema: il fatto che la cassiera non avrà più lavoro. E questo è veramente la preoccupazione della tecnologia, cioè il rischio che di fatto certe attività diverranno inutili. Ci troveremo di fronte a degli *illetterati tecnologici*, che si aggiungeranno agli illetterati tradizionali. Saremo nella situazione, in cui il non sapere - per esempio come navigare in Internet - sarà equivalente ad essere un illetterato tecnologico, che nella società attuale è come non sapere né leggere né scrivere.

La protezione del dato è, come dicevo, una cosa assolutamente fondamentale e si basa sostanzialmente su una situazione che è particolarmente interessante perché, come dicevo, è un confronto, una sfida tra coloro che tutelano o che creano il valore, proteggono l'informazione, e coloro che la vogliono, come dire, recuperare. L'efficacia di un sistema informatico protetto è fundamentalmente determinata dall'anello più debole, da quello che è meno sensibile. Quindi un elemento debole di questo sistema può bloccare tutto il sistema. È chiaro che si tratta anche di un problema molto più vasto.

Vorrei sottolineare che, in un certo senso, l'evoluzione tecnologica è anche pilotata da un gioco, direi quasi divertente. Da una parte, dai competitori ufficiali, che scrivono le regole: il banchiere che impone regole di accesso basate su codici informatici, mentre una volta si entrava con la chiave; e dall'altra parte gli hackers, che sono l'equivalente moderno degli antichi ladri che cercano di imbrogliare, che realizzano dei virus, che elaborano dei sistemi, che cercano di combattere le regole.

Quindi c'è questa lotta eterna tra il bene e il male: in questo quadro ci sono

delle persone che vogliono proteggere e difendere i dati ed altre persone che vogliono rubare, impadronirsi di qualcosa che non appartiene loro. Tutto avviene in modo virtuale, e con la velocità della luce attraverso tutto il sistema globale, attraverso Internet. E quindi questo mercato della protezione dei dati è in continua evoluzione, e non è e non sarà mai a regime. Perché il valore aggiunto della difesa del sistema è misurato tra la tecnologia dell'azienda di produzione dei dati e la tecnologia, privata, pirata. Poiché l'obiettivo del pirata è quello di appropriarsi della tecnologia dell'azienda di protezione dati, c'è questo gioco nel quale uno deve essere sempre davanti all'altro ma non sa che se si ferma è perduto.

Ci sono tre, quattro, cinque sistemi che sono utilizzati in questa cosa. C'è la crittografia, che utilizza diversi algoritmi. Ricordiamoci ai vecchi tempi della guerra mondiale quando si doveva avere il codice per capire cosa facevano i sottomarini tedeschi, o cosa facevano i sistemi americani. Erano cose che potevano veramente cambiare il corso di una guerra. Ora, si utilizzano sistemi sempre più avanzati di crittografia, che tra l'altro è una scienza, una grande scienza, nella quale si sono cimentati anche grandi matematici che hanno dato contributi importanti. Si stanno facendo in questo campo enormi progressi. Oggi abbiamo crittografie a 16 bit, a 24 bit, a 64 bit. Ci sono anche dei problemi, evidentemente, su come si devono considerare queste crittografie. Per esempio gli oggetti hardware crittografici in America hanno al loro interno un dispositivo che è essenzialmente controllato dallo Stato americano, da quello che sa tutto ed è in grado, in qualunque momento di andare a decodificare questo oggetto e quindi chi ha un sistema di questo genere è obbligato a dare in qualche modo la sua informatica. Certo, anche nelle cose più semplici possono esserci situazioni di questo genere. È chiaro che quando ci sono poche industrie che producono queste cose, molte volte è impossibile anche alla persona che compra quel dispositivo sapere cosa c'è dentro e l'elemento informatico e di protezione mi sembra importante. Quindi l'hardware, che può forse essere l'unico modo per proteggerci contro queste cose, deve essere un hardware che deve essere fatto in condizioni tali da non permettere questo tipo di fuga. Come ho detto la fuga dei dati è sempre il punto più debole.

Concludendo, credo che abbiamo davanti a noi un forte progresso nel campo della protezione dei dati dal punto di vista tecnologico; questa tecnologia è caratterizzata dal fatto che i clienti non vogliono essere uguali agli altri, vogliono essere diversi dagli altri perché vogliono garantire un sistema che sia incompatibile con tutti gli altri.

Noi cerchiamo la compatibilità, dappertutto. Tutti gli oggetti li vogliamo quanto più compatibili possibili, ma nella questione della protezione dei dati cerchiamo al contrario l'incompatibilità. Quindi, c'è un modo molto diverso di ragionare. E poi un altro problema è che in questa evoluzione esistono delle strutture, dei

sistemi che si devono sviluppare a medio e lungo termine. Lo sviluppo di queste cose in questa guerra tra ladri e guardie è continuo, ed è evidente che quello che conta è la nostra capacità di proseguire in questo sviluppo nei sistemi di protezione dei dati. Le grandi aziende che si occupano di questi prodotti hanno un rapporto di fiducia, se vogliamo, con coloro che poi portano avanti questo tipo di tecnologie, in quello che deve essere un rapporto continuativo, personale, fiduciario.

Noi viviamo in un mondo virtuale in cui il valore dell'oggetto non esiste più. Per esempio, prendiamo il valore di un calcolo, di un software, prendiamo un dischetto, o un programma. Qual'è il valore di questo programma? Potrebbe essere il valore del dischetto che ci siamo appena comprati? Certamente no. Deve essere qualche cosa che questo dischetto contiene, e che è un valore che è puramente arbitrario, determinato dalla domanda e dall'offerta, in una situazione completamente virtuale in cui effettivamente il vero valore non esiste.

Quindi noi passiamo da un sistema in cui i valori sono rappresentati da cose obiettive: un chilo di carne costa una certa quantità di quattrini, un chilo di pane costa una certa quantità di quattrini (questo è obiettivo, si sa che ha un valore), a un sistema in cui l'informazione, la protezione, lo sviluppo, la programmazione, il cui valore viene fissato sulla base di regole che di fatto sono totalmente arbitrarie. Ad esempio, il valore di un software sarà proporzionale al costo effettivamente sostenuto per produrlo? No, il costo dipende da quanti uno ne vende. Perché il costo di un programma, dieci programmi, cento programmi un milione di programmi è sempre lo stesso. Prendiamo il costo, per esempio, della Microsoft. Quanto vale oggi Microsoft? Non vale la spesa accumulata, divisa per il numero di copie che uno ne ha fatto, il costo rimane costante ma il numero di copie sta crescendo. Quindi è chiaramente un problema in cui usciamo da un mondo fatto di cose obiettive, reali, di vecchie abitudini ed entriamo in situazioni che sono giustamente di compravendita, ma che sono basate su dei principi completamente straordinari. Secondo me le regole del sistema, il modo di fare le cose sono totalmente diverse ed è veramente una grande partita di poker in cui molte volte non si vedono le carte e quindi in questo campo credo che la nostra industria deve essere capace e competitiva nel procedere ed evidentemente è quello che mi auguro, come anche che questo tipo di riunione non rimanga ancora una volta di più un discorso, come dire, di principi, ma che sia un modo pratico per assicurare la miglior protezione possibile e riuscire a farlo nelle condizioni più competitive possibili.

Esprimo i miei ringraziamenti a chi ha presieduto questa riunione che ritengo sia stata molto stimolante e significativa su un tema così complesso.

Grazie.

Gaetano Rasi

La protezione dei dati come sicurezza va completata con il rispetto della persona umana. Questa mi pare la sintesi di questo Convegno che, ripeto, è un Convegno che ne propone subito un altro. Nel metodo problematico sta il progresso delle idee e della consapevolezza umana.

Grazie per la vostra attenzione. Ringrazio i componenti della Tavola Rotonda che hanno innescato questa nuova problematica. Ringrazio il prof. Rubbia per le conclusioni.

A presto quindi, al prossimo Convegno. Grazie.



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Redazione

Garante per la protezione dei dati personali

Piazza di Monte Citorio, 121
00186 Roma
fax 06 69677785
www.garanteprivacy.it
www.dataprotection.org
e-mail: garante@garanteprivacy.it

Pubblicazione della

**Presidenza del Consiglio dei Ministri
Dipartimento per l'informazione e l'editoria**

Direttore: **Mauro Masi**

Via Po, 14 - 00198 Roma - tel. 06 85981

Stampa e distribuzione:

**Ufficio grafico dell'Istituto Poligrafico e Zecca dello Stato
presso il Dipartimento per l'informazione e l'editoria**



È nota la distinzione fra *crescita* economica e *sviluppo* economico, l'uno riferito all'aumento della quantità prodotta, l'altro riferito anche alla *qualità* distribuita. Gli indici dello sviluppo umano tendono ad inglobare, oltre gli elementi riferiti alla produzione, anche valutazioni riguardanti la sanità, la durata della vita, il livello di istruzione. Tutti questi aspetti aggiuntivi si giovano dei benefici derivanti dalle accelerate e diffuse innovazioni tecnologiche. Il passo ulteriore, perché lo sviluppo economico coincida con il progresso civile, è legato alla tutela della dignità dell'uomo, della sua identità, della sua libertà. L'intento di questo volume è quello di fare il punto sul rapporto tra le innovazioni tecnologiche ed il rispetto dei dati personali.