DAL CONTROLLO DELLA TECNOLOGIA AL CONTROLLO SULLA TECNOLOGIA: NECESSITÀ DI UN APPROCCIO TECNICO-GIURIDICO

SHARA MONTELEONE

Tecnocontrollo

- Tecnologie pervasive e diritti fondamentali:
  Profili di compatibilità e prospettive evolutive

- Integrazione tre diritto e tecnologie digitali nella Società dell'Informazione → es.Data Protection

- ***A legal-technical approach***

→ esigenza di rinnovare gli strumenti giuridici disponibili e di utilizzare le stesse **tecnologie come fattori di tutela**

- **Il quadro normativo di riferimento**

  - Convenzione Europea sui diritti dell'uomo del '50 (l'art. 8 riconosce ad ogni persona il diritto al rispetto della sua vita privata e familiare);
  - Convenzione di Strasburgo n. 108 dell' '81 "sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale";
  - Direttiva n. 95/46/CE, relativa alla "tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati";
  - Carta dei diritti fondamentali dell'UE di Nizza del 2000 (art. 8 sulla "protezione dei dati di carattere personale".
  - Direttiva n. 2002/58/CE "relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche"
  - Codice in materia di protezione dei dati personali (D.lgs.n.196/2003) in vigore dal 01/01/04
  - Direttiva 2006/24/CE *data retention*

Digital Rights Management system

- DRMs: insieme delle MTP e del sistema hardware e software per la gestione e il controllo delle condizioni di accesso e uso delle opere digitali

→controllo più ampio sull'accesso e sull'uso di un'opera digitale

- *previsione legislativa delle MTP e delle informazioni elettroniche*
- *limiti ulteriori alle libere utilizzazioni*

→'effetti collaterali' su privacy fruitori/utenti: **controllo 'culturale'**

- Non necessariamente incompatibili: tecnologia è neutra
- Critiche mosse non ai DRMs ma alla legislazione

→ Necessità di diversa prospettiva legislativa più rispondente alle varie esigenze:

- Protezione dei dati personali e DRMs compatibili

Provv. n.104 del 18/01/2005 **Gruppo dei Garanti europei**

- ✓ Identificabilità continua del fruitore
  - ✓ uso di Identificatori Univoci
- ✓ Tracciamento e monitoraggio 'a priori' di singoli atti
- ✓ Profilazione (spesso per finalità di marketing→ regola dell'*opt-in*)

→ Esigenza di rispettare i **principi** stabiliti dalla disciplina europea (Direttiva 2004/48/CE fa salve le norme in materia di data protection):

- ✓ Principio di necessità/anonimato, finalità, trasparenza
- ✓ Norme su decisioni automatizzate
- ✓ Diritto a non essere discriminati e a non subire condizionamenti nelle scelte culturali e intellettuali

…DRMs compatibili

- Tutela privacy degli utenti:
  limite al potere di controllo delle informazioni digitali
  →(es. sanzioni all'uso di MTP che comporta il trattamento occulto di dati personali)

Soluzioni:

→ Sviluppare strumenti tecnici per minimizzare l'impiego di dati personali

→ Incorporare il bilanciamento di interessi nei DRMs

→ Architettura dei DRMs privacy-oriented, più flessibili

- Trattamento dei dati on-line e raccolta invisibile

  ***Cookies*, *files* di *log*:**

  → *Rischio di* monitoraggio e profilazione utente a fini commerciali

  → Divieto di utilizzare la rete di comunicazione elettronica per accedere alle informazioni archiviate nei terminali(Art 122);

  → deroghe con il consenso informato dell'interessato e entro i limiti del codice deontologico; (**art 5 Dir. n. 2002/58**)

- Necessità di contemperare **anonimato con identificabilità**: *files* di *log* e *cookies* associati a dati ricavabili dai drms
  - Anonimato protetto
  - necessario rispettare i principi fondamentali (trasparenza, proporzionalità, finalità)

- **Raccomandazione n. 2/2001 del Gruppo dei Garanti** sui requisiti minimi:
  - incoraggiare la consultazione in forma **anonima** di siti commerciali e l'uso di pseudonimi;
  - **conservare** i dati raccolti per il tempo strettamente necessario;
  - e-mail: gli indirizzi reperiti su Internet all'insaputa dell'interessato **non** sono

Dati di traffico e di localizzazione

- ***Data Retention*: limiti di proporzionalità e necessità**
  - Art 132 (modificato da l.155/05)
  - Direttiva n. 2006/24/CE
    - **Problemi: durata e autorizzazione all'accesso**

- dati relativi all'ubicazione→ possono essere trattati solo se anonimi o con il consenso dell'interessato, ***revocabile*** in ogni momento, gratuitamente e con una funzione semplice, anche in via temporanea, e per ogni collegamento alla rete

  → Libertà di scelta → possibilità di disattivare in ogni momento il meccanismo di localizzazione

- **Comunicazioni indesiderate** (comprese e-mail, sms, mms finalizzati all'invio di materiale pubblicitario):

  → regola dell'**opt-in**, consenso preventivo dell'interessato, possibilità di opporsi in ogni momento (Art.130)

Videosorveglianza (I)

- Provvedimento generale su **Videosorveglianza (29/04/'04)**:

→ 'funzioni istituzionali' (per i soggetti pubblici); obbligo di legge, sicurezza, consenso o provvedimento del Garante, per i privati (liceità)

→ escluso ogni uso superfluo; software conformati in origine in modo da non utilizzare dati identificativi o cancellarli; (necessità)

→ le altre misure sono insufficienti (proporzionalità): valutata in ogni **fase** o modalità del trattamento (dislocazione, angolo visuale, uso di zoom automatici;

→ Provv Garante (27/02/05): Illiceità di sistemi di videosorveglianza per accertare infrazioni amministrative minori;

→ gli scopi specifici e trasparenti (finalità di pubblica sicurezza ≠ profilazione a scopo promozionale)

→ Provv. (04/05/'05) Telecamere negli stadi per reiterate violenze

- **Videosorveglianza (II)**

  se il trattamento presenta “rischi specifici”(art17):

  →“**verifica preliminare**” della stessa Autorità (sistemi di raccolta di immagini incrociata con altri particolari dati personali, ad es. biometrici, con codici identificativi o con dispositivi che rendono identificabile la voce)

- digitalizzazione delle immagini e **videosorveglianza dinamico-preventiva**

  → obbligo di notificazione (se indicano la posizione geografica di persone od oggetti; se volti a definire il profilo dell’interessato) (art. 37)

  - dati **biometrici** (finora ammessi per finalità di sicurezza pubblica e privata) → illegittimi se sproporzionati e non necessari

  → Rilevazione presenze sul lavoro; utilizzo di servizio di ristorazione (Provv. 16/12/04)

  → tutela dei **lavoratori** nell’uso dei sensori: divieto di controllo a distanza

Ubiquitous computing

→ pervasività **funzionale e spaziale**; trasparenza e web presence;

- Problemi in termini di tutela dei diritti fondamentali derivano da:
  - **Wireless Communication** (presuppone la presenza di sensori collegati tra loro da una rete ad hoc);
  - **Ambient Intelligence** per l'identificazione e la localizzazione di persone e oggetti;
  - **Contenuti multimediali** virtuali
  - **Miniaturizzazione** degli apparati tecnici

- Determinante il **contesto** in cui le tecnologie vengono impiegate (campus universitario, aeroporto, museo, laboratorio di restauro)

- Necessario rivisitare gli attuali standards e le architetture tecnologiche **per preservare** il diritto alla privacy

  - Es. realizzare l'anonimato protetto degli identificatori
    → associazione con l'utente solo successivamente

Rfid ed etichette intelligenti

- Impiego: logistica, anticontraffazione, documenti di viaggio e…?

  - Controllo sui prodotti si estende ai consumatori
  - Possono contenere microchip per elaborazione dei dati
  - Pericolo di riscrittura dell'etichetta da parte di terzi

  - ✓ Provv. Garante 09/03/2005 su Rfid:
    - Prescrizioni contro forme indebite di controllo
    - Rischi dall'adozione di standards comuni
    - Realizzare a livello tecnico **l'esercizio dei diritti**

      → Garantire la visibilità e la possibilità di **disattivazione**

- Videosorveglianza, Ubiquitous computing, Rfid

  - Società della “Conoscenza”

  → condizionamento delle scelte individuali e collettive

  - Necessità di relativizzare la tecnologia

  - Far rispettare i principi di necessità e proporzionalità, del consenso informato e della trasparenza

  - Tecnologie ‘**conformate’** e diffusione delle P.E.T.

    →(Relazione Com. E. 2003 sull’applicazione direttiva n.95/46/CE)

  → Incoraggiare la produzione di dispositivi *privacy-oriented* e a prezzi contenuti (es. smart cards multifunzionali)

- Verso **nuovi diritti dell'utente**

  - Diritto al **controllo del proprio terminale**
    → Scelta dei dati da inserire e quando disattivare

  - sensibilizzazione degli utenti non solo sui **diritti** ma anche sugli **strumenti tecnici** di tutela
  - ritorno al concetto originario di ***privacy,*** più ampio
    - "*dati personali"* non esaurisce le aspettative di tutela
    - Carta di Nizza → necessità di riaffermare il valore della persona

  - Terza generazione di leggi per un **approccio tecnico-giuridico**
    → Regolamentazione non esterna ma 'dall'interno'

    → Rimessa al legislatore l'individuazione dei valori alla base degli standard tecnologici, ossia i diritti e i doveri