DATA PROTECTION E COMUNICAZIONI: NECESSITÀ DI UN APPROCCIO TECNICO-GIURIDICO

SHARA MONTELEONE
INRIA Grenoble-Rhône Alpes
PRIAM Project

Privacy e DP nella Società della Conoscenza

- Data protection: esigenza trasversale per i vari settori delle comunicazioni
  - Convergenza multimediale e contenuti (videotelefoni…)
  - Flusso di dati sulle reti richiede controllo e sicurezza
- (DP e privacy: strumenti complementari per assicurare:
  - Costruzione identità e personalità senza condizionamenti
  - Capacità individuale di controllare aspetti dell'identità proiettata
- Tecnologie dell' *Era IA* pongono nuove sfide:

  → ripensare al 'right to privacy' e ritorno al concetto originario
  - Supporto alla capacità di <u>autonomia</u> degli individui:
    - Potere di scelta e riflessione autonoma senza pressioni o costrizioni
    - Capacità decisionale per la partecipazione ai processi deliberativi

Plan of talk

I) *Applicabilità ed effettività della normativa in materia di DP*

II) *Approccio tecnico-giuridico*

→ Dal controllo della tecnologia al controllo sulla tecnologia

III) *A* case study: Priam project

- **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*
  - *Proposta di modifica alla direttiva 2002/58 (nov 2007)*

- ***Tecnocontrollo*: > diffusione in vari settori dell'uso di tecnologie dell'informazione e comunicazione > flusso di dati personali**

Tecnologie pervasive di comunicazione e diritti fondamentali:

Profili di compatibilità e effettività:

- Necessity, proportionality, lawfulness, pertinence, purposes limitation, transparence
- Consenso informato
- Diritti dell'utente

DP = > controllo su flusso di dati (revocare consenso)

Ritorno a concetto primordiale di privacy rinnovato

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

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

- *Privacy Enhancing Technologies:*

interazione tra soluzioni normative e tecniche

Applicabilità in concreto (esempi):

Raccolta dati:

- **Necessity** principle → hardware and software must be made out reducing at minimum the use of identifiable data (Art 6 dir. 95/46)
- **Transparence principle** → obligation to inform of the presence of cameras and sensors (Art 10 dir. 95/46)
- **Proportionality** → Are technical devices and their functioning proportional to the purpose (to provide specific value-added services)?
- **Pertinence and not excess** → user's **tastes** can be excessive regarding the service provision
- **Purpose** → specific, legitimate purposes (that service not others)

- Traffic and location data
  - →**necessity**: erased or made anonymous when no longer needed for the transmission of the communication (except for billing aims)
  - → **subject to the consent (revocable)**, their processing is allowed for marketing purposes and for the provision of value-added services (art 9 dir. 2002/58/CE)
- *Main issue: how to assure it (erasure, making anonimous, revocable consent)?*

Criteri di validità del consenso (Art 29 WP 114, 25/11/2005)

- Presupposto: natura unilaterale

- Libertà:
  - atto positivo (diverso da principio di apparenza) e scelta genuina
  - assenza di condizionamenti, pressioni (debole)
  - Non necessitato (clausola inserita nelle condizioni generali di contratto)
- Consapevolezza:
  - informativa (Tecnologie x garantire meglio l'applicazione degli obblighi)
- Specificità:
  - Finalità determinate: manifestazione separata per fini diversi
- Forma:
  - scritta per dati sensibili (*ad substantiam*): Fr: *espresso*; it: *scritto*
    - tecnologia che garantisca l'autenticità e l'integrità del consenso (*scritto* funzionale → anche elettronica e automatizzata?)

Applicazioni ancora limitate di PET

- Carte di pagamento scalari per telefono, per acquisto programma tv: realizzano anonimato protetto (identificazione indiretta del soggetto)
  - Garante: evitare un controllo centralizzato e favorire strumenti tecnici che permettano al soggetto di selezionare/controllare i propri dati e disattivare i dispositivi di localizzazione

1) *Drms and data protection → "conformed" technologies*
2) *Cookies and log file*
3) *Dati di traffico e localizzazione*
4) *Rfid application and Ubiquitous Computing*
5) *User's control on own **terminal equipement***

- *New kind of regulation*

1) Digital Rights Management system

- DRMs: insieme delle MTP e del sistema hardware e software
  →controllo più ampio sull'accesso e sull'uso di un'opera digitale

→'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: dai rischi di violazione a nuove possibilità di protezione

- Protezione dei dati personali e DRMs compatibili

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

- ✓ Identificabilità continua del fruitore (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

- ✓ Diritto a non essere discriminati e a non subire condizionamenti nelle scelte culturali e intellettuali

- 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

- 2) Trattamento dei dati on-line e raccolta invisibile (profilazione)

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

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

  → uso con il consenso informato dell'interessato e entro i limiti del codice deontologico; (**art 5 Dir. n. 2002/58**): tecnicamente possibile (browsers Mozilla ≠ Internet Explorer)...

- Necessità di contemperare **anonimato con identificabilità**: *files* di *log* e *cookies* associati a dati ricavabili dai drms

  - **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;
    - indirizzi e-mail reperiti su Internet all'insaputa dell'interessato **non pubblici**
  - **Comunicazioni indesiderate** (comprese e-mail, sms, mms finalizzati all'invio di materiale pubblicitario):

    → regola dell'**opt-in**, consenso <u>preventivo</u> dell'interessato, possibilità di opporsi in ogni momento (Art.130)
  - Motori di ricerca: Art 29 WP148:
    - Dati non in eccesso; informativa; cancellazione o anonimizzazione; indicazioni per industrie; rispetto diritti interessato

3) Dati di traffico e di localizzazione

- Files di log
- Dati di localizzazione (GPS)

→ trattati solo se anonimi o con il consenso dell'interessato, ***revocabile*** in ogni momento, gratuitamente e con una funzione semplice anche in via temporanea

Tecnologia al servizio dei diritti→ Libertà di scelta → possibilità di disattivare in ogni momento il meccanismo di localizzazione

→ identificazione dei titolari sullo stesso display

(Conservati per esigenze investigative gravi reati (art 132)

- 4) Ubiquitous computing
  - comunicazione mobile multimediale di nuova generazione

  → pervasività **funzionale e spaziale**

  - 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)

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

- 5) Rfid ed etichette intelligenti
  - Controllo sui prodotti si estende ai consumatori
  - Pericolo di riscrittura dell'etichetta da parte di terzi

  - ✓ Provv. Garante 09/03/2005 su Rfid (Art 29 WP doc. 01/19/2005):
    - Prescrizioni contro forme indebite di controllo
    - Realizzare a livello tecnico **l'esercizio dei diritti**
      - → Garantire la visibilità e la possibilità di **disattivazione**

- 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. eu 2003 sull’applicazione direttiva n.95/46/CE):

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

→ Capacità di graduare/controllare il livello di condivisione dati

- Tecnologie per una migliore protezione:

→ Comunicaz. Comm eu sull’applicazione direttiva 95;

→ Parere Art 29 WP 150 sulla proposta di modifica direttiva 2002/58

- Verso **nuovi diritti dell'utente**
  - Diritto al **controllo del proprio terminale (spesso mobile)**
    → Scelta dei dati da inserire e quando disattivare; info su cookies
  - 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
    → Rimesso alla tecnologia (*PET*) il compito di rendere effettivi i valori
- Rafforzamento dei diritti (all'informativa, accesso, rettifica) attraverso la tecnologia (e.g. Art 29 WP 5/2004: raccomanda l'uso di caselle on-line)
  - Accesso alla *privacy policy* tramite semplice click
  - Browsers che consentono di riconoscere e impedire i cookies
  - Pics (*platform for internet content selection*) del 3WConsortium per la selezione dei siti protetti

PRIAM project: Privacy Issues in AMbient intelligence
INRIA Rhône-Alpes, France

- Partnerns: Inria (Grenoble, Lyon, Rennes)
- University of Twente
- Faculty of Law of Saint-Etienne
- Multidisciplinary projet: lawers and computer scientists

- Ambient Intelligence:
  - Ubiquitous computing / communication; intelligent user interface
  - accesso ai servizi e info ovunque; adattamento alle necessità dell'utente, miniaturizzazione dei dispositivi

PRIAM project: Nuove prospettive e sfide (per il diritto)

- Vari livelli di fonti normative (legislative, tecniche, deontologiche, sociologiche): limiti, interazioni, complementarietà;
- Bisogno di protezione effettiva: come definire applicabilità e effettività?
- Dal consenso esplicito del soggetto all'analisi dei rischi automatizzata: valore legale di un consento automatizzato

Nuove prospettive e sfide (per la tecnologia)

- Priam approach: flessibilità + responsabilità
  - Lingaggio per esprimere le *privacy preferences*
  - Combinazione di controlli a priori e a posteriori
  - Linguaggio logico-formale
  - Definizione delle responsabilità
  - Attuazione tramite procedimento automatizzato

  - Stretto legame tra diritti di privacy e tecnologia

    - Legge $\rightarrow$ modello formale $\rightarrow$ adempimento

Software agent per la privacy

- Un agente intelligente per esprimere il consenso al trattamento
  - **Compatibilità**: rispetto dei criteri di validità (libero, informato…)
  - **Efficacia** (es: l'agent puo' assicurare che il titolare invii l'informativa)

  - Ruolo dell'Autorità nell'indicare misure per rendere il software conforme alla normativa:
    - La conformità dell'agente alle indicazioni: sorta di presunzione di legittimità
  - Ruolo dei codici di condotta
    - Tecnologia relativizzata e norme adattate al contesto