PERSONAL DATA PROTECTION AND e-COMMUNICATION:

EFFECTIVENESS AND ENFORCEABILITY OF THE CURRENT REGULATION TO THE NEW SCENARIOS OF TECHNOLOGY

SHARA MONTELEONE
MICC, FIRENZE

Introduction

- Object of the research:
  - Studying the legal framework in the field of Data Protection and the enforceability/implementation issues in the sector of e-Communication;
  - Finding out possible solutions → new technologies and fundamental rights: compatibility and prospects

  - Directive n. 95/46/CE: "…the functioning of an internal market requires not only that personal data should be able **to flow freely** from one Member State to another, but also that the fundamental rights of individuals should be safeguarded";
  - Directive n. 2002/58/CE: "…The successful cross-border development of these services is partly dependent on the **confidence** of users that their privacy will not be at risk".

  - The Data Protection regulation offers a good example of **integration** between juridical and technical rules

- Summary

I) *Privacy as fundamental right and its evolution in the 'Information Society';*

II) *Legal framework;*

III) *Personal Rights protection and technological potential: a balance of interests*

IV) *A legal-technical approach: need to innovate the current juridical measures and to use the technologies as factors of protection*

I)

Right to keep the control on our personal data against discrimination and ***conditioning*** *in our decisions*

→ the exercise of the rights depends also on the aware use of the own technical equipment

Data Protection and ***e-Democracy***

→ "We can't separate the *e-Government* from the *e-participation* and there can not be *e-participation* without *e-inclusion*" (S. Rodotà 2006)

→ private life, market, politics are not necessary *in antitesi*

Need to put the person at the centre of the regulation → Chart of Nice

II) **The legal framework**

- European Convention on Human Rights 1950 (art. 8);
- Convention of Strasbourg n. 108/81;
- Directive n. 95/46/CE, "frame-directive"
- Charter of fundamental rights of the European Union 2000 (art. 7 and 8)
- Directive n. 2002/58/CE "e-Privacy"
  - Italian Data Protection Code (D.lgs.n.196/2003)
- Directive 2006/24/CE "*Data Retention"*

- *+ Soft Law → Self regulation (Code of practices) and technical rules*

III) Enforceability of the D.P. regulation: the ***Vicom project***

www.vicom-project.com

→ an architecture for **Virtual Immersive Communication Services**

possible scenario**: a campus**

→ **provision of personalized services and interaction with the environment**

Main issues:

- The system uses personal data (need to assure a fair processing)
- Wireless Communication (presupposes the presence of cameras and sensors linked each others;
- Ambient Intelligence for the identification and localization of people and objects – miniaturization of the tools;
- Multimedia Virtual Contents (enrich the reality with *ad hoc* data)

- Spatial and functional intrusion; transparence; web presence
- Need to review the technical standards and architectures in order to **preserve** the right to privacy

a) access to the campus
b) inside the campus: the provision of services

- **Fundamental principles and general rules** (supranational and national regulation)
  - Fundamental rights and freedom; personal dignity and identity (Art 2 it. Code)
  - Necessity, proportionality, lawfulness, pertinence, purpose limitation (art. 6/7, directive 95/46/CE)
- **Specific rules:**
  - Section X Italian Data Protection Code (e-Communication)
  - remedies (claim to the Garante or to the judicial authority)
  - Sanctions (civil, administrative and penal measures)

- ***a) access to the campus***
  - The student (his *personal agent*) is automatically identified, localized, driven…(on the basis of the personal data gathered at the first access)
    - **Necessity** principle → the hardware and software must be made out reducing at minimum the use of identifiable data (Art 6 dir. 95/46)
    - **Consent:** free, specific, aware (Art 7 dir. 95/46; 18 it. Code):
      - different rules if the responsible of the data processing is

      a public body (exceptions only for institutional duties

      → is it possible to talk of the Vicom services as 'institutional duties'?)

      or private subject (only in specific cases

      → services are provided by a society which processes the student's data)
    - **Transparence principle** → obligation to inform of the presence of cameras and sensors

b) Inside the campus: the services provision

b1) *the System knows the user's personal data*

- **Proportionality principle**
  → Are the use of some kind of technical devices and **their functioning proportional** to the purpose of the processing (to provide for specific value-added services)?

- **Pertinence and not excess**
  → (not pertinent data collected by a **Commune** for the investigation of crimes)
  → data related to the user's **tastes** can be excessive regarding the service provision

- **Finality**
  → specific, legitimate purposes (Garante 3/11/05 "*Telepass and free consent*")

- Data processed *contra legem* **can not be more used**

b2) *the system knows in every moment the user's position* (I)

- **Traffic and location data** (art 6,9 dir. 2002/58/CE):

  → 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

  - ***Opinion of EU Working Group (9/2004):***
  1) unlimited retention of such data is unlawful
  2) answers to a specific need (judicial purposes)

- Recent **Data Retention directive n.24/2006/CE**: new obligations

→ **available** data for the purpose of investigation, prosecution of *serious* crimes

→ retained for periods not less then **6 months** and not more then **2 years**

→ enforcement before Sept.'07 (except for Internet data, 2009)

main issues:

- ✓ proportionality and necessity of such huge retention; not authorized accesses

Opinions of EDPS (26/09/05) ***and of Art 29 WP (***25/03/06)

→ possible solutions:

- localize the user without identify him/her
- use identification data, but with previous consent
- chose 'Protected identification' (association with the specific subject only afterwards

- Freedom of choice → possibility to **defuse** the localization system

- Such processing must be **notified** to the national Authority (art 37 It. Code)

- On-line processing (the *Personal Agent* can be connected to **Internet**)

  → *cookies*, *log files*

  → **risk of hidden collection of data, monitoring and profiling for marketing purposes**

  - Art 5 dir. 2002/58/CE: they are allowed only for lawful purposes, when necessary and with the informed **consent** of the user (given in different ways)

b3) *the system uses a suitable number of sensors* (I)

- Videosurveillance Doc. Art 29 WP (02/11/2004)
- **Videosurveillance Act (Garante 04/29/'04)**: minimum requirements

Lawfulness → 'institutional duties' *for public entities*;

→ law requirement, consent, security purposes *for privates*;

Necessity → software made out *ab origine* in order to avoid identifiable data

Proportionality → the other measures are unsuitable: evaluated in every face (dislocation, visual angle, automatic zoom; interconnection of the system with others)

→ Garante (27/02/05): unlawful videosurveillance system for investigation of administrative infractions;

→Garante (15/06/04): Commune: no video-recording for promotional aims

Finality (public security ≠ profiling activity)

→ Garante (04/05/'05): Cameras in the stadium justified for repeated violence

b3(II)

- *VIT used involve a processing that presents "specific risks" (art.17 It Code)*

→ obligation to ask the national Authority for a "**previous check**"

(videosurveillance systems, matching of images and other specific data such as biometric data or ID codes of smart cards or voice identification devices)

→ also in case of digital images and ***dynamic-preventive videosurveillance***

- Specific modalities will be indicated in a Code of practice to be adopted (art. 134 It. Code)

→ administrative and criminal penalties (if there is a harm)

b3(III)

In case of software for the interpretation of gestures and facial recognition

- **Biometric data:** till now admitted for security purposes (public and private)

→ is their use ‘’proportionate’ to provide a value-added service?

- ✓ **Art 29 WP (Working doc. on biometrics 08/01/2003**)

→ Garante: *extrema ratio* (independently from the consent);

→ assiduity control at workplace; check of refectory service (Garante 16/12/04)

→ Matching of biometric data and images only if exists an effective risk and if encrypted (Garante 17/11/05, access to a Bank)

→ workers rights protection in the use of sensors**:** far control is forbidden (Garante 21/07/05,)

- (art 14 It. Code):
  - It is not allowed to adopt judicial or administrative acts based ***exclusively*** on a personal data processing aimed to the *profiling*

b IV) *offering of personalized information*

- Value-added services (suggestions on events/products of the campus etc.)

  → "**possible *spam***"?

  - not requested communications are allowed with: (art **13 dir. 2002/58/CE**)

  → previous **consent** and possibility to refuse them in every moment

  → except for similar products or services already accepted

- Realistic representation (situation in the classroom, virtual driver guide)
  → preferable **synthesized** image (not identification)

- **Virtual lesson** → software for the interpretation of the gestures made out according the mentioned principles (*anonimity,proportionality*)

A legal technical-approach

- Determinant the **contest** in which the VIT are used (campus, airport, museum, restoration lab)

- *Council of Europe Conference of Prague (October 2004):*
  → **interaction** among normative (legislation and self-regulation) solutions and technological ones (diffusion of **P.E.T**.)
- *International Conference DP Commissioners of London* (November 2006)

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

  - *Valid also for Rfid application and Ubiquitous Computing*
  - *Drms and data protection → "conformed" technologies*
  - User's rights to exercize a control on his own ***terminal equipment***

A Legal-techical approach

- I) Rfid and smart labels

  - Applications: logistic; anti-piracy; clothes, travel documents, etc

→ control on products is extended to the consumers' behaviours

→ ubiquitous microchips for the data processing: dislocation

→ risk that not authorized subjects rewrite the label

  - ✓ Art 29 WP doc. 01/19/2005; Garante 03/09/2005:
    - Indications against unlawful controls
    - Risks from the adoption of common standards
    - Realize at the technical level the exercise of **the rights**

→ Guarantee the **visibility** and possibility to **defuse** the system

- II) DRMs and data protection

  - 'Collateral effects': **cultural** control and **privacy** invasion

    - Not necessary incompatible: the technology is neutral

  → From the risk of privacy invasion to the possibility of privacy protection

  - **Art 29 WP n.104 01/18/2005**: DRMs compatible with data protection
    - Constant Identification of the user (through **Unique Identifiers**)
    - Tracing and monitoring *a priori* of single user's act → profiling

      - fundamental principles on data protection must be respected:
        → possibility to realize the 'protected anonymity' of the identifiers

    - Solutions:

    → develop technical measures to **minimize** the use of personal data

    → incorporate the privacy values in the DRMs → privacy-oriented architecture

    → "build intellectual privacy into **law** and into **code**" (J.E.Cohen, Berkley TLJ,2003)

A legal-technical approach

- "Knowledge Society"
  - loss of autonomy with regard to personal decisions

    ✓ need to make the technology relative
    ✓ Compliance with necessity, proportionality, purpose limitation, transparency
    ✓ Improve 'conformed' technologies and diffusion of P.E.T
      → EU Comm. Report on on the first pplication of the directive 95/46/CE
      → EU Comm. Communication on the diffusion of PET (05/02/2007)

- **Effective** rights of the data subject:
  - The right to not be subjected to intrusive conditionings
  - **The right to keep the control on the own terminal equipment**
    - Autonomy of decision (which personal data reveal and when defuse the system)

- Make the users aware of their rights as well of the technical solutions for the data protection → make them responsible
- Come back to the *original* concept of privacy (data protection is not exhaustive)

A legal-technical approach

- New generation of law for a legal-technical approach

  - **"Internormativité":** dialogue between the juridical and not-juridical rules (social, ethic, technical)

    → effectiveness, lawfulness, conformity (*criteria for juridical validity)*
      - Promoted by the EU doc. "better regulation" (2003)

  - **Regulation not from *outside* but from *inside* the technology**
  - The role of **law: to define the public values** (included privacy ones) that **must be taken into account in the formulation of the technical standard**

  - **Co-regulation** system: better choice (law finds effectiveness in the technical solutions and in the self-regulation ones)