



# 31

Madrid, 4. y 5 de noviembre 2019  
conferencia internacional  
de autoridades de protección  
de datos y privacidad

# Privacy: Conditions for its survival in our I.S.

Yves Poullet  
Professor Faculty of Law (Namur)  
Director of the CRID  
<http://www.crid.be>

---

PRIVACIDAD:  
HOY ES  
MAÑANA

# New Privacy threats in our I.S.

- **Imbalance of the respective powers** of those responsible for data processing on the one hand and the person concerned on the other. This imbalance can lead to all kinds of discriminations;
- **“De-contextualisation”**: the data circulating on the web were “issued” by people concerned with a precise objective, or in a particular context. The exchanges of data of all kinds and the possibilities to use search engines with any key words engender the risk of being judged “out of context”;
- **Opacity of the functioning as much of terminals (cookies, RFID) as infrastructures** (see “distributed agents” localised throughout information systems such as those known as being of “ambient intelligence”). This opacity carries the fear of unsolicited and unwanted information processing, and the motivation henceforth is to conform to a behaviour believed to be expected in these new invisible places of surveillance;

# New Privacy threats in our I.S (2).

- **Reductionism**: more and more, collected data concerning events, even the most trivial in our lives, are multiplied, and information systems analyse us via these data which reduce the choices and human beings, even our personalities, to “profiles”. In “ambient intelligence” systems where man is put on the network with all the paraphernalia of his surroundings, he becomes, at the heart of the network, a communicating object among others;

PERSON = his or her DATA (1981)= a PROFILE (NOW)

- **Blotting out of the distinction between the public sphere and the private sphere**. Man, lost in the crowd, can be followed, be traced. Inversely, even in his home, doubly locked in, he can be seen via the GMS (global monitoring system) in his pocket, the RFID which he/she can carry, via his/her use of interactive TV, his computer connected to Internet, spied, followed and his intimate secrets pierced.

# Which solutions?

- 1st step: How to better the Data Protection legislation?
  1. Identifiability means also contactability and traceability;
  2. Digital identifiers are sensitive data
  3. Compatibility means absolute respect of the context
  4. Consent is never a sufficient condition for legitimizing data processing
  5. Reciprocal benefits' principle leads to a more effective right to access

# Which solutions?(2)

- Step 2: New objects and actors to be regulated
  - terminals must be privacy compliant and by default must be privacy friendly; Their functioning must be transparent
  - Privacy Impact assesment for I.S. designers
  - need to regulate new actors as the gatekeepers (beyond the actors regulated by the Directive e-privacy);
  - profiling methods must be regulated according the specific risks they are raising

# Which solutions?(3)

- Let's come back to the Article 8 of the EHCR:
  - from the physical domicile to the virtual one;
  - from correspondance to e-communications
- Let's develop new synergies
  - with computer crime legislation
  - with consumer protection legislation

# CONCLUSIONS

- DATA PROTECTION WILL NEVER EXHAUST PRIVACY conceived as encompassing all conditions for the respect of Human Dignity and Liberties.
- Data Protection is only a tool and never an end as such.
- ...and DPA are not firstly judges.