From Data Protection to Data Retention

Round Table organised by
Asociatia pentru Internet si Tehnologie & Council of Europe Information Office, Thursday 6th March 2008, Bucharest

Joseph A. Cannataci

Professor of Law &
Director – Centre for Law, Information & Converging Technologies,
University of Central Lancashire, UK

Professor of Law & Information Technology, Head of Division,
Law & IT Research Unit, University of Malta

Visiting Professor in Information & E-Commerce Law, University of Bucharest

About the speaker

- Member of the Executive of BILETA (British & Irish Law, Education & Technology Association)
- Panelist (& often Chair), Czech Arbitration Court on ".eu" Top Level Domain names, ADR On-line Dispute Resolution
- Member, Drafting Committee, Cybercrime Convention, 1996-2001
- Vice-Chairman, Group of Specialists on impact of New Communication Technologies on Fundamental Rights & Democratic Values, Council of Europe, 1998-2000
- Principal co-author, Guidelines for Protection of Privacy on the Internet, COE 1999
- Rapporteur on use of personal data for Police Purposes, Project Group on Data Protection, Council of Europe 1992-1993
- Chairman, Committee of Experts on Data Protection, Council of Europe 1996-1998 (Vice-Chairman 1992-1996)
- Chairman, COE Working Parties on DP in Insurance, New Technologies 1994-2000
- Chairman, MEDIALEX, COE 1994
- National delegate, Committee of Experts on Legal Data Processing, Council of Europe, 1986-1996
- IT Law Practitioner B2B, 1986-2008
- Country Representative for Computer Law Association (1996-2008)

Outline of Presentation

- Transposition & hierarchy of Privacy rules in Europe – "Data Protection in context"
- Today I will cover
  - Privacy, Data Protection & EU Constitutional Law – Where future directions may lie
  - COE Recommendations & EU Developments on
    - Development of rules on medical data
    - From data protection to Data Retention – the development of rules for use of personal data by Police & Security agencies
    - Some questions on Insurance during discussion time

Privacy at Constitutional level

- **National Level**
- **Council of Europe**
- **European Union**

National level

- 13 countries include data protection principles in their constitution
- This is ½ of EU states
- So, the new developments in the “European Constitution” only reflected already-practised data-protection principles

Developments in the CoE

- Convention for the Protection of Individuals – aka: Convention 108
- Now signed by 37 member states
- Sectoral Recommendations developed rules on **processing of *personal* data**
- These are **NOT binding but** stimulated important development on the issues

The EU

- Convention 108 was an important source
- 3 Directives –
  - **95/46/EC**
    - Processing of personal data
    - Excellent link to Human Rights
  - **97/66/EC**
    - Privacy in the telecommunications sector
  - **2002/58/EC**
    - Privacy in the electronic communications sector
- Charter of Fundamental Rights of the EU

Charter of Fundamental Rights

- Article 8 -

- Not a *legally binding* effect on EU institutions but a *source of law…until Lisbon (December 2007)*
- At first, there was no mention to protection of personal data
- Later, direct reference was made to the ***Aquis Communitaire***

The Development - I

- 1st version –
  - '*Every natural person shall have* ***a right to protection for his personal data***'
  - No detailed list made on purpose due to possible technical advances
  - Still, information must be processed *fairly* and for *specified purposes*
  - The data subject's consent remains vital

The Development - II

- 2nd version –
  - '*Everyone has the right to **determine for himself** whether his personal data may be disclosed and how they may be used.'*
  - The **definition** is a bit explicit and there are guidelines as to how and what this right stands for
  - The proposals reflect the differences between the 2 rights: i) right to freedom of information
    ii) right to protection of personal data

The Development - III

- 3rd version –
  - *'Everyone has right to protection of personal data concerning him. Such data must be processed* ***fairly for specified purposes on the basis of his consent*** *… everyone has the right to* ***access****'*

The EU Constitution

- **Article II-68** (Article 8 of Charter of F.R. of EU) –
  - Right to protection of personal data

- **Title IV, Part I –**
  - Provides rules for right of protection of personal data processed by Union institutions etc…

- Importance of these provisions:
  - Promotion of this right at an **International Constitutional** level

Implication of Constitutional Enforcement

- Link between Data Protection and Human Rights
- Data Protection and National Security
  - Does the latter have priority over data protection?
  - The Constitution would give power to EU Courts
  - More effective control by Member States
  - Remedy to the citizen
- Uniformity of Laws
- Reduce overloading and overlapping of the laws

Data Protection & Medical Data

- The importance of medical data at COE
- The mission of the 1976 Working Party
- The 1980 Recommendation
- The detailed review
- The “new” Recommendation on Medical Data – R(97)5
- Ten years on there is nothing better than R(97)5

Medical Data & Privacy

Respect for Privacy

3.1. The respect of rights and fundamental freedoms, and in particular of the right to privacy, shalll be guaranteed during the collection and processing of medical data.

3.2. Medical data may only be collected and processed if in accordance with appropriate safeguards which must be provided for by domestic law.

Individuals or bodies working on behalf of health-care professionals who collect and process medical data should be subject to the same rules of confidentiality incumbent on health-care professionals, or to comparable rules of confidentiality.

Medical Data & Purpose

Collection and processing of Medical data

4.1. Medical data shall be collected and processed fairly and lawfully and only for specified reasons.

4.6. Unless otherwise provided for by domestic law, the holder of parental responsibilities may act as the person legally entitled to act for the unborn child, the latter being a data subject.

4.7. Genetic data collected and processed for preventive treatment, diagnosis or treatment of the data subject or for scientific research should only be used for these purposes or to allow the data subject to take a free and informed decision on these matters.

Medical Data – Genetic Data

Collection and processing of Medical data

4.9. For purposes other than those provided for in Principles 4.7 and 4.8, the collection and processing of genetic data should, in principle, only be permitted for health reasons and in particular to avoid any serious prejudice to the health of the data subject or third parties.

Medical Data – Information of Data Subject

Information of the Data Subject

5.1. The data subject shall be informed of the following elements:

c. The existence of a file containing his/her medical data and the type of data collected or to be collected;

d. The purpose or puposes for which they will be processed;

e. Where applicable, the individuals or bodies from which they may be communicated;

f. The persons or bodies to whom and the purposes for which they will be communicated;

Information of the Data Subject

e. The possibility, if any, for the data subject to refuse his consent, to withdraw it and the consequences of such withdrawal;

f. The identity of the controller and of his/her representative, if any, as well as the conditions under which the rights of access and of rectification may be exercised.

Medical Data & Security

Security

9.1. Appropriate technical and organisational measures shall be taken to protect personal data – processed in accordance with this recommendation – against accidental or illegal destruction, accidental loss, as well as unauthorised access, alteration, communication or any other form of processing.

Medical Data & Security

Security

9.2. In order to ensure in particular the confidentiality, integrity and accuracy of processed data, as well as the protection of patients, appropriate measures should be taken:

…

f. To guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment (control of communication);

g. To guarantee that it is possible to check and establish *a posteriori* who has had access to the system and what personal data have been introduced into the information system, when and by whom (control of data introduction).

Data Protection & the Police

- Painful birth of R(87)15 – a victory
- The significance of the notion of purpose
- In the ascendant – the adoption of R(87)15 at Schengen
- The first battle – the 1993 review
- The second battle – the 1998 review
- 1999-2001 Reports Art 29.
- The 2003 Report of Art 29
- The 2005 Report of Art 29
- The Data Retention Directive of 2006

The painful birth of R(87)15

- R(87) 15 was born within the Committee of Experts on Data Protection (CJ-PD) during 1984-1986
- CJ-PD characterised by strong leadership, Spiros Simitis,(later for draft EU constitution) to Nov 1986 (adoption) succeeded by Peter Hustinx, today EU DP Commissioner.
- Many of the data protection experts at CJ-PD in Strasbourg accompanied by police & security representatives
- The police & security reps tried very hard to persuade CJ-PD to permit “general purpose” collection but failed

The victory of R(87)15 = Purpose

- Ambiguity created by Convention 108 re exclusion from provisions for security purposes
- R(87)15 resolved this ambiguity by unambiguously subjecting police data to same data protection regime as other data
- R(87)15 scored victory by entrenching the notion of purpose for collection and processing of data, even for police use

In the ascendant: the early years 1987-1993

- Never popular with the police
- Greeted as model for democracy and cited often especially in the 1989-1992 period in Central & Eastern Europe
- Classic post 1989 use in Stasi files in Germany-the purpose challenged
- Riding the wave: in the post-1989 surge forward for democracy, adopted as data protection standard for Schengen Treaty

From Recommendation to Treaty?

- No stopping R(87)15 in the early years
- Recommendation 1181 (1992)1 on police co-operation and protection of personal data in the police sector) the member states of the Council of Europe had agreed to move towards a convention enshrining the principles of R(87)15
- What happened then?
  - Why don't we have a new convention today?
  - Why, instead, do we have a data retention directive?

The first battle: 1993

- Would anyone dilute R(87)15?
- CJ-PD requested to review it and Cannataci report ensued
- several experts concurred “that the provisions of the Recommendation constitute an inalterable necessary minimum” (CJ-PD (93) 48).
- The number of requests for serious revision of the text, whether to strengthen or to weaken the provisions, was deemed to be too small to merit a re-opening of the discussion on R (87) 15 as a priority matter for the Project Group on Data Protection.
- Cannataci report preserved status of R(87)15

The second skirmish: 1998

- Periodic review every 5 years
- The Patijn Report
- More detailed recommendations
- The 1998 Report concluded that up till then no serious problems had been raised that would have necessitated changing the recommendation.
- The report proposed that the Committee of Ministers recommend that national legislators explicitly deal with certain questions of data protection, either in the national Data Protection Act, the national Code of Criminal Procedure, or national or regional Police law.
- But the integrity of R(87)15 was preserved

The Police & the Internet

- R(87)15 was a pre-Internet animal
- Interpol & Europol were not in synch in their data protection standards
- The Police and security forces slowly started gaining experience with Internet & cybercrime
- Immigration issues with Schengen were pushing uses of hi-tech ID systems (from mag-stripe to biometric)

Cybercrime vs. Privacy 1996-2001

- The first signs of a losing battle
- Concern with cybercrime increased in inverse proportion with concern with privacy
- The crime lawyers were in the ascendant: the attempts by CJ-PD to insert breach of privacy as a substantive offence in the Cybercrime convention failed;
- The role of the US is inestimable: in order to get the US on board a Council of Europe convention, the PC-CY was prepared to downplay Privacy as an issue

The role of the US

- US approach to data protection less strict than European approach
- In Cybercrime, US were interested in
  - agreeing minimum substantive offence
  - Creating 24/7 collaboration for detection & investigation
  - Creating mechanism for preservation of evidence & subsequent prosecution
- Privacy was just not an issue (but when is it to security forces?)

Changing times – 9/11

- R(87) 15 was created when Europe had largely settled the terrorist issues which had plagued Germany & Italy in the 70s
- 2001 brought with it 9/11 – a disaster which heralded much trouble for data protection
- First victim: Airline passenger lists and the dispute between EU and the US

Waking up to the Internet

- Post-9/11 Police & Security forces became more aware of terrorist & crime uses of the Internet
- To Police & Security Forces, the Internet is simply another communications system
  - "to tap"
  - And especially to provide "traffic data"
- Police (esp in Germany) had been using traffic data to locate terrorists since the seventies. The lessons of the Clemens Wagner case from Baader-Meinhof era were well-learnt

We want the traffic data!

- So the debate commenced
- The Internet is rich in traffic data=let's get at it
- Art. 29 (and many others) pointed out many fallacies in Police & Security force arguments:
  - There are many ways of getting around monitoring of traffic and content data
  - Monitoring all data is grossly disproportionate measure and puts civil society at risk

Art 29 Working Party's arguments

- retention of traffic data for purposes of law enforcement should be allowed only under strict conditions and that the retained data should only be kept for a limited period and only where necessary, appropriate and proportionate in a democratic society.
- In its **Opinion on the Draft Data Retention Directive** the Article 29 Working Party questioned whether the justification for any compulsory and general data retention coming from the competent authorities in Member States had been clearly demonstrated and backed up with evidence and also whether the proposed data retention periods in the draft Directive were convincing.
- The Working Party also stated that in any case, the conditions under which the competent authorities could access and use such data in order to combat the threat of terrorism should be clearly spelled out.

The data retention directive

- One could say that the Article 29 Working Party's 'list of desirables' constitutes a return to basic data protection principles and in this sense preserve the spirit of R(87)15. *A contrariu sensu,* the extent to which the specific safeguards were addressed or ignored in Directive 2006/24, may be considered to be a measure as to how much R(87)15 is being "killed softly":
- Basically ignored all the data protection concerns
- Basically ignored Art 29 & forged ahead

The Criticism

- “Harsh criticism”
- Art 29
- Peter Hustinx
- Measures are disproportionate
- The notion of purpose is not respected
- Not enough safeguards are established
- The cost-efficiency of data retention nowhere demonstrated – how many terrorists & criminals have been apprehended because of Internet traffic data?

Directive 2006/24 vs. Data Protection 1

- *Purpose specification* – Directive 2006/24 does not clearly define and delineate the specific purposes for which data should be retained. Rather, it mandates that the retained data must be made accessible to authorities investigating on non-specified "serious crimes". Thus, the sacred principle of purpose specification, so hard-fought to achieve in R(87)15, has been ignored.
- *Access limitation* – Directive 2006/24 provides that the retained data is to be provided only to the competent national authorities, but it does not further provide that the competent national authorities should be specifically designated law enforcement authorities or that a list of such designated authorities should be made public. Neither does it clarify that other stakeholders, like the provider himself, do not have access to the data or that the data can only be provided if this is needed in relation to a specific criminal offence.

Directive 2006/24 vs. Data Protection 2

- *Data minimisation* – Directive 2006/24 defines data categories in Art 5.
- *No data mining* – The limitation in Art 4 of 2006/24 to "specific cases" seems to prohibit data mining activities. However (unlike much of the thrust in R(87)15) the Directive does not specify that the retained data can only be provided if this is needed in relation to a specific criminal offence.
- *Further processing* – contrary ot the opinion of the Art 29 Working Party or the thrust of R(87)15, Directive 2006/24 contains no provision ruling out or limiting stringently further processing for other related proceedings.

Directive 2006/24 vs. Data Protection 3

- *Access Logs* – Contrary to the opinion of Art.29 Working Party, the Directive 2006/24 does not create safeguards by providing that any retrieval of the data should be recorded and the records made available to the supervisory authority.
- *Judicial / independent scrutiny of authorized access* – Once again, an important safeguard recommended by the Art. 29 Working Party is not mandated by the Data Retention Directive.
- *Retention Purposes of Providers* – Yet again in breach of the advice of the Art.29 group, Directive 2006/24 does not provide safeguards by specifying that data should be retained by the service providers solely for public order purposes, and not for other purposes, especially their own.

Directive 2006/24 vs. Data Protection 4

- *System Separation* – There is no specific provision in Directive 2006/24 mandating, in particular, that the systems for storage of data for public order purposes should be logically separated from the systems used for business purposes and protected by more stringent security measures.
- *Security Measures* – Although Article 7 of Directive 2006/24 lays down general requirements on minimum standards concerning the technical and organisational security measures to be taken by providers, these are not sufficient and in particular the relationship between the adequacy of safety-measures and the costs is not addressed in the text of the provision.

Is R(87) 15 dead?

- Who has really funded an in-depth implementation review of R(87) 15?
- Can we trust the Police & security forces to be telling us the truth anyway?
- Data retention directive lowers the standards by
  - giving legitimacy to the opponents of "purpose"
  - Creates new dangers in large databases of traffic data which previously did not exist

Data Retention Directive Dangers

- It is submitted that the Data Retention Directive achieves the death (or at least a comatose state) of “purpose”…but only for traffic data.
- The respect for the principle of purpose for gathering data, in this case “traffic data”, now takes second place to the notional usefulness of such data in the fight against terrorism and crime.
- The danger inherent in having whole masses of data preserved, for years and subject to the monitoring by the police and security forces for “their” purposes is being ignored.

R (87) … neither dead nor dormant

- This being said, strictly speaking R(87)15 is neither dead nor dormant.
- It is still applicable in every area of personal data except communications traffic data.
- It still retains all its original strengths as well as its intrinsic weaknesses. As a mere Recommendation, it has no binding power on the member states of the Council of Europe.

Need to be written into EU Law

- Quite simply, Hustinx is right in identifying a lacuna and the equivalent of R(87)15 needs to be written into EU law. For there can be no doubt that R(87)15 had achieved a degree of international consensus within Europe.
- Whether a renewed commitment to this consensus will take the shape of a new Convention of the Council of Europe or an Additional Protocol to Convention 108 incorporating R(87)15 or a new EU Directive adopting as much of R(87)15 as a fierce internal debate will allow (or at least two of the previous options) remains to be seen.
- Whichever way it goes, it can also be viewed as being part of a cycle or even a cycle of cycles...

Quasi-constitutional EU Charter

Article 8 Protection of personal data

3. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Looking into the future...

- It is interesting to speculate on the effect that the resurrected European “constitution” could have on the fate of R(87)15.
- The “yes” vote in Luxembourg and German premier Merkel’s paved the way to the new quasi-constitutional status+may lead to developments favourable to R(87)15 given that the quasi- onstitutional nature of the Charter retains a positive bias towards data protection rules.
- There is a case to be made for the Data Retention Directive to be un-constitutional (see Germany), provided always that by the time the Lisbon treaty is ratified, EU 2006/24 would not have been scrapped on account of its not being cost-effective.