Council of Europe and Jurisprudence of the European Court of Human Rights in the field of Data Protection in Law Enforcement

Graham Sutton

Structure of presentation

- Identify the main elements of data protection by reference to the Council of Europe's legal instruments
- Look at a few cases from the European Court of Human Rights

Council of Europe data protection instruments

- 1950 Article 8 of European Convention on Human Rights
- 1981 Council of Europe Data Protection Convention (Convention 108)
- 2001 Additional Protocol to Convention 108
- Recommendations dealing with specific topics, including the use of personal data in the police sector

European Convention on Human Rights

- Article 8.1: “ Everyone has the right to respect for his private and family life, his home and his correspondence.”
- Article 8.2: Provides exemptions for “national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.
- Exemptions must be: “in accordance with the law” and “necessary in a democratic society”.

Data Protection: Purpose

Data Protection Convention: Article 1

“ The purpose of this convention is to secure ... for every individual... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.”

Data Protection: Balance

- It is not the aim of data protection to prevent personal data being used
- It seeks to balance organisations' need to use personal information with individuals' right to respect for their privacy

> "Recognising the need to balance the interests of society in the prevention and suppression of criminal offences and the maintenance of public order on the one hand and the interests of the individual and his right to privacy on the other."

Police Data Protection Recommendation: Preamble

Data Protection: Scope

Data Protection Convention: Articles 2 and 3

- The scope of data protection is very broad:
  - It applies to all activities, including law enforcement.
  - It applies to anything done with personal data: from collection to destruction, including disclosing and merely holding data (“processing”)
  - It covers all information about identifiable individuals (“personal data”)
  - Personal data can be text, images or sound
- Convention applies only to automated processing, but Parties can apply it to manual records

The Data Protection Principles

Data Protection Convention: Article 5

- Personal data must be:
  - processed fairly and lawfully
  - collected for a specified, legitimate purpose and not further processed “incompatibly”
  - adequate, relevant and not excessive
  - accurate and, where necessary, kept up to date
  - not kept for longer than required for the original purpose
- These rules are the core of data protection.

Special categories of data

Data Protection Convention: Article 6

- “Appropriate safeguards” are required for personal data relating to racial origins, political opinions, religious beliefs, health, sexual life and criminal convictions.
- These are commonly called “sensitive data”.

Data Security

Data Protection Convention: Article 7

- Appropriate security measures must be taken against accidental or unauthorised destruction, loss, and unauthorised access, alteration or disclosure
- Measures should include
  - physical security
  - technological means
  - organisational means
    - training
    - need to know

Individuals' rights

Data Protection Convention: Article 8

- Individuals have the right to
  - find out whether their personal data are being processed
  - get access to the data ("subject access")
  - have inaccurate data corrected and unlawfully processed data blocked or erased
- Individuals do not have to give reasons for seeking access
- The right of subject access is one of the main pillars of data protection

Derogations

Data Protection Convention: Article 9

- Derogations from the data protection principles and the right of access are permitted in the interests of
  - protecting State security, public safety, the monetary interests of the State, the suppression of criminal offences;
  - protecting the individual concerned or the rights and freedoms of others
- Derogations must be “provided for by law” and “necessary in a democratic society”

Sanctions and remedies

Data Protection Convention: Article 9

- There must be “appropriate sanctions and remedies for violations” of domestic data protection
- Specific provision depends on national legal traditions and institutions

Supervision

Additional Protocol: Article 1

- Processing of personal data is subject to oversight by an independent data protection supervisory authority
- The authority has the power to
  - investigate and intervene in processing
  - bring violations to court
  - deal with individuals' complaints
- Independence is essential since the authority must be free to take action against the Government as well as all other organisations

International transfers

Additional Protocol: Article 2

- Personal data may not be transferred to a country which does not provide an “adequate” level of protection
- For Council of Europe purposes, all countries that have ratified the Data Protection Convention are “adequate”
- Otherwise, “adequacy” is assessed on a case by case basis, having regard to all the circumstances
- Derogations from the “adequacy” requirement where there are legitimate prevailing interests, especially important public interests; or where there are adequate safeguards

Recommendations of the Committee of Ministers

- CM/Rec (2010) 13: Profiling
- R(2002) 9: Insurance
- R(99) 5: Privacy on the Internet
- R(97) 18: Statistics
- R(97) 5: Medical data
- R(95) 4: Telecommunication services
- R(91) 10: Disclosures by public bodies
- R(90) 19: Payment
- R(89) 2: Employment
- R(87) 15: Police
- R(86) 1: Social security
- R(85) 20: Direct marketing

Data Protection and the Police (1)

Recommendation R(87)15

- The Convention applies to the police. The Recommendation, which is part of the Schengen acquis, makes additional provision.
- Personal data should be limited to those needed "for the prevention of a real danger or the suppression of a criminal offence"
- Sensitive data should only be collected "if absolutely necessary for the purposes of a particular enquiry"
- Data should only be used for police purposes

Data Protection and the Police (2)

Recommendation R(87)15

- Strict rules on disclosing personal data, both within the police and to other agencies, and on overseas transfers
- Subject access may be refused only where “indispensable” for police purposes, or to protect the data subject or others.
- Reasons for refusal must be given in writing. Derogation as for subject access.
- Data must be deleted when not needed for police purposes. Criteria to be considered include: court judgements; rehabilitation; spent convictions; age of data subject; nature of the data.

European Court of Human Rights: Jurisprudence

- European Court of Human Rights has no direct jurisdiction over Data Protection Convention, but case law does refer to the Convention
- Data protection case law comes (indirectly) from the Court's consideration of cases under Article 8 of ECHR
- Consider a small selection of important decisions
- The decisions are complex. These summaries are simplistic.

Interference with right to private life

Leander v Sweden:1987

- Applicant sought employment in a museum on a naval base. After a security check, he was refused employment but not told why or allowed to comment.
- The ECtHR found that storing and release by security police of information about applicant's private life was an interference with his right to private life

Subject access: independent supervision

Gaskin v UK:1989

- Applicant had been in care as a child. As an adult, he sought access to his care records. He was given some, but refused others where the authors objected. There was no opportunity to seek an independent review.
- The Court found that the applicant had a vital interest in receiving the information about his early development. Refusal by the authors could be compatible with Article 8, but the principle of proportionality required that an independent authority be able to arbitrate.

Private life at work

Niemitz v Germany :1992

- The applicant's office was searched, under warrant, for incriminating documents in a criminal case.
- The court found that the search of the applicant's workplace involved interference with his rights under Article 8. The derogations might be more far-reaching in such cases.

Fundamental importance of data protection: Particular sensitivity of HIV information

Z v Finland: 1997

- The case involved a criminal trial in which both the defendant and his wife were HIV positive. During the trial, doctors were compelled to disclose both the husband's and the wife's medical records.
- The ECtHR found that there had been interference with the wife's right to private life. In considering whether it was proportionate, it took into account that data protection was of fundamental importance to the right to private life. The need to protect confidentiality was of particular importance where HIV was involved. Interference could be justified only by an overriding requirement in the public interest.

The need for safeguards

Rotaru v Romania: 2000

- The applicant complained that the Romanian Intelligence Service held information on his private life, some of it 50 years old, and he could not refute the untrue information.
- The ECtHR found that there was an interference with the applicant's private life, and that there was a basis in domestic law. However, the law provided insufficient limits on the powers available: for example, the kind of information collected; the period for which it was kept; the people able to consult it; the purposes for which it may be used.

The need to inform data subjects

Perry v UK: 2003

- The police made a covert video-recording of a suspect who refused to take part in an identity parade. They showed the video, along with others, to witnesses in place of an identity parade.
- The ECtHR found that there had been an unjustified interference with the applicant's right to private life. The police had not obtained his consent to the recording, informed him that it was being made, or informed him of his rights.

Disclosure of personal data in court

L.L. V France: 2006

- The applicant had been involved in divorce proceedings. His wife produced a medical report about him which he said she had obtained fraudulently. The case went to appeal and the appeal court quoted from the report.
- The ECtHR found that the appeal court had disclosed personal data about the applicant. The appeal court could have based its decision on other evidence, the report being only of subsidiary use. The interference with the applicant's right to private life, in view of the fundamental importance of the protection of personal data, was not proportionate.

Protection of private life on internet

KU v Finland: 2008

- A message on an on-line dating site about the alleged availability of the applicant, a 12 year old boy, was posted anonymously. The ISP would not reveal the identity of the originator of the message, to allow charges to be brought, because of the law on confidentiality of communications. The Finnish courts agreed.
- The ECtHR found that there had been a violation of the boy's right to private life. Freedom of expression and confidentiality of communications were primary considerations. Users of internet services must have a guarantee that their own privacy and freedom of expression will be respected. But such guarantee cannot be absolute and must sometimes give way to other legitimate concerns, including the protection of the rights and freedoms of others

Unrestricted retention of DNA etc

S.and Marper v UK: 2008

- DNA profiles, cellular samples and fingerprints of the applicants, one a minor, were retained indefinitely after their criminal trials had resulted in no finding of guilt.
- The ECtHR found that retaining all three categories of information was an interference with the right to private life. There was a risk of stigmatisation in treating the information of convicted and unconvicted people in the same way. This could be especially harmful in the case of minors. The retention of the data did not strike a fair balance between public and private interests.

The Future

- Technology continues to develop
- Data protection becomes even more important
- The Council of Europe is working on plans to modernise the Convention, and conducting a further review of the Police Recommendation

Thank you