JUS5630 – 2013
Lecture 2
Data protection law in context, particularly its interrelationship with human rights
(7th February 2013)

Lee Bygrave

1. Disposition

- Data protection pursuant to international human rights law
- Data protection in a national/domestic legal landscape – the case of Norway

2. Data protection principles in summary

- Fair and lawful processing
- Minimality in amount of data processed
- Purpose specification
- Use limitation
- Data/Information quality
- Data/Information security
- Data subject participation and control

- Additionally, other more general principles come into play – e.g., proportionality principle

3. International human rights law

- UNDHR Article 12
- ICCPR Article 17

  "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.

  2. Everyone has the right to the protection of the law against such interference or attacks".
- ECHR Article 8

  "1. Everyone has the right to respect for his private and family life, his home and correspondence.

  2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of 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".
- American Declaration of the Rights and Duties of Man (1948), Article V
- Article 11 of 1969 American Convention on Human Rights (1969), Article 11
- Cf. African Charter of Human Rights and Freedoms (1981): no express protection for privacy

4. ICCPR Article 17

- Human Rights Committee, General Comment 16, 1988:

  - Art 17 requires legal implementation of essential data protection guarantees in both private and public sectors
    - Query: exhaustive specification? Probably not.

5. ECHR Article 8

- Gradual, case-by-case recognition of data protection guarantees by ECtHR and ECommHR
- Broad, evolutive view taken of Art. 8
- But any data protection guarantees must be "inherent" in Art. 8
- Inspiration from data protection instruments
- But note principle of autonomous meaning
- Essential object of Art. 8:
  - protect individual against "arbitrary interference by public authorities" in his/her private life
- Broad view of ambit of "private life"
  - extends beyond domestic sphere (see, e.g., *Peck v. UK* (2003))
  - embraces development of interpersonal relationships (*Niemietz v. Germany* (1992))
- Positive obligations on State (elaborated further below)
  - e.g., with respect to establishing procedure for independent determination of information access claims (*Gaskin v. UK* (1989))
- Doctrine of "margin of appreciation" (elaborated further below)
- Application of Art. 8 to data processing practices of private sector bodies?
  - State obligation to provide data protection with respect to private sector processing? See *Von Hannover v Germany* (2004)
  - Can a private individual sue directly another private sector body for breach of Art. 8? Probably not
- Does Art. 8 protect corporate/collective entities as such?
  - See especially *Société Colas Est and others v France* (2002) – company offices = "domicile" / "home"
- Determining interference pursuant to Art. 8(1) – significant factors:
  1. consent
  2. awareness
  3. reasonable expectations (see, e.g., *Halford v. UK* (1995); *Copland v. UK* (2007))
  4. existence of rules permitting interference
  5. nature of the data/information concerned
  6. re-purposing of the data/information
  7. place in which interference occurs
     - NB. Non-consensual storage of personal data without further use may = interference (*Amman v. Switzerland* (2000))
     - NB. All cases so far of interference have involved non-consensual processing of data; under what conditions would ECtHR find interference despite existence of valid consent?
- Justification pursuant to Art. 8(2): cumulative criteria of …
  1. legal authority
  2. necessity
  3. purpose
- Legal authority:
  1. no need for legislative authority
  2. authority must, though, satisfy typical "rule-of-law" principles: foreseeability, clarity, non-arbitrariness
     - the legal measure "must indicate the scope of any ... discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity ... to give the individual adequate protection against arbitrary interference": *Malone v. UK* (1984), para. 68
  3. variation according to *gravity* of the interference

        - "interception of telephone conversations represent[s] a serious interference with private life and correspondence and must accordingly be based upon a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated": *Kruslin v. France* (1990), para. 33
    4. variation according to *purpose* of the interference
        - "the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly": *Malone v. UK* (1984), para. 67
- Necessity of interference – two criteria:
    1. "pressing social need"
    2. "proportionate to the legitimate aim pursued"
- Proportionality assessment varies according to:
    1. the gravity of the interference
    2. the sensitivity of the information
    3. the safeguards implemented
        - "Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only insofar as *strictly* necessary for safeguarding the democratic institutions": *Klass v. Germany* (1978), para. 42
        - "In view of the highly intimate and sensitive nature of information concerning a person's HIV status, any State measures compelling communication or disclosure of such information without the consent of the patient call for the *most careful scrutiny* on the part of the Court, as do the safeguards designed to secure an effective protection": *Z v. Finland* (1997), para. 96.
- Positive obligations on State:
    1. security measures
        - *I v. Finland* (2008) – deficiencies in hospital record-keeping system
    2. information access rights
        - *Gaskin v. UK* (1989); *McMichael v. UK* (1995); *Guerra v. Italy* (1998); *McGinley & Egan v. UK* (1998)
        - status of Art. 10? *Leander v. Sweden* (1987); cf. *Társaság a Szabadságjogokért [TASZ – Hungarian Civil Liberties Union] v Hungary* (2009)
    3. information rectification rights
        - transsexual cases: *Rees v. UK* (1986); *Cossey v. UK* (1990); *B v. France* (1992)
        - sufficient recognition of interest in "self-identification"?
- Doctrine of margin of appreciation – applies with respect to:
    1. proportionality assessment
    2. extent of States' positive obligations
    3. establishment of fact

    Narrowed according to:
        1. how important right concerned is
        2. how serious interference is
        3. purpose of interference
        4. extent of common European standards – see, e.g., *S & Marper v. UK* (2008)

6. Data protection law in context: example of Norway

- Constitution § 102
- principle of legality
- Formal incorporation of ICCPR and ECHR
  - semi-constitutional status (see Human Rights Act § 3)
- Criminal Code 1901
  1. § 390 (punishes violation of privacy caused by "public communication of information relating to personal or domestic affairs")
  2. §§ 145 & 145a (privacy of communications)
  3. § 121 (punishes breach of statutory duty of confidence; cf. Administrative Procedures Act § 13; Medical Doctors Act § 31 etc.
  4. §§ 246 et seq. (punishes defamation)
- Criminal Procedure Act, Chapter 16a
  - (regulating police wire-tapping for purposes of investigating narcotics crime and for purposes of national security)
- Case law on non-statutory protection of personality: see especially …
  1. Supreme Court decision of 1952 ("Two suspicious persons")
  2. Supreme Court decision of 1977 (access to medical records)
  3. Supreme Court decision of 1991 (covert video surveillance)
- Case law on identification of persons in relation to investigation and trial of criminal offence
- Marketing Act § 1
  - use of name for marketing purposes
- Intellectual Property Act § 45c
  - reproduction of photographs
  - Supreme Court decision of 2001 (<teazer.tv>)

For slightly outdated overview in English, see chapter on "Norway" by Bygrave & Aarø, in M. Henry (ed.), *International Privacy, Publicity and Personality Laws* (London: Butterworths, 2001), pp. 333–346. For more comprehensive and up-to-date treatment in Norwegian, see Schartum & Bygrave, *Personvern i informasjonssamfunnet* (Bergen: Fagbokforlaget, 2011, 2nd ed.).