Data protection and criminal law

Inter-University Centre Dubrovnik
International Spring Course
24th March 2016

Prof. Hannes Tretter
Research Centre Human Rights, University of Vienna
Co-Director, Ludwig Boltzmann Institute of Human Rights

Some history

- **Start of data protection (DP)** → Sixties in USA (establishment of a national centre for electronic data processing)
- **Criticism** based on **"right to privacy"** (1890, *Warren & Brandeis*) → demand for legal protection → Privacy Act 1974
- **Discussions** also in **Europe**, between 1970 and 1980 data protection laws in Germany and Austria
- **Landmark:** "Census judgement" of the German Constitutional Court → **"Right on informational self-determination"** (right to dispose on own data)

Where do we leave tracks?

- Paying with debit, credit or customer cards
- Shopping online, via Amazon, eBay & Co.
- Transferring money or setting up a custody account
- Filing a tax form, using online forms
- Using GPS in a car or on the mobile
- Using health insurance cards
- Leaving DNA/genetic samples or traces
- Making a phone call or sending an e-mail, a letter
- Outings in Blogs, You tube, Twitter and Facebook
- Using preferred websites in Google & Co.
- Entering the public monitored by cameras and drones
- Use of personal data in administrative or court procedures as a party or witness – who will get access of the files?

→ **Numerous personal data lead to “glassy individuals”.**

Contemporary data protection law

- **Focus on:**
  - Official registration of data processing by privates
  - Data collection and use by authorities bound on concrete legal aims and the principle of proportionality
  - Right to information and “informed consent”
  - Right to rectification of irregular data
  - Right to delete unlawfully processed data
  - Effective remedies before independent organs against violations of the right to data protection by authorities and private companies
- **European standards (CoE, EU)**
- **Case-law of the ECtHR**

Right to data protection in Europe (I)

- **Deduced from right to privacy, right to private life, right to "individual self determination" →**
  - tackling threats by new information technologies.
  - Milestone: BVerfG "Census judgement" 1983 →
  - "Digitally affected individual" adjusts personal conduct
- Strong influence by **case-law of the ECtHR**
- **Article 8 ECHR**
  - includes right to data protection → **Note:** There must always be an interference with the right to private life!
- **Article 8 EU Charter of Fundamental Rights:**
  - right to data protection (picking up Art 8 ECHR case-law)
- **Constitutionally guaranteed in European States**

Right to data protection in Europe (II)

- Right is **affected** if personal data are **processed** by
  - collecting, recording, storing, transmission, dissemination
- **Protected are personal data with regard to, i.a.,**
  - private sphere (not only in own four walls, also in public)
  - personal identity (i.a. ‚race', ethnic origin, age, disability, health, DNA, finger prints)
  - political opinion, religious or philosophical belief
  - personal orientations/preferences (i.a. sexual orientation)
  - communications (i.a., phone calls, mailing, meetings)
  - personal daily life (i.a. bank account, shopping, estate)
  - business/professional life, trade-union membership
  - public life (i.a. political engagement)

Right to data protection in CoE

- **CoE Convention 108/1981**
  - Covers all fields of processing personal data,
  - provisions are intended to regulate the **processing of personal data in general**, not only in the private sector →
  - applies also to data protection in the area of police and criminal justice although Parties may limit its application.
- **CoE Police Data Recommendation 1987**
  - Legal tasks of police and criminal justice authorities often require the processing of personal data which may entail serious consequences for individuals.
  - Recommendation gives **guidance to authorities** on how they should give effect to the principles of the Convention 108 in police and criminal justice matters.

EU law on data protection/private sector

- **Directive 95/46/EC on personal data protection**
  - Personal data must be processed **fairly and lawfully** and only for specified, explicit and legitimate **purposes**
  - **Collected data must be**
    - adequate, relevant and not excessive in relation to purpose,
    - accurate and kept up to date,
    - must not be kept longer than necessary for the purpose.
  - **Special protection for 'sensitive' data**
    - revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health and sex life.
  - **Restrictions** only
    - in case of 'informed consent' or in 'vital interest' of data subject,
    - if necessary in case of legal obligations/interests of others,
    - if necessary in case of public interests.
  - Right to **information**, **rectification** and **deletion**
  - **Effective remedies** in case of violation of the right

ECtHR case-law on data protection in criminal proceedings (I)

- ***B.B. v. France*, 2009**
  - The ECtHR decided that the inclusion of a convicted sex offender in a **judicial database** fell under Art 8 ECHR.
  - Because of sufficient data protection safeguards such as
    - the right of the data subject to request erasure of the data,
    - the limited length of data storage and limited access to such data,
  - a fair balance had been struck between the private and public interests at stake → no violation of Art 8 ECHR.
- ***S. and Marper v. UK*, 2008**
  - Applicants were charged with, but not convicted of criminal offences.
  - The unlimited **storage of biometric data** (fingerprints, DNA profiles and cellular samples as well as limited possibilities to request deletion constituted a disproportionate interference with the right to respect for private life, although permitted by a statute → violation of Art 8 ECHR.

ECtHR case-law on data protection in criminal proceedings (II)

- ***Allan v. UK*, 2002** (similar *Vetter v. France*, 2005)
  - Private conversations of a prisoner with a friend in the prison visiting area and with a co-accused in a prison cell were secretly recorded, constituted an interference with the right to private life.
  - Since there was no statute regulating the use of covert recording devices by the police at the relevant time, the said interference was not in accordance with the law, and therefore a violation of Art 8 ECHR.
- ***Klass and Others v. Germany*, 1978**
  - Applicants were suspected to cooperate with RAF terrorist, why their letter mails and telecommunication were put under secret surveillance.
  - ECtHR found that applicants were informed of the surveillance afterwards, and sufficient safeguards against abuse had been put in place.
  - Secret surveillance was justified because necessary in a democratic society in the interests of national security and for the prevention of crimes – and in particular proportional in times of terrorist threats.

EU law on data protection in police and criminal matters (I)

- **Council Data Protection Framework Decision** 2008/977/JHA (DPFD) on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters →
- **Applicability of DPFD** is limited to data protection in **cross-border cooperation** between authorities of EU or its MS, **does not extend to national security**.
- **Providing protection of personal data of natural persons** when their data are processed for preventing, investigating, detecting or prosecuting criminal offences or of executing a criminal penalty.

EU law on data protection in police and criminal matters (II)

- **DPFD** relies on the **principles and definitions** contained in the **CoE Convention 108/1981** and in the **Data Protection Directive 95/46/EC** (DPD):
  - Data must be used only by a **competent authority** for the purpose for which they were transmitted/made available.
  - The receiving MS must respect any **restrictions** on the exchange of data in the law of the transmitting MS.
  - Use of data by the recipient MS for a **different purpose or any onward transfer** requires the consent of the transmitting MS although there are exemptions in urgent cases.
  - The competent authorities must take the necessary **security measures** to protect personal data against any unlawful form of processing.

EU law on data protection in police and criminal matters (III)

- Each MS must ensure that one or more **independent national supervisory authorities** are responsible for advising and monitoring the application of the provisions adopted pursuant to the DPFC.
- They shall also deal with **claims lodged by any person** concerning the protection of his/her rights and freedoms regarding the processing of personal data by authorities.
- The **data subject is entitled to information** about any processing of his/her personal data, and has the right of access, rectification, erasure or blocking.
- Where the exercise of these rights is refused, the data subject must have a **right to appeal** to the competent national supervisory authority and/or to a court.

EU law on data protection in police and criminal matters (IV)

- If a person suffers damage due to violations of the national law implementing the DPFD, this person is entitled to **compensation from the controller**.
- Generally, data subjects must have **access to a judicial remedy** for any breach of their rights guaranteed by national law implementing the DPFD.
- In case of **transfer of personal data to third States**,
  - the receiving State has to ensure an **adequate level of protection** for the intended data processing, or
  - provides **safeguards which are deemed adequate** by the transmitting MS according to its national law.
- **Current question:** "Safe Harbour" Agreement, respectively improved "Privacy Shield" Agreement EU – US.

Data protection in case of cybercrime The CoE “Budapest Convention” 2001

- **Convention on Cybercrime 2001**
  - addresses crimes committed against and by means of electronic networks, enables international cooperation,
  - requires MS to update and harmonise their criminal laws against hacking, copyright infringement, computer-facilitated fraud, child pornography, etc.,
  - provides for procedural powers covering the search of computer networks and the interception of communications in the context of fighting cybercrime.
- **Additional Protocol** to the Convention
  - deals with the criminalisation of racist and xenophobic propaganda in computer networks.

Thank you for your attention!

PPT available soon on:

http://bim.lgb.ac.at

Relevant literature:

FRA, Handbook on European data protection law, 2014