Hannes Tretter

Summary Lecture Data Protection and Criminal Law

A. Some history

- Discussion on protection of privacy and data protection started in the sixties in USA (establishment of a national centre for electronic data processing).
- Critical view on "yellow press" publishing incriminating pictures that are violating a "right to privacy" (1890, *Warren & Brandeis*) → demand for legal protection → US 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)

B. Contemporary data protection law

- Contemporary data protection law is focussing on
  - Official registration of data processing by private companies
  - 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 against violations of the right to data protection by authorities and private companies
- European standards (EU, CoE)
- Case-law of the ECtHR and the CJEU

C. Where do we leave tracks?

- Paying in shops with debit, credit or customer cards
- Buying a flight ticket (passenger name records)
- Shopping online, as 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
- Testifying in the course of criminal procedures

→ **A huge amount of personal data of each of us**

D. Right to data protection in Europe

- Deduced from right to privacy, right to private life, right to individual self determination →
    - by exploring the substance of these rights tackling contemporary threats and challenges
- Strong influence by case-law of the ECtHR
- Article 8 ECHR: right to private life includes right to data protection according to ECtHR case-law
- Article 8 EU Charter of Fundamental Rights: right to data protection
- Constitutionally guaranteed in most States
- 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)

E. European standards pursuant to Directive 95/46/EC on personal data protection and the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 108/1981

- Personal data must be processed fairly and lawfully and only for specified, explicit and legitimate purposes
- Data must be adequate, relevant and not excessive in relation to purpose, and accurate and kept up to date
- Special protection for 'sensitive' data: data must not be kept longer than necessary for the purpose
- Restrictions i.a. only in 'vital interest' of data subject
    - in case of 'informed consent' or publication by data subject,
    - if necessary for legal claims or on medical/health reasons
- Processing of data on criminal, civil and administrative cases only under control of official authorities
- Right to information, rectification and deletion
- Effective remedies in case of violation of the right

→ But: The Data Protection Directive does not apply to the area of police and criminal justice!

F. EU law on data protection in police and criminal matters

- 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 aims at providing protection of personal data of natural persons when their personal data are processed for the purpose of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty.
- The applicability of the DPFD is limited to ensuring data protection in cross-border cooperation between competent authorities of the EU or its Member States (MS) and does not extend to national security.
- The DPFD relies to a large extent on the principles and definitions which are 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 and only for the purpose for which they were transmitted or made available.
    - The receiving MS must respect any restrictions on the exchange of data provided for in the law of the transmitting MS.
    - Use of data by the recipient state for a different purpose is, however, allowed under certain conditions. The logging and documenting of transmissions is a specific duty of the competent authorities in order to assist with the clarification of responsibilities arising from complaints.
    - Onward transfer of data, received in the course of cross-border cooperation, to third parties requires the consent of the MS from which the data originate, 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.
    - 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 or her rights and freedoms regarding the processing of personal data by competent authorities.
    - The data subject is entitled to information about the processing of his or her personal data, and has the right of access, rectification, erasure or blocking. Where the exercise of these rights is refused on compelling grounds, the data subject must have a right to appeal to the competent national supervisory authority and/or to a court.
    - 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.