Surveillance and Employment in Austria: A Human Rights based Approach

PAW – Privacy at Workplace

Conference in Pécs 03. April 2012

Ing. Dr. Christof Tschohl
Legal Researcher University of Vienna
Workinggroup Legalinformatics (ARI)

christof.tschohl@univie.ac.at

http://rechtsinformatik.univie.ac.at/

Assumptions regarding Surveillance and Employment

1. The employee is determined by the employer

- The employee may not choose place, time and manner of work
- The employee is under supervision and direction

2. The legal framework aims to constitute balance

- Both sides can argue legitimate interests for/against surveillance
- A fair balance has to consider the proportionality principle

3. The Human Rights methodology is based on the idea of appreciation of values

- Just few Human Rights are absolutely protected (e.g. Art 3 EMRK)
- The term „proportionality“ has to be filled with tangible meaning
- Human Rights Research has to argue methodically comprehensible
- A human rights based approach thereof can provide useful guidance

Constitutional Background in Austria

§ 1 Data Protection Act (DSG) - Fundamental Right to Data Protection → in constitutional rank

- *„§ 1. (1)* ***Everybody*** *shall have the* ***right to secrecy for the personal data*** *concerning him,* ***especially with regard to his private and family life****, insofar as he has an interest deserving such protection. Such an interest is precluded when* ***data cannot be subject to the right to secrecy due to their general availability*** *or because they cannot be traced back to the data subject"*

- *Right to Secrecy applies for automatically and manually processed personal data*

Legitimate use of personal data (§ 1 (2) DSG)

- In the **vital interest** of the data subject
- With the **consent** of the data subject
- **Overriding legitimate interest** of another

  - **The essential criterion is the purpose of the measure !**

(2) "[…] Even in the case of permitted restrictions the intervention with the fundamental right shall be ***carried out using only the least intrusive of all effective methods****."*

Constitutional Background in Austria II

„Horizontal Effect“ → § 1 (5) DSG

*(5) The fundamental right to data protection, except the right to information, shall be **asserted before the civil courts against organisations that are established according to private law**, as long as they do not act in execution of laws. In all other cases the Data Protection Commission shall be competent to render the decision, unless an act of Parliament or a judicial decision is concerned.*

Moreover: The European Convention of Human Rights (ECHR) forms part of the Austrian Constitution

Article 8 ECHR – Respect for privacy and family life and correspondence

- The Constitutional Court (VfGH) refers regularly to the jurisprudence of the European Court of Human Rights (ECtHR) / also the Supreme Court (OGH)
- Scope includes professional context (Niemietz v. Germany/1992)
- Interception of office phone can violate Article 8 ECHR (Halford v. UK/1997)
- Monitoring of e-mails (traffic data!) in the workplace can cause a breach of Article 8 ECHR (Copland v. the United Kingdom /2007)

A **“horizontal effect” is mediated by interpretation** of § 16 ABGB (civil code) containing a general personal right (but not on constitutional level)

Balance of Interest in Employment Context

1. Privacy and Data Protection vs. Fundamental Right of Property

- Property is protected by Art 5 StGG (State Basic Law) and Art 1, 1st additional protocol to the ECHR
- Purpose has to serve a **legitimate interest** defined by **objective criterion** (e.g. abusive behaviour during sick leave due to a particular suspicion)

2. Proportionality Principle

- A Measure has to be **suitable to serve the purpose**
  - Not suitable e.g. (Data Protection Commission, 120.951/0009-DSK/2004): Work time recording ok, but the log of the entry-time not
- *"…least intrusive of all effective methods."* (§ 1 (2) DSG)
- Finally: **Adequacy** (in the narrow sense): Harm and benefit need to be in appropriate balance with respect to the purpose of the measure

3. Modell of gradually control aggregation

- Increasing of control/surveillance intensity "step by step"
- Less intrusive measures (e.g. anonym traffic control) could educe facts which justify further (more intrusive) measures

Applying the Principles: Practical Examples I

Control of the IT-System

1. **Ensuring Functionality of Equipment**
   - Employer as the owner of the IT-System may collect data regarding the use of IT-Equipment → first step: automatically and anonym
   - Prevention of "malware" may justify even the control of content → but firstly by automatic means (virus programme)

2. **Detecting significantly deviations from normal use**
   - second step: monitoring (personal related) for employee control
   - Preventing abusive use of equipment (e.g. private printing)
   - Preventing abusive use of paid work time (e.g. private Internet surfing)

3. **Access to Communication Data of the employee**
   - If the first steps lead to a concrete and substantial suspicion for infringement or criminal behaviour → safeguards and procedures!
   - Access to private data (even at the work place) just under particular circumstances justified – not automatically due to the "abuse of work time" for private purposes

Applying the Principles: Practical Examples II

Control of Internet-use

- Cache of a Proxy-Server contains the URL (websites) → content data
- Logging amount by the Proxy or Firewall is a matter of setup
- Visited websites could also contain "sensitive data" (websites on particular medical information etc.) of the data subject (employee) → higher level of protection (§ 9 DSG)
- Even there a legitimate overriding interest could justify (§ 9 Z 11 DSG)
- Is private use of internet allowed or prohibited ? → if allowed: proportionality requirements even more strikt!

Control of E-Mail

- An E-Mail Server allows (technically) for multiple logging/retention of all traffic information and content
- Official business E-Mail: Business interests justify control largely
- No access to private E-Mail content – even if private use is not allowed
- If not distinguishable: Access maybe limited to the "subject matter" line
- If content is obviously private: hard stop!

Applying the Principles: Practical Examples III

Control of Telephony

- Traffic data of business related calls is in general allowed
- Content data (interception) of business related calls → just with notification of both (!) communication partners and just if necessary with regard to the specific purpose and business area
- Interception of private calls from business premises is basically not allowed, even not if a private use is prohibited
- Traffic data of private calls: just for "billing" purposes and partly masked or with the consent of the workers council (§ 96 (1) No 3 ArbVG) or the individual consent (§ 10 AVRAG)

location data in the course of "remote" working

- E.g. Austrian Post announces tracing of routes and time of delivery by mobile handheld-devices
- E.g. trip- and location recorder in vehicles
- Possibility of location tracing by mobile phone-cell-ID → just if phone contract by the employer, otherwise no access (no lawful use case in data retention or "billing data" disclosure)
- Just if particular reasons justify overriding legitimate interest (proportionality!!) → measure may not just touch but violate Human Dignity

Limits, Safeguards and Information

Measures which touch the Human Dignity

- § 96 (1) No 3 Labour-Constitution Law (ArbVG) → Introduction of Surveillance Measures or technical systems for employee control **need the consent of the workers' council** if the touch the Human Dignity
- § 10 AVRAG: If there is no workers' council just with employees consent
- Human Dignity is touched by an intrusion in the core of privacy (e.g. entrance logging if regarding also toilets)
- Supreme Court (OGH): Time recording system by "fingerprint" identif.
- But also highly intensive control of the work performance touch the HD
- Also Video surveillance is touching the Human Dignity → but prohibited by § 50a (5) DSG if solely carried out in order to control the employee

Safeguards on technical level

- Surveillance possibilities shall be kept on the necessary minimum on technical level → "privacy by design" ("Human-Machine-Interfaces"; logging-settings of proxy servers, time-tracking-systems, etc.)

Information

- Information about the surveillance measures; information policy;
- In a particular case of interception the workers' council or individual should be informed / the workers' council should give his consent

Thanks for Your Attention

Ing. Dr. Christof Tschohl
Legal Researcher University of Vienna
Working Group Legal Informatics (ARI)

christof.tschohl@univie.ac.at
http://rechtsinformatik.univie.ac.at/

“You have nothing to hide?
you shoud’nt admit that!”