



Mag. iur. Dr. techn. Michael Sonntag

Mitarbeiterüberwachung

Datenschutzrecht

Institut für Informationsverarbeitung und
Mikroprozessortechnik (FIM)
Johannes Kepler Universität Linz, Österreich

E-Mail: sonntag@fim.uni-linz.ac.at
<http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



- OGH: "Während die Treuepflicht des Dienstnehmers diesen zum Einbekennen von Privatgesprächen verhält, verpflichtet die dargestellte Grundrechtsbindung sowie die Fürsorgepflicht den Dienstgeber, Eingriffe in Persönlichkeitsrechte auf die schonendste noch zielführende Art vorzunehmen."
(OGH 13.6.2002, 8 ObA 288/01p)
- Grundlegende Annahme für das folgende:
Keinerlei Privatnutzung erlaubt!
- Grund: Ist Privatnutzung erlaubt, greift der Datenschutz voll
 - Es ist im Vorhinein nicht erkennbar, ob Daten privat oder beruflich sind, daher sind **alle** als privat zu betrachten!
 - Ähnlich: Kommen auch potentiell sensible Daten vor, sind **alle** als "sensibel" zu behandeln



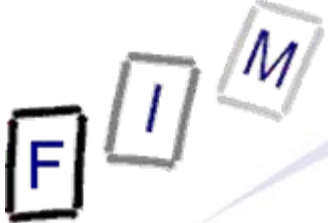
Persönliche "Überwachung"

- Überwachung durch direkte Beobachtung von Vorgesetzten
 - Dies ist rechtlich kein Problem!
 - Mitarbeiter sind zur Arbeit verpflichtet, diese darf auch von anderen Menschen überwacht werden
 - Datenschutz wird erst bei Automatisierung wirklich relevant
 - » Ansonsten: Aufzeichnungen (auch auf Papier)
- Problematisch ist weiters, wenn die Überwachung „geheim“ erfolgt, d.h. ohne dass Mitarbeiter es bemerken
 - Man soll auch einmal kurz unbeobachtet Nasebohren statt arbeiten dürfen ...
 - » Psychologischer Druck
 - » Siehe Videoüberwachung!
- Weiteres Problem: Auch Nicht-Mitarbeiter sind ev. betroffen
 - Klassisches Beispiel: Mithören bei Telefongesprächen



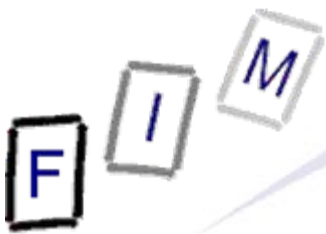
Vorbedingungen autom. Kontrolle

- Abschluss einer Betriebsvereinbarung über die Nutzung der Kommunikationstechnik; allenfalls Einzelvereinbarungen
 - Erzwingbare Mitbestimmung bei generellem Verbot
 - Tatsächliche Kontrolle nicht nötig, potent. Möglichkeit reicht!
- Information der Mitarbeiter
 - Was wird gesammelt; wie und durch wen ausgewertet
 - Muss separat von der Betriebsvereinbarung erfolgen
- Kontrolle
 - muss sachlichen Zusammenhang mit vertraglich geschuldeter Leistung besitzen
 - muss legitimes Kontrollinteresse betreffen
 - darf Menschenwürde nicht verletzen
 - » Keine dauernde Überwachung!
 - » Eignung, Erforderlichkeit, Angemessenheit
- Datenschutzgesetz: "überwiegende berechnigte Interessen"



Datenschutzrechtliche Sicht

- Grundlage: Sind Kontrolldaten personenbezogen?
 - Ein Unternehmen kann normalerweise die Mitarbeiter identifizieren, typ. über den Rechner (=Schreibtisch)
 - » Daher: Anonymisieren → Kein Datenschutzproblem mehr!
- Erforderlich: Zweckdefinition
 - Warum werden diese Daten gesammelt, was passiert damit?
 - » Wie genau, wann gelöscht, wer bekommt sie etc.
- Darauf beruhend: Interessensabwägung
 - Außer: Gesetzlich vorgesehen
 - » Archivpflichten, Lohnabrechnung, ...
 - Interesse des Unternehmens vs. Geheimhaltungsinteresse
 - » Grundlage: Arbeitnehmer = Unterwerfung unter Kontrolle
 - "Persönliche Abhängigkeit" ist typisches Merkmal!
 - » Daraus folgt: Gelindestes erforderliches Mittel



Stufenweises Vorgehensmodell

1. Vollautomatische Kontrolle der Systemsicherheit/-funktion
 - Fast uneingeschränkt zulässig
 - » D.h. Verhinderung ohne Protokollierung oder Information/Auswertung durch einen Menschen
 - » Anonymisierte Auswertungen (Statistik) möglich!
 - Problematisch sind "Zwitter": Sicherheit + Kontrolle
2. Bei signifikanten Abweichungen auch Überwachung möglich
 - » Ankündigung und Androhung erforderlich (generell möglich)
 - Achtung: Grenzwerte
 - » Es darf keine dauernde Kontrolle (bzw. solche Gefühl) erfolgen!
 - Auch durch Mitarbeiter möglich
 - » Keine Vollautomatisierung erforderlich
 - Personenbezogene Protokollierung ab hier speziell möglich
3. Individuelle Inhaltskontrolle bei konkretem Verdacht
 - Auch Inhaltsüberwachung möglich



- Aufzeichnung aufgerufener URLs an der "Firmengrenze"
 - Proxy/Firewall: Jeder URL (inkl. Bilder, ...) wird aufgezeichnet
 - Achtung: Hier "ausgehend", nicht "ankommend!"
 - » Ankommend: IP-Adress.-Speicherung ev. verboten/verpflichtend
 - » Ausgehend: Kein spez. Problem; ohnehin voller Personenbezug
 - Umso länger diese aufbewahrt werden, umso stärkere (potentielle) Kontrolle → Mehr Mitspracherechte (BR!)
- Stufenmodell:
 - Anonyme Auswertung: Anhaltspunkte für Fehlverhalten?
 - » Beispiel: Wie oft wurden welche Websites aufgerufen?
 - Ausfiltern von Bildern, Werbebannern, ...: Nur "Haupt"-Seiten
 - Lokalisierung: Wer hat diese Seiten aufgerufen?
 - » Nicht: Welche Seiten hat jeder Mitarbeiter aufgerufen!
 - » Noch besser: Wer hat diese Seiten mehrmals aufgerufen?
 - » Hier wird nur überwacht (eigentlich: ausgewertet), wenn/wer verbotene Handlungen ausführt



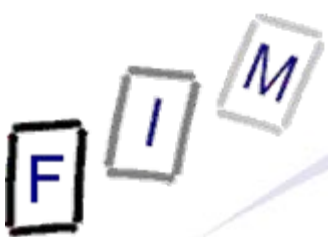
Exkurs: Webserver Logs

- Aufzeichnung der IP-Adressen derjenigen, welche Webseiten des Unternehmens abgerufen haben
- Deutschland: Verboten, da personenbezogene Daten
 - Kein relevanter Grund für Aufzeichnung vorhanden
 - » NAT, dyn. Zuteilung → Untauglich für Ausschluss
 - » Aber: Rückverfolgung von Angriffen, Gegenmaßnahmen?
 - Ausnahme: Abrechnung
- Österreich: Erlaubt, da nur indirekter Personenbezug
 - Ohne den Provider ist eine Zuordnung nicht möglich
 - » Achtung: Gilt nicht für interne IP-Adressen!
 - » Achtung: Gilt nicht wenn Benutzer sich registrieren/anmelden!
- Inhaltlich: Werden auch Parameter geloggt (d.h. Formularinhalte; GET statt POST) so handelt es sich potentiell um personenbezogene Daten (z.B. Name, Adresse)
 - Datenschutzgesetz in voller Härte anzuwenden!



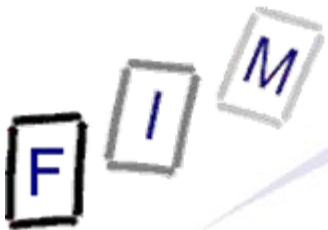
Web-Surfen: Browser-History/Cache

- Untersuchung des Computers im Nachhinein
 - Welche Seiten/Inhalte wurden besucht bzw. besichtigt
 - Ausschließlich berufliche oder auch solche privater Natur?
 - » Problem: Werbebanner, Popups, etc.!
 - » Besser: Nur URLs (=History) besichtigen
- Rechtlich heikel!
 - Analog E-Mails: Vorgesetzter darf sich E-Mails zeigen lassen, aber nicht unbedingt selbst durchwühlen
 - » Passt nicht ganz: E-Mails enthalten auch empfangene private!
 - Oder eher Akt mit Geschäftsbriefen?
- Als letzte Maßnahme erlaubt: Alle Inhalte gehen vom Nutzer aus, dieser dürfte nur beruflich nutzen
 - Aber: Nur als letzte Maßnahme, d.h. Mitarbeiter bereits ausgeschieden/unerreichbar und konkreter Verdacht
 - Ansonsten: Befragen und vorlegen lassen



Web-Surfen: Automatische URL/Inhalts-Filter

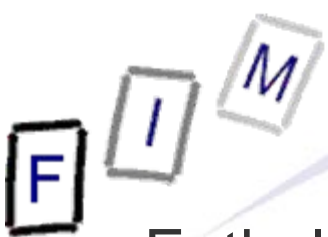
- Proxy filtert "unerlaubte" URLs heraus bevor er sie weitergibt
 - Bzw. "verbotene" Inhalte auf dem Weg hinein
- Rechtlich gesehen unproblematisch:
 - Vollautomatisiert, d.h. niemand erfährt davon
 - » Wird hingegen geloggt → Wie Webserver-Logs zu behandeln!
 - Keine Zensur, da keine Privatnutzung erlaubt
 - Fehlerhafte Filterung: Mitarbeiter muss Admin kontaktieren
 - » Kein Problem, da ja an sich erlaubte und arbeitsnotwendige Inhalte betroffen sind!
- Hilfsvariante: Anonymisiertes loggen, d.h. nur welche Seiten wie oft aufgerufen wurden
 - Tritt eine Häufung auf, dann kann detailliert geloggt werden
 - » Siehe Stufenmodell!



E-Mail Überwachung

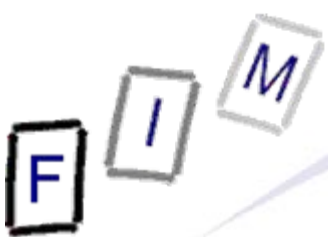
- Grundproblem der Überwachung: Ankommende E-Mails!
 - Selbst bei vollständigem Privat-Verbot können private E-Mails sehr wohl hereinkommen
 - » Nicht-Mitarbeitern kann dies nicht verboten werden!
 - » Aber: Woher stammt die E-Mail Adresse?
 - Wann bekommt man eine private Mail ohne die Adresse vorher mitgeteilt zu haben? → Möglichkeit der Hinweises darauf!
- Daher: Getrennte Behandlung ein-/ausgehender E-Mails!
 - Ausgehend: Kein Problem; "alles" erlaubt
 - Eingehend: Vorkehrungen für Privatpost erforderlich
 - » Es sind aber immer noch die Geräte des Unternehmens!
- Manuelle bzw. automatische Untersuchung von E-Mails
 - Erlaubt: Untersuchen der Geschäfts-Korrespondenz
 - Verboten: Lesen von Privat-Notizen

E-Mail Überwachung: Mailserver Logs

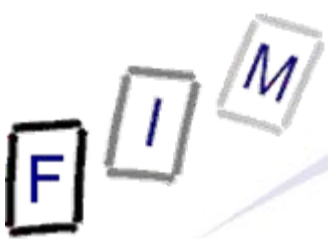


- Enthalten immer personenbezogene Daten (E-Mail Adresse)
- Achtung - Oft wird sehr viel protokolliert:
 - Überschrift, Absender-E-Mail: Aufgrund ankommender private Mails wäre das im Prinzip verboten!
 - Aber: Dies ist eine kleine Minderheit und nicht das Ziel der Aufzeichnung/Auswertungen; Unternehmens-Infrastruktur
 - » Kleine Problemfälle außerhalb seiner Kontrolle sollen Unternehmer nicht an wichtigen Maßnahmen hindern
 - Siehe: "Überwiegendes berechtigtes Interesse"
 - Dennoch: Wozu ist dies nötig?
 - » Absender E-Mail: Rückverfolgung; Kontaktierung bei Problemen
 - Immer gleich: Keine persönliche Prägung
 - » Überschrift: ????
 - Nachfragen: Auch ohne Überschrift möglich
 - Technik-Relevanz: 0! Aber: Spam?
 - Zusätzlich: Persönliche Prägung

→ Daher: Überschrift nicht protokollieren!



- Filterung nach Schadsoftware ist erlaubt:
 - Sicherung der Infrastruktur ist sehr wichtiges Anliegen
 - Sehr geringe Rate an falschen Alarmen
- Automatisches Löschen bzw. Reinigen
 - Datenbeschädigung: Privat-Mails & Fehler (Aber: Schaden?)
 - » Private Mails: Löschrecht (?) → Wäre gar kein Delikt
 - » Entschuldigungsgrund: Anderes nicht möglich; Unzumutbarkeit
- Problemlose Möglichkeiten:
 - Ablehnung der Entgegennahme
 - » Filterung **vor** Abschluss des Protokolls (=keine Übernahme!)
 - Externe Kennzeichnung
 - » Löschung wäre dann "Privatrisiko" des Empfängers
 - Für Viren nicht zu empfehlen!
 - Entfernung des Virus & Quarantäne mit persönlicher Freigabe bzw. besonderen Regelungen



- Externe Markierung (z.B. "[SPAM?]" in Titelzeile einfügen)
 - Kein Persönlichkeitseingriff, kein Schaden
 - » Ev. "Kennzeichnung" des Absenders, daher „?“
- Automatisches Löschen aufgrund der Markierung
 - Verantwortlichkeit dessen, der die Regel konfiguriert
 - » Beruflich: Anweisung; Privat: Eigenentscheidung
 - Aber: Keine vollautomatische Differenzierung möglich!
 - Ist eine Anweisung für automatisches Löschen erlaubt?
 - » Rate der Falscherkennung ist hier relativ hoch
 - Bei beruflichen E-Mails: "Betriebsrisiko"
 - » Berechtigtes Inhaberinteresse hier deutlich geringer als bei Viren
 - » Problem nur bei privaten E-Mails
 - Wie bei Viren: Dürfte gelöscht werden → Kein Problem
 - Vollautomatische Ablehnung der Entgegennahme immer zulässig!
 - Häufigkeit? Belastung der Einrichtungen des Unternehmens?
 - » Meiner Meinung nach erlaubt!



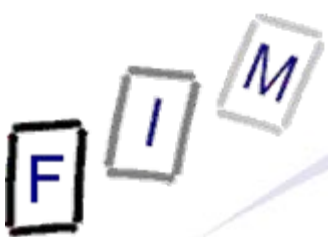
E-Mail Archivierung

- Vollautomatische (Komplett-)Archivierung ist erlaubt
 - Schutz gegen versehentliches Löschen, Systemfehler
 - Und: Archivierungspflichten!
 - » Z.B. Steuer: 7 Jahre
 - Betrifft sowohl ausgehende als auch eingehende E-Mails
 - » Privat-Erlaubnis: Ev. erforderlich Kennzeichnung einzuführen, sodass nicht archiviert würde
 - Meiner Meinung nach nicht nötig: Information über Archivierung + trotzdem absenden reicht als Zustimmung aus
 - Privates versenden: Verboten → Kein Problem
 - Privates empfangen: Selten; Ohne "Anregung" wohl rar
- Weiterhin zu beachten: Kenntnisnahme nicht erlaubt!
 - Aber wohl keine besonderen Vorkehrungen nötig, z.B. Markierung mit späterer automatischer Ausblendung bei Suchen
 - Missbrauch → Schadenersatz (konkreter Schaden nötig!)
 - » Immaterieller nur bei öff. Bloßstellung (MedienG)



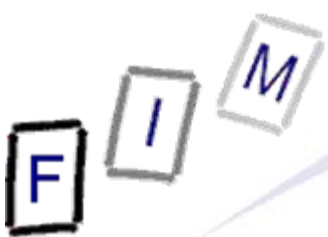
Keylogger, Screenshots, IM, Chat, Blogs etc.

- Keylogger und Screenshot-SW, selbst wenn mit Wissen der Mitarbeiter installiert, sind unzulässig
 - So detaillierte Überwachung verletzt die Menschenwürde
 - Berechtigte Interessen des Unternehmens nicht erkennbar
 - » Allgem. schon, aber für diese Intensität der Datensammlung?
- Chat/SMS: Mittelding zwischen E-Mail und Telefon
 - Schriftlich, aber sehr informell
 - Nach Benutzungsart wohl eher dem Telefon zuzuordnen
- Instant Messaging: Audio (=Telefon) oder Text (=Chat)
 - Daher insgesamt wie Telefon zu behandeln!
- Blogs, Wikis: Wenn vom Unternehmen, dann volle Kontrolle
 - Privat: Gleich normaler Webnutzung, d.h. verboten bzw. Überwachung möglich (siehe Proxy-Logs)



Was ist mit trotz Verbot vorhandenen privaten Inhalten?

- Erklärt der Mitarbeiter auf Befragung bestimmte Daten als "Privat", so dürfen sie in der Regel nicht untersucht werden
 - Ev. trotzdem ein Grund für Entlassung!
 - Keine Einsichtnahme, keine Kopien
 - Aber: Löschen!
 - » Wohl erforderlich: Möglichkeit geben, sich diese zu kopieren!
- Ist der Mitarbeiter nicht erreichbar?
 - Kontrolle erlaubt
 - Sobald feststeht dass privat, muss aufgehört werden!
- Nur in Ausnahmefällen ist Kontrolle privater Daten erlaubt
 - Beispiel: Konkreter Verdacht auf Firmenspionage
 - » Daher: Individuell, nicht kollektiv!
 - Erster Schritt: Vollautomatisch ohne Kenntnisnahme
 - » Nur wenn gar nicht vermeidbar: Durch Menschen
 - Besser: Polizei einschalten



Zutrittsberechtigungen und Personenlokalisierung

- Bloße Arbeitszeiterfassung und Prüfung von Zutrittsberechtigungen ist erlaubt
 - Siehe zu letzterem die entsprechende Musteranwendung!
- Problembereiche:
 - Berechtigungsprüfung = Lokalisierung (GPS, RFID)
 - Nutzung der Daten für andere Zwecke
 - » DSK: Eingabezeit der Arbeitszeit darf nicht für Kontrolle der Arbeitszeit verwendet werden (Erfassung über Web-Formular)
 - Einsatz von Biometrie: Z.B. Zeiterfassung per Fingerabdruck
 - » OGH: Trotz Nicht-Rückführbarkeit (d.h. keine Rekonstruktion des Fingerabdrucks aus den Daten) Berührung der Menschenwürde
 - Schon die bloße Abnahme ist eine hohe Kontrollintensität
 - Ergebnis: Nicht verboten, aber Zustimmungspflichtig
 - Hauptgrund: Relevante Verbesserungen gegenüber existierenden Systemen wurden nicht (genug) erläutert
 - **Überwiegende** berechnete Interessen!



Vorratsdatenspeicherung?

- Selbst bei Privat-E-Mail-Erlaubnis ist ein Unternehmen kein **öffentlicher** Telekommunikationsdienstleistungsanbieter
 - Achtung: In D wird dies aufgrund leicht anderer Formulierung im Gesetz anders gesehen → Dort wohl erforderlich!
 - Bei rein interner Nutzung von diversen Kommunikationsmethoden ohnehin nicht!
- Daher: Keine Verpflichtung zur Vorratsdatenspeicherung!
- Aber: Sofern Daten gespeichert werden, sind diese natürlich auf Gerichtsbeschluss, ... herauszugeben!
 - Daher eher vermeiden, Daten zu speichern
 - » Was nicht da ist, muss auch nicht herausgegeben werden

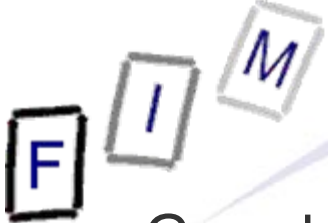


Einbeziehung des Betriebsrates

- Sehr umstritten, wann genau dies erforderlich ist
- OGH: Bloße Aufzeichnung angerufener Telefonnummern (Privat: Teilweise, Beruflich: Komplett) erfordert zwingend die Mitbestimmung des Betriebsrates
- Lehre: Geht zu weit, da gar keine Auswertungen der Rufnummern erfolgte und Information sowieso verpflichtend ist
 - Aber: Warum aufzeichnen, wenn keine Auswertung?
 - » Psychologisch ist die potentielle Auswertung für die Angestellten der tatsächliche Auswertung wohl gleichzustellen!
- Allgemein:
 - Unbedenklich – Berührt Menschenwürde – Verletzt MW
- E-Mail: Formelle Kommunikation, ähnlich Briefen
 - » Gilt zumindest bei beruflicher Kommunikation wohl noch immer!
 - Telefon: Informell, persönlich → Stärker geschützt
 - » Mithören (der Inhalte) stärker eingeschränkt als bei E-Mails

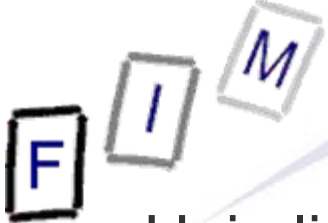
F I M

Daten als Beweismittel



Dürfen illegal gesammelte Daten vor Gericht verwendet werden?

- Grundsatz: Alle Beweise können vor Gericht verwendet werden
 - Erhebungsverbote (Themen/Mittel/Methoden) sind nur ein Indiz für ein Verwertungsverbot
 - » Beispiele: Beichtgeheimnis, Ärztl. Schweigepflicht, Folter, Aussage + spätere Berufung auf Zeugnisverweigerungsrecht
 - Allgemein: Verwertungsverbot, wenn auf verbotenerm Wege erlangt und Schutzzweck der Verbotsnorm erfordert es
 - » Strittig! Beispiele: Diebstahl ✓, Entführung/Nötigung ✗
 - » Generell verboten: Wenn schon das Beweisthema verboten ist
- Aber: Beweiswert hängt stark von der Erlangungsart ab!
- Allgemein: Meistens erlaubt, aber Strafbarkeit der illegalen Erlangung bleibt daneben bestehen
 - Verurteilung wegen Datenschutzverletzung
 - Negatives Urteil über Schadenersatz revidieren?
 - » Kosten + Geldstrafe als Schaden, der aus DS-Verletzung folgt
 - » Eher nicht: Rechtsmissbrauch!



- Heimliche Tonbandaufnahme
 - An sich Verletzung des Datenschutzes/Persönlichkeitsrechts
 - Vorlage bei Gericht erlaubt, da versuchter Prozessbetrug
 - » Notwehr → Erlaubt
 - Tonband = Auskunftssache → Vorlagepflicht für Inhaber
 - » Verwendung wohl eher zulässig!
 - OGH: Nur in besonderen Ausnahmefällen
 - » Notwehr, Notstand, überragende berechnigte Interessen
 - Müssen aber schon **bei dessen Erlangung** bestehen!
- Praxis: Vorlegen einer Abschrift des Gespräches
 - Der Inhalt der Kommunikation wird nicht vom DSGVO geschützt!
 - Variante 1: Gegner gibt dieses Inhalt zu → Erfolg!
 - » Kein Bedarf für Tonband; Verurteilung wegen DS-Verletzung potentiell möglich („Habe ich damals live mitstenografiert!“)
 - Variante 2: Gegner streitet Inhalt ab → Versuchter Prozessbetrug → Tonband vorlegen = Notwehr



Änderungen durch Novelle

Nur ehemaliger Plan!

- § 8 Abs 3 Z 5 DSG: Keine Verletzung schutzwürdiger Geheimhaltungsinteressen bei nicht-sensiblen Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor einer Behörde notwendig ~~und die Daten rechtmäßig ermittelt wurden~~
 - Anpassung an die Richtlinie (dort kein Erfordernis)
 - EB: Bisher keine Ermittlung zur Anspruchsdurchsetzung
 - » Nur Erlaubnis zur Zweckänderung ohnehin existierender Daten
 - Jetzt: Denkmöglichkeit des Einsatzes für Verfahren
 - » Vorherige relativ präzise Bestimmung des zu verf. Anspruches
- Dann praktisch jede Ermittlung erlaubt, wenn erforderlich zum Beweis eines Rechtes
 - Daher nicht: Bloß präventive Überwachung
 - Wichtig für Praxis: Telefon-Verträge (→ Beweisnotstand!)

F I M

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!