



Mag. iur. Dr. techn. Michael Sonntag

# Videoüberwachung

## Datenschutzrecht

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

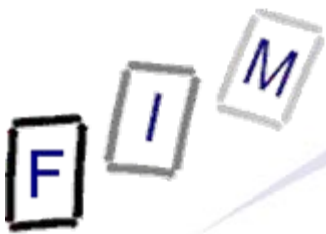
E-Mail: [sonntag@fim.uni-linz.ac.at](mailto:sonntag@fim.uni-linz.ac.at)  
<http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



# Videüberwachung

- Videoüberwachung: Visuelle Beobachtung von Personen, Orten oder Gegenständen
  - Nicht: Audioüberwachung
    - » Hier sind die Regeln viel strenger; privat gar nicht erlaubt!
  - Egal: Live oder Aufzeichnung
    - » Rechtlich gibt es dann allerdings schon Unterschiede
  - Praxis: Überwachung eines Ortes
    - » Aber das muss nicht so sein!
- Grundsatz: Technische Implementierung egal
  - Linsen-/Spiegelsystem, VHS-Kassette oder Videokamera
- Bedarf: Sehr hoch!
  - Auch Private möchten dies durchführen
  - Aufgrund sinkender Kosten praktikabel (früher: zu teuer)

**Hier nicht behandelt: Polizeiliche Überwachung**

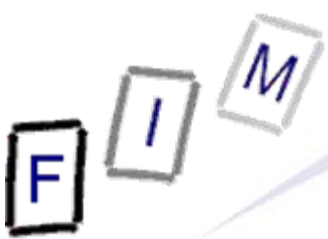


# Bisherige Rechtslage

- Ungeklärt und sehr umstritten!
- Einzelne Videoüberwachungen wurden genehmigt, allerdings zu Beginn nur als Probebetrieb und unter Auflagen
  - Beispiel: Wiener Linien → U-Bahn Überwachung
    - » Löschungspflicht, Zeitbegrenzung etc.
- Andere Videoüberwachungen waren zwar anzumelden, wurden aber problemlos registriert
  - Beispiel: Kassenüberwachung in Banken
    - » Achtung: Betriebsrats-Zustimmung erforderlich!
- Großes Problem war allerdings die private Überwachung
  - Wann ist sie erlaubt?
  - Alle müssten eigentlich angemeldet worden sein...
    - » Das ist sicher nur in wenigen Ausnahmefällen erfolgt!



- **Auskunftsrecht: Wie durchführen?**
  - Was ist, wenn eine zweite Person zu sehen ist?
  - Wiener Linie: Kein Auskunftsrecht, da die Aufnahmen nicht ausgewertet werden (außer bei Vorkommnissen) und daher die Suche nach der Person überhaupt erst zu einer solchen Verarbeitung der Daten führen würde!
    - » Als rechtliche Argumentation eher schwach...
- **Eigentlich immer sensible Daten: Rasse**
  - „Lösung“ der DSK: Nur dann sensible, wenn nach sensiblen Daten ausgewertet wird
    - » Das entspricht wohl nicht der EU-RL, denn verarbeitet (=aufgezeichnet) werden solche Daten ja sehr wohl ...
    - » Ist aber durchaus praxistauglich und entspricht der Gefahr ...
- **Kennzeichnungspflicht: Nicht explizit**
  - Ergibt sich ev. aus allgemeinen Grundsätzen
  - Unklar, wo, wie groß, was, Ausweichmöglichkeiten, ...



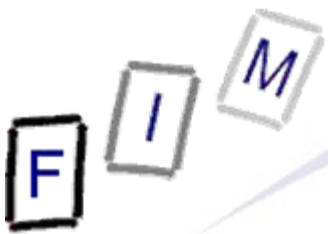
# Wann liegt eine Videoüberwachung vor?

- Systematische Feststellung von Ereignissen
  - Daher sind auch Serienfotos davon erfasst
  - Wohl auch: Einzelaufnahmen bei jedem Ereignis
    - » Detektiv fotografiert jeden, der Wohnung betritt/verlässt
- Bestimmtes Objekt oder bestimmte Person
  - Fokussierung erforderlich: „Was“ soll überwacht werden
    - » In der Praxis wohl keine große Einschränkung
    - » Ev.: Kamera mittragen, die filmt was man selbst sieht
      - U.U. keine Überwachung der eigenen Person
- Technische Bildaufnahme/-übertragungsgeräte
  - „Personenaufsicht“ ≠ Videoüberwachung
  - Analog oder digital → Egal!
- „Personen sind zu sehen, die identifizierbar sind“ (RegVorlage)
  - » Gilt aber ev. auch für Dinge, z.B. Autos (Nummerntafel!)
  - Immer, wenn personenbezogene Daten enthalten sind



# Wann liegt eine Videoüberwachung vor?

- Es muss sich eine „Überwachung“ ergeben
  - Regelmäßig (Zeit- oder Ereignisgesteuert)
- Nicht betroffen ist daher:
  - Touristisches oder künstlerisches Fotografieren
    - » „Einmalig“, auch wenn mehrere Fotos gemacht werden
  - Ausschließlich private oder familiäre Zwecke
    - » Beispiel: Kindergeburtstag
      - Auch nicht systematisch, wenn jedes Jahr gefilmt wird
- Videoüberwachung = Bild
  - Es darf **keine Tonaufzeichnung** erfolgen!
  - Reine Audioüberwachung ist ebenso nicht umfasst, diese ist „ganz normal“ zu beantragen (und wohl kaum zu erlangen!)



# Was sind rechtmäßige Zwecke?

- Schutz des überwachten Objekts bzw. Person
  - Bei privater Überwachung erfordert das ein Rechtsverhältnis zu diesem Objekt/Person
    - » Typisch bei Objekt: Eigentümer, Mieter etc.
    - » Beispiele bei Person: Verwandte (Kinder/Eltern), Securitydienst
- Erfüllung rechtlicher Sorgfaltspflichten
  - Arbeitnehmerschutz: Überfälle, Unfälle, ...
    - » Z.B. Kassenschalter, Überwachung gefährlicher Maschinen
  - Wegehalterhaftung: Überwachung von öff. Verkehrsflächen
    - » Haftung nur bei grober Fahrlässigkeit; siehe aber Winterdienst!
  - EisenbahnG, VeranstaltungsG, ...
- Jeweils inklusive Beweissicherung
  - Zum Schutz der Person und zum Beweis, dass man schützte
  - Zum Beweis für etwaige verbotene Aktionen/Fehlverhalten



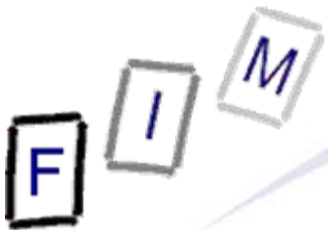
# Keine schutzwürdigen Geheimhaltungsinteressen bei ...

- Allgemein, d.h. Privatbereich und hoheitlicher Bereich:
  - » Hier keine Interessensabwägung, da schon im Gesetz
  - » Hoheitlich: Benötigt zusätzlich ein besonderes Gesetz
- Lebenswichtiges Interesse einer Person
  - » Beispiel: Videoüberwachung von Notfallbetten im Krankenhaus
- Daten über ein Verhalten, das ohne jeden Zweifel Schluss zulässt, dass es auf öffentliche Wahrnehmung gerichtet ist
  - » Genaue Bedeutung umstritten!
    - Variante 1: Bewegen in der Öffentlichkeit → Auf öffentliche Wahrnehmung gerichtet → Jede beliebige Aufnahme öffentlicher Wege/Straßen/Bereich wäre erlaubt
    - Variante 2: Absichtliche Öffentlichkeit herbeiführen, z.B. Straßenkünstler → Muss in Öffentlichkeit stattfinden **UND** zusätzlich besonders auf eine Wahrnehmung durch Viele ausgerichtet sein
  - » Variante 2 entspricht wohl mehr Intention und Wortlaut



# Keine schutzwürdigen Geheimhaltungsinteressen bei ...

- Allgemein, d.h. Privatbereich und hoheitlicher Bereich:
  - **Ausdrückliche Zustimmung des (aller!) Betroffenen**
    - » Das Recht auf Datenschutz ist verzichtbar
    - » Wird als potentiell „sensibel“ eingestuft, daher **ausdrücklich**
      - Konkludente Zustimmung ist also nicht möglich
      - Aber kein Schriftformerfordernis oder ähnliches
  - **Die Liste ist nicht abschließend**
    - » Dann ist aber eine Interessensabwägung erforderlich
- Auch im höchstpersönlichen Lebensbereich möglich!
  - **Übertragung von Videos der eigenen Wohnung ins Internet**
    - » Mit (eigener) Zustimmung
    - » Problem: Besucher



# Keine schutzwürdigen Geheimhaltungsinteressen bei ...

- Kein hoheitlicher Bereich (→ Privatwirtschaftsverwaltung!)
  - » Hier abschließende Liste: „Ausschließlich“ dann nicht verletzt
- Bestimmte Tatsachen rechtfertigen die Annahme, das Überwachungsobjekt/-person könnte Ort/Ziel eines gefährlichen Angriffs werden
  - » Tatsachen, nicht bloße Vermutungen!
  - » Muss allerdings nicht schon einmal vorgekommen sein
  - » Wenn es schon einmal passiert ist, muss eine gewisse Wahrscheinlichkeit bestehen, dass es wieder vorkommt
    - Dies ist aber nur in Ausnahmefällen auszuschließen!
    - Sollte innerhalb der letzten 10 Jahre erfolgt sein, außer es gibt für die Tat eine kürzere Verjährungsfrist
  - » Gegenüber dem Täter sowieso
    - Wäre Rechtsmissbrauch, würde der Täter sich darauf berufen!
  - » Dritte müssen bei schweren Taten im Interesse des Opfers zurückstehen



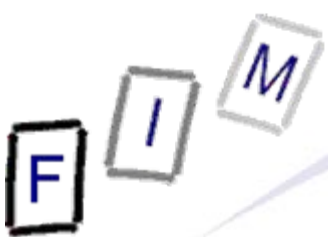
# Was ist ein „gefährlicher Angriff“?

- Geht über das Sicherheitspolizeigesetz hinaus
  - Alles, was dort als solcher gilt, reicht daher jedenfalls aus
- Umfasst auch:
  - Konkrete Gefährdungen von Geschäfts- oder Betriebsgeheimnissen
    - » Verdacht auf Betriebsspionage
      - Konkrete Anhaltspunkte nötig!
  - Konkrete Gefahren „grober Verwaltungsübertretungen“
    - » Schwarzfahren? MM nach eher nicht!
  - Überwachte Person besitzt überdurchschnittlichen Bekanntheitsgrad in der Öffentlichkeit
    - » Oder das überwachte Objekt ist Aufenthaltsort einer solchen
    - » Prominente dürfen sich selbst bzw. ihr Haus überwachen lassen
      - Achtung: Deren Zustimmung alleine reicht nicht, da ja auch andere Personen (Putzpersonal, Chauffeur, Dritte) erfasst sind
      - Von diesen fehlt die Zustimmung und wird hierdurch „ersetzt“!



# Was ist ein „gefährlicher Angriff“?

- Umfasst auch:
  - Person/Ort ist ein verfassungsmäßiges Organ oder der Aufenthaltsort eines solchen
    - » D.h., es muss in der Verfassung stehen
    - » Beispiele: Nationalrat, Landtage, Regierung/Ministerien, Gerichte
      - Diese sind „von Natur aus“ Terrorismusgefährdet
  - Überwachtes Objekt ist ein beweglicher Gegenstand von erheblichem Geldwert oder Aufenthaltsort solcher
    - » Z.B. Banken, Juweliere, Antiquitätengeschäfte, Tabaktrafiken
    - » Achtung: Nicht „abstrakt“ → Angriffsgefahr nötig
      - Wird aber wohl fast immer gegeben sein!
  - Gegenstand ist von außergewöhnlichem überdurchschnittlichem künstlerischem Wert
    - » Z.B. Besondere Kunstgegenstände in Museen („Saliera“!)
      - Nicht aber allgemein in Museen oder für jegliche Kunst!



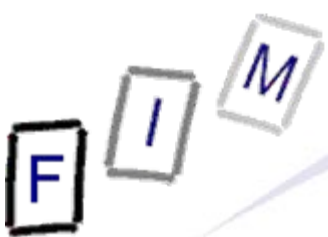
# Exkurs: „Gefährlicher Angriff“ laut SicherheitspolizeiG

- Bedrohung eines Rechtsgutes durch rechtswidrige Verwirklichung des Tatbestandes gerichtlich strafbarer Handlung
  - Vorsätzlich; nicht bloß auf Begehren eines Beteiligten verfolgt
    - » Keine Privatanklagedelikte (z.B. Angriffe auf Ehre)
  - Aus StGB (ohne kriminelle/terroristische Vereinigungen), SuchtmittelG (ohne Erwerb bzw. Besitz zum Eigengebrauch), VerbotsG, FremdenpolizeiG
- Verhalten, das darauf abzielt und geeignet ist, eine solche Bedrohung vorzubereiten
  - Nur in engem zeitlichem Zusammenhang mit angestrebter Tat
- Beispiele: Diebstahl, Körperverletzung, Entführung, Raub, NS-Wiederbetätigung, Sachbeschädigung (→ Sprayer!)



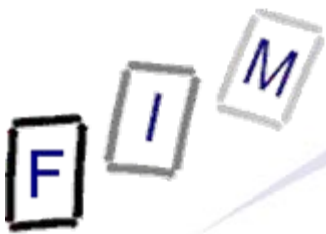
# Keine schutzwürdigen Geheimhaltungsinteressen bei ...

- Nicht-hoheitlicher Bereich
  - Unmittelbar anwendbare Vorschriften legen spezielle Sorgfaltsvorschriften fest
    - » Speziell: Nicht „allgemeine Arbeitssicherheit“, sondern „darf nur in Betrieb sein, wenn keine Person in 5m Abstand ist“!
    - » Unmittelbar anwendbar: Völker- oder Gemeinschaftsrecht, Gesetze, Verordnungen, Bescheide, gerichtl. Entscheidungen
    - » Können auch aus „bloßen“ Haftungsbestimmungen folgen
    - » Beispiele: EisenbahnG, VeranstaltungsG, Wegehalterhaftung
      - Um nicht für Dritte haften zu müssen → VÜ erlaubt
  - Überwachung ist bloße Echtzeitwiedergabe und erfolgt zum Schutz von Leib, Leben oder Eigentum des Auftraggebers
    - » **Keine Speicherung, keine Auswertung!**
      - D.h. auch kein Durchsuchen nach Personen die in Fahndungsdatenbank stehen, Vergleich mit Fotos, Bewegungsprofile suchen etc.
    - » **Achtung: Vermögen, Ehre, Ansehen, ... sind hier nicht enthalten!**
      - Vermögen: Geschäftliche Chancen sind kein Eigentum!

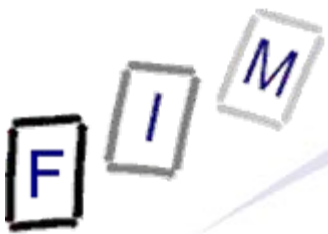


# Obligatorische Verhältnismäßigkeitsprüfung

- Der Verhältnismäßigkeitsgrundsatz ist zu beachten
  - „ auf gelindeste zum Ziel führende Art“
- Dies bedeutet:
  - Keine Videoüberwachung, wenn die Betroffenen besonders stark beeinträchtigt würden
    - » Z.B. Einfamilienhaus daher leichter als Mehrfamilienhäuser
      - Gehören „alle zusammen“ statt mehrere Mieter
  - Keine Videoüberwachung, wenn das gleiche Ergebnis auch mit anderen Mitteln erreichbar ist
- Beispiele (stammen aus Regierungsvorlage!):
  - Geschäfte: RFID-Chips statt Video zur Diebstahlkontrolle
    - » Sind RFID-Chips so viel besser???
  - Wohnhäuser-Schutz: Sicherheitstüren, Gegensprechanlagen, Alarmanlagen
    - » Videoüberwachung hat meist andere Ziele als Einbruchschutz!



- Höchstpersönlicher Lebensbereich
  - Handelt es sich nicht um die erste Gruppe (Lebenswichtig, öffentliches Verhalten, Zustimmung), so ist der höchstpersönliche Lebensbereich immer ausgenommen
  - Dort darf keine Videoüberwachung erfolgen, unabhängig vom Interesse des Auftraggebers
    - » Egal wie teuer das Produkt ist, das potentiell gestohlen wird!
  - Umfasst: Privatwohnungen (Inneres!), Umkleide-/WC-Kabinen (wohl auch: Pissoir)
- Keine Mitarbeiterkontrolle erlaubt
  - Dies bedeutet: Ob, wie, wie effizient etc. diese arbeiten
  - Vollkommen verboten, kann daher nie als Zweck dienen
    - » Falls die Überwachung erlaubt ist (z.B. Kassenschalter), darf keine Auswertung in dieser Hinsicht erfolgen!



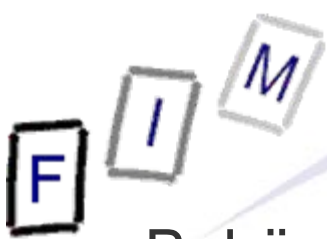
# Videüberwachung in Unternehmen

- Durchaus möglich, sofern die zulässigen Zwecke vorliegen
  - **Beispiel: Hantieren mit teuren Gegenständen**
    - » Diamanten sortieren, Goldmünzen verpacken etc.
    - » Geld-Handhabung (Kassen), Tresore mit wertvollem Inhalt
    - » Geschäfts-/Betriebsgeheimnisse: Tresore, Sicherheitsräume, IT-Räumlichkeiten, Backup-Lagerung/-Rechenzentren
- Aber:
  - **Keine Auswertung hinsichtlich Arbeitskontrolle**
    - » Anwesenheit (Stechuhr-Ersatz/-Kontrolle)
    - » „Nebentätigkeiten“, z.B. Surfen im Internet
  - **Zustimmung des Betriebsrats ist davon nicht betroffen**
    - » Wird meistens erforderlich sein, da Videoüberwachung die Menschenwürde berührt!
      - „Verletzt“ → Höchstpersönlicher Lebensbereich ist ohnehin ausgeschlossen, eher geringer Rest-Anwendungsbereich des Verbots



# Erlaubte Übermittlungen

- Problem: Zufallsfunde. Was darf mit diesen erfolgen?
  - Beispiel: Videoüberwachung eines Bankschalters gegen Überfälle - aufgenommen wird aber ein Taschendiebstahl
- Übermittlung ist erlaubt, auch wenn sich Handlung/Angriff nicht gegen das überwachte Objekt/Person richtete
  - An zuständige Behörde/Gericht wegen begründetem Verdacht, dass eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentiert wurde
    - » Nicht: Verwaltungsdelikte, Privatanklagedelikte, ...
  - An Sicherheitsbehörden zur Abwehr gefährlicher Angriffe und krimineller Verbindungen.
    - » Diese dürfen zur erweiterten Gefahrenforschung und zur Fahndung auf private Aufzeichnungen zugreifen
    - » Darf nur öffentliches Verhalten betreffen!
    - » Eingriffe in Privatsphäre sind auf Verhältnismäßigkeit zu prüfen

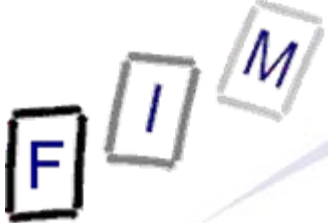


# Erlaubte Übermittlungen

- Behörden und Gerichte können immer die Herausgabe als Beweismittel „fordern“ (=Anordnung, Bescheid, d.h. formell!)
  - Ebenso: Beweissicherung, d.h. Verhinderung der Löschung
- Dies setzt voraus, dass die Behörden entsprechende Durchsetzungsmöglichkeiten besitzen
  - Gewährt also alleine gar keine Kompetenz!
  - Verhindert nur, dass eine existierende Erlaubnis leerlaufen könnte, da man “wegen DSGVO“ nicht herausgibt
- Ob die Übermittlung rechtmäßig war oder nicht, ist dann nur mehr Aufgabe der Behörde/des Gerichts
  - D.h., der private Herausgebende ist „aus dem Schneider“
- Grundlagen:
  - §§ 384ff ZPO: Beweissicherung, z.B. durch Sachverständige
  - § 19 AVG: Ladungen und mitzubringende Beweismittel
  - §§ 109ff StPO: Sicherstellung, Beschlagnahme

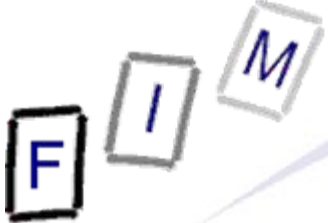


- Absolute Verbote ohne jegliche Ausnahme:
  - Kein automatisierter Abgleich
    - » Suche nach „unerwünschten Personen“
  - Kein Durchsuchen nach sensiblen Daten
    - » Feststellung der Hautfarbe, Krankheiten, etc.
- Achtung: Diese gelten nur für Überwachungen nach DSGVO!
  - Bei solchen nach dem SicherheitspolizeiG könnte dies durchaus möglich sein
    - » Kommt auf sonstige Gesetze bzw. allgemeine Grundrechte an!
    - » Beispiel: Abgleich mit Fahndungsfotos, Scannen von Autonummern auf als gestohlen gemeldete



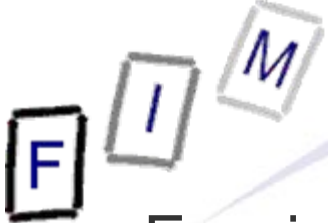
# Protokollierungspflicht

- Jeder Verwendungsvorgang ist zu protokollieren
  - Ausnahme: Echtzeitüberwachung
    - » Dort gibt es nichts zu protokollieren, da keine Aufzeichnung oder Auswertung erfolgen darf!
- Allgemeine Regelung: „Im notwendigen Ausmaße“
  - Hier: Lückenlos und ohne jede Abwägung
  - Was auch immer damit passiert, ist aufzuzeichnen
- Beispiele:
  - Wiedergabe: Jemand schaut (einen Teil) an
  - Durchsuchen nach bestimmten Zeiten/Personen/Orten
- Umfang:
  - Wer machte Wann Was Womit
    - » Beispiel: Müller spielte am 9.3.2010 Video von 0:20 bis 0:25 ab
  - Warum wohl auch, aber nur wenn el. verfügbar
    - » Sonst muss es eben später begründet werden!

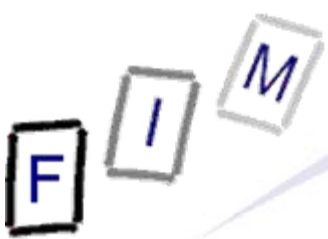


# Löschungspflicht

- Daten sind spätestens nach 72 Stunden zu löschen
- Außer:
  - Konkreter Anlass für Verwirklichung der zugrundeliegenden Schutz- oder Beweissicherungszwecke
  - Übermittlungsanforderung
    - » Behörden, Gerichte, Sicherheitsbehörden (siehe oben!)
- Fällt das Fristende auf Samstag, Sonntag, gesetzlichen Feiertag oder Karfreitag → Nächste Werktag ist Ende
  - Beispiel: Aufnahme von Mittwoch (0:00 Uhr) → Wäre am Samstag ab 0:00 Uhr laufend zu löschen → Frist endet daher erst am Montag
  - Problem: Regelung gilt für Tage, nicht Stunden
    - » Unklar ist daher, wann genau am Montag!
      - 0:00-0:59? Sinnlos und wohl kaum gemeint
      - 23:59? Etwas zu starke Ausdehnung?

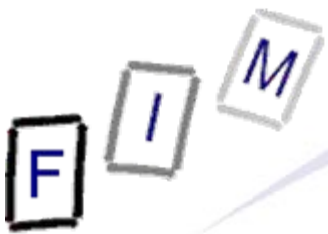


- Ev. sinnvollere Interpretation:
  - Die Dauer beträgt nicht 72 Stunden sondern 3 Tage
  - Beispiel: Mittwoch-Daten sind dann spätestens bis Montag Abend zu löschen
    - » Freitag Abend können sie noch erhalten bleiben (3 Tage) → Daher Ende erst am Samstag, der wird auf Montag verlängert
  - Aus allgemeinen Datenschutz-Pflichten → Grundsatz der Datenvermeidung → Löschung sofort nach Feststellung, dass keine Aufbewahrung erforderlich ist, d.h. kurz nach Beginn der Geschäftszeiten am Montag
- Weiteres Problem: 24-Stunden-Aufnahmen
  - Müssen diese minutenweise gelöscht werden?
  - Sonst wäre die letzte Minute 72 Stunden aufbewahrt, die erste hingegen 96 Stunden lang!
    - » Technisch wohl meist schwierig!
  - Mögliche Lösung: Wie technisch aufgezeichnet; max. ein Tag



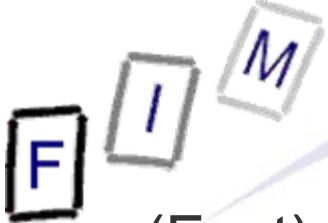
# Löschungspflicht: Strenge Auslegung

- Bei strenger Auslegung der Löschungspflicht
  - Wenn man es nicht in 72 Stunden schafft, dann muss man eben früher löschen
  - Ergebnis: 24 Stunden-Band muss binnen 48 Stunden nach Ende der Aufzeichnung gelöscht werden
    - » Dies ist durchaus eine mögliche Auslegung
      - Nach 2 Tagen weiß man, ob die Bank überfallen wurde!
      - Aber: Einschleich-Diebstahl? Denken Private immer sofort daran, die automatische Löschung zu stoppen? ...
  - Ergebnis: Ende am Wochenende → Montags 0 Uhr löschen
    - » Zumindest dieses Ergebnis kann kaum angenommen werden, da dies sicher nicht der Gesetzesintention entspricht!

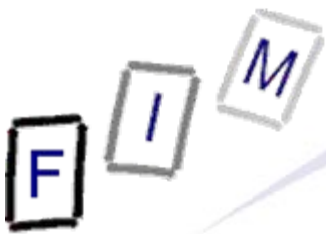


# Ausnahmen von der Löschungspflicht

- Eine längere Aufbewahrungsdauer ist durchaus möglich, muss aber von der DSK genehmigt werden!
  - Interessensabwägung
  - Begründung erforderlich
    - » Schwer, da ja Standardmäßig schon geregelt!
  - Besondere Gründe der Zweckerreichung müssen die längere Dauer regelmäßig erfordern
    - » Nicht: 3 Tage, außer im Betriebsurlaub, da bis zu dessen Ende
  - Rücksichtnahme auf allgemeine Verkehrssitte soll erfolgen
    - » Z.B. Öffnungszeiten von Geschäften
      - Stammt aus Regierungsvorlage, ist aber unklar: Welche Geschäfte haben regelmäßig mehr als 3 Tage geschlossen? Ev. anwendbar für „Sondergeschäfte“, die jede Woche nur einen Tag geöffnet haben!



- (Fast) Jede Videoüberwachung muss gemeldet werden
  - Nach DSGVO – nicht SiPoIG/...!
- Diese unterliegen der Vorabkontrolle
  - Nach neuem Recht bedeutet das, dass keine automatische Kontrolle stattfindet, sondern jeder Antrag von der DSK „händisch“ begutachtet wird!
    - » Also kein „durchschwindeln“ mit geschönten Aussagen möglich!
    - » Hintergrund: Die „bestimmten Tatsachen“ für die Annahme eines zukünftigen gefährlichen Angriffs + allgemeine Gefährlichkeit
- Ausnahme: Keine Vorabkontrolle bei spezieller Sicherheit
  - Videodaten werden verschlüsselt
  - **Einziger** Schlüssel wird bei DSK hinterlegt
  - Auswertung daher nur in begründetem Anlassfall durch eine bestimmte Stelle (in Zusammenarbeit mit DSK)
    - » Potentielles Problem: 72 Stunden! „Anhalten“ muss daher immer möglich sein, auch ohne Auswertung.



- Ausnahme: Keine Meldepflicht
  - Echtzeit-Videoüberwachung
    - » Keine Auswertung und keine Aufzeichnung; siehe vorher!
  - Speicherung (Aufzeichnung) erfolgt nur auf einem analogen Speichermedium
    - » Beispiel: VHS-Videokassette
    - » Grund: Sind nur schwer und aufwendig zu durchsuchen
      - Gefährdung unbeteiligter Dritter ist stark herabgesetzt
    - » Achtung: Digitalisierung = Datenverarbeitung → Meldepflicht
      - Also kein Umweg möglich, indem nur analog gespeichert und später dennoch digital verarbeitet wird!
- Achtung: Keine Meldepflicht ≠ DSGVO nicht anwendbar!
  - Protokollierungspflicht, Löschen binnen 72 Stunden, ...
  - Grundrecht gilt und allgemeine Grundsätze sind zu beachten
  - Auskunftspflicht, Löschrecht etc. weiterhin existent
  - ...



# Zusammenfassung Meldepflicht

- Echtzeitüberwachung oder nur analoge Speichermedien
  - Keine Meldung nötig
- Hinterlegung des einzigen Schlüssels
  - Meldepflichtig
  - Keine Vorabkontrolle
- Sonstige Videoüberwachungen entsprechend Spezialregeln
  - Meldepflichtig
  - Vorabkontrolle
  - Sicher genehmigt (bei Erfüllung der Voraussetzungen)
- Restliche Videoüberwachungen
  - Nicht genehmigungsfähig, d.h. abschließende Regelung!
    - » Unklar, ob es noch andere relevante Überwachungen geben könnte, die sonst genehmigungsfähig wären!
    - Potentiell: Videoüberwachung zur Gesundheitsvorsorge (§ 9 Z 12), Aufzeichnung von Gottesdiensten zu geistlichen Zwecken (§ 9 Z 13)



# Registrierungsverfahren

- Die „bestimmten Tatsachen“ müssen in der Meldung glaubhaft gemacht werden
  - Das bedeutet, genau erklären welche und warum
  - Darstellen, was der Tatsachenhintergrund ist (ev. Beweise anbieten, Nummern von Anzeigen/Gerichtsverfahren etc.)
- Sind nach § 96a ArbVG Betriebsvereinbarungen abzuschließen, so müssen diese vorgelegt werden
  - Ersetzbare (=durch Schlichtungsstelle) Zustimmung des Betriebsrats zur Einführung von Systemen...
    - » zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung personenbezogener Daten der AN, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen
    - » zur Beurteilung von Arbeitnehmern, sofern Daten erhoben werden, die nicht durch betr. Verwendung gerechtfertigt sind



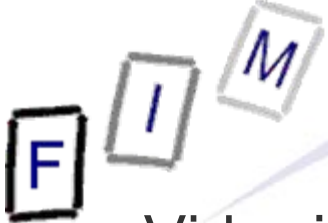
# Registrierungsverfahren

- Werden mehrere Personen oder Objekte überwacht
  - + derselbe Auftraggeber
  - + gleichartige Beschaffenheit oder räumliche Verbundenheit
  - + gleiche Rechtsgrundlage
  - = Eine einzige Meldung für alle zusammen möglich
- Verwaltungsvereinfachung: Statt „Kopien“ abzugeben ist eine „Sammel-“Meldung möglich
  - Das ist keine Erlaubnis für eine Ausweitung in der Zukunft auf lauter gleichartige Überwachungen!
  - Achtung: Alles was jetzt sein soll, auf einmal melden
    - » In Zukunft das gleiche noch einmal? → Kopie der Meldung machen und separat anmelden!



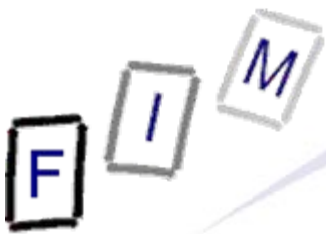
# Geplante Standardanwendungen

- Achtung: Nur inoffizielle Aussagen!
  - Verordnung wird noch etwas auf sich warten lassen
    - » VO für el. Meldung ist bis 1.1.2012 zu erlassen; wird vermutlich auch der Zeitpunkt für neue Standard-/Musterverordnung sein
- Kassenüberwachung in Banken
  - Ist praktisch immer zu genehmigen
  - Betriebsratszustimmung ohnehin erforderlich
  - Bisher keine Probleme damit bekannt
- Videoüberwachung von Einfamilienhäusern
  - „Sichtbereich“ der Kamera wird definiert werden müssen
    - » Kein öffentlicher Grund, keine Nachbarn?
  - Achtung: Für Zwei-/Mehrfamilienhäuser wird es wahrscheinlich **keine** Standardanwendung geben!



# Kennzeichnung

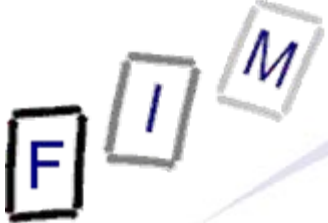
- Videoüberwachungen müssen gekennzeichnet werden
  - Muss „geeignet“ sein → Wohl Verweis auf allg. Grundsätze
  - Auftraggeber muss eindeutig dargestellt werden
    - » Außer, dieser ist Betroffenen nach Umständen bereits bekannt
      - Beispiel: Innerhalb eines Firmengeländes
  - Ort: So, dass potentiell Betroffene der Videoüberwachung tunlichst ausweichen können
    - » Also keine Verpflichtung, aber wenn es leicht geht, muss es so eingerichtet werden
- Kein bestimmtes Symbol vorgeschrieben!
  - Kann auch aus reinem Text bestehen
- Keine Kennzeichnung bei hoheitlicher Überwachung, die nicht meldepflichtig ist!
  - Bundesheer, verfassungsm. Einrichtungen, LV, EU, Vorbeugung/Verhinderung/Verfolgung von Straftaten
    - » Beispiel: Videoüberwachung eines Drogendeals 😊



- Existiert wie bei allen anderen Datenanwendungen
  - Zeitraum und Ort sind möglichst genau anzugeben
    - » Inoffiziell: Zeit auf 30-60 Minuten genau
  - Identitätsnachweis in geeigneter Form
  - Mitwirkungspflicht: Wohl auch Übermittlung eines Fotos
    - » Wie soll sonst gesucht werden...
  - Auskunft = Kopie in einem üblichen technischen Format
  - Alternativ: Einsichtnahme auf Geräten des Auftraggebers
    - » Auf Verlangen des Betroffenen!
      - Kann der Auftraggeber wohl nicht ablehnen:  
Leute die keine (passenden) Abspielgeräte besitzen
    - » Recht auf Kopie besteht weiterhin
  - Sonstige Infos (Übermittlungen, Zweck etc.): Schriftlich!
    - » Außer der Betroffene stimmt einer mündlichen Auskunft zu



- Keine Auskunft bei Echtzeitüberwachung
  - Wenn man zuschaut, ist man schon nicht mehr zu sehen!
- Auskunftsverweigerungsrechte bleiben gleich
  - Schutz des Auskunftswerbers aus besonderen Gründen
  - Überwiegende öffentliche Interessen:
    - » Einsatzbereitschaft BH, LV, Vorbeugung/... Straftaten, ...
- Überwiegende berechnigte Interessen des Auftraggebers oder eines Dritten
  - Sonderregelung für Videoüberwachung:
    - » Auskunft durch schriftliche Beschreibung des Verhaltens
    - » Auskunft unter Unkenntlichmachung anderer Personen
  - Wohl Wahlrecht zwischen beiden für Auftraggeber
    - » Was einfacher ist
- Hintergrund: Auskunft ist bei Videoüberwachung ohnehin relativ sinnfrei ...



# Strafbestimmungen

- Ist es keine gerichtlich strafbare Handlung oder nach anderen Verwaltungsbestimmungen strenger zu bestrafen, so ist eine Strafe bis € 25.000 zu verhängen:
  - Automationsunterstützter Abgleich mit anderen Daten
  - Durchsuchen nach sensiblen Daten
  - Nicht-Protokollieren einer Verwendung
- Bereits der Versuch ist strafbar
- Datenträger und Geräte können eingezogen werden
  - Kameras, Kassetten/Festplatten, Computersysteme etc.
- Bisher Ermächtigungsdelikt, jetzt Officialdelikt
  - Die Polizei muss das Delikt selbständig verfolgen, sobald sie davon auf irgendeine Weise erfährt!
    - » „Ermächtigung“ muss sich auf bestimmte Personen beziehen, daher keine Verfolgung bei unbekanntem Tätern möglich!

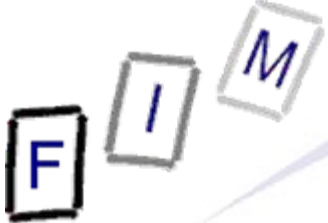


- Gerichtlich strafbar:
  - Z.B. Vorbereitung zu einem anderen Delikt (Ausspähen für Einbruch, Videoaufzeichnung für Erpressung)
- Zuständigkeit: Bezirksverwaltungsbehörde des Sitzes des Auftraggebers
  - Kein inländischer Sitz → Sitz der DSK



# Übergangsbestimmungen

- Videoüberwachungen, die vor dem 1.1.2010 registriert wurden, bleiben rechtmäßig so wie sie registriert waren
  - Sofern sie am 31.12.2009 den geltenden Bestimmungen entsprachen
  - Sofern die DSK keine Befristung verfügt hat
- Wurde nur befristet genehmigt, so gilt die Erlaubnis nur
  - bis zum Ende der Befristung, aber
  - längstens bis zum 31.12.2012
    - » Zwei Jahre „Schonfrist“
    - » Dann muss jedenfalls neu genehmigt werden
  - Unbefristete Genehmigungen bleiben hingegen weiterhin unbefristet gültig!

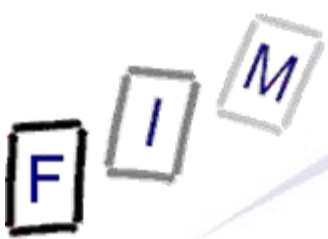


- Die folgenden Folien betreffen Sonderprobleme
- Diese sind noch nicht wissenschaftlich aufgearbeitet
- Es handelt sich daher nur um eine vorläufige Darstellung ohne Anspruch auf Richtigkeit oder Vollständigkeit!



# Sonderprobleme: Wärmebildkameras?

- Wie sind Infrarotkameras zu behandeln?
- Vermutlich wie jede „normale“ Videokamera auch
  - Es sind Bilder von Personen/Objekten, unabhängig vom verwendeten Frequenzspektrum
  - Es kommt auch sonst nicht auf die Technik an: Analoge oder digitale Aufzeichnung, beides ist Videoüberwachung!
- Aber: Bei Wärmebildern wird häufig keine Erkennbarkeit der abgebildeten Personen mehr vorliegen
  - Es handelt sich dann wohl großteils um anonyme Daten!
    - » Nicht: Eine bestimmte Person soll überwacht werden. Diese wird sich aus den Umständen wohl identifizieren lassen!
  - Das ist aber nicht immer so: Z.B. Wohnung filmen → Wohnungseigentümer ist eher identifizierbar, Besucher nicht
  - Daher wohl genauso zu melden/genehmigen/... wie jede „normale“ Videokamera



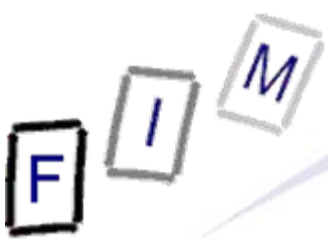
# Sonderprobleme: Nacktscanner?

- Nacktscanner in Flughäfen werden nicht privatrechtlich betrieben (Sicherheitsvorschriften für Betreiber) bzw. dienen jedenfalls der Verhinderung von Straftaten
  - Daher sind sie ohnehin großteils ausgenommen!
    - » Auskunft, Anmeldung etc.
- Grundprinzip: Ev. gar keine Videoüberwachung
  - Kein Video bzw. keine Serienfotos
    - » Nur ein einzelnes (ev. mehrere) Bilder
  - Keine „fortlaufende Feststellung von Ereignissen“
    - » Fortlaufend: Ev. „wer betritt Sicherheitszone (=Ort)“
    - » Ereignisse: Es geht jedoch nicht um das „Betreten“, sondern um etwas ganz anderes: Was man mit sich führt
  - Personen überhaupt erkennbar?
- Meiner Meinung nach keine Videoüberwachung!



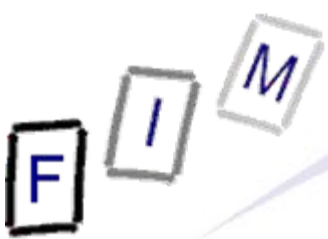
# Sonderprobleme: Wetterkameras?

- Zweck ist jedenfalls nicht die Aufzeichnung von Personen
  - Aber: Eine Videoüberwachung ist es dennoch!
    - » Ereignisse = Wetter; Ort = Wo sie hinsieht
- Problem: „Wetter“ ist kein erlaubter Zweck!
  - § 50a Abs 2: Schutz von Objekt/Person oder Sorgfaltspflicht
- Abgesehen davon:
  - Echtzeitübertragung; keine Auswertung, keine Aufzeichnung
  - Keine Meldepflicht, keine Auskunft
  - Doch jemand zu sehen: Nicht erkennbar, wer es ist
    - » Wer sich davorstellt und winkt: „öffentliches Verhalten“
    - » Gefährlich daher: Wer unwissentlich vorbeigeht und noch erkannt werden kann!
- Ähnliches Problem: Coffee-Cam



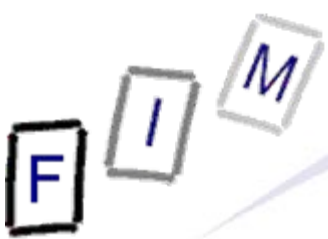
# Sonderprobleme: Wetterkameras?

- Bessere Argumentation: Werden keine personenbezogenen Daten verarbeitet, sind wir überhaupt aus dem DSGVO draußen
  - Daher kommen die Regelungen über die Videoüberwachung dann erst gar nicht zur Anwendung!
    - » Dies würde z.B. die „Coffee-Cam“ lösen
- Meiner Meinung nach daher: Verboten, sofern die Kamera so ausgerichtet ist, dass im „Normalfall“ erkennbare Personen erfasst werden!
  - Werden normalerweise keine Personen erfasst oder sind diese durch niemanden erkennbar, so liegt gar keine Verarbeitung personenbezogener Daten vor → Erlaubt
    - » Siehe aber Kamera-Attrappen sogleich; Persönlichkeitsrecht!
  - Ausnahmen durch „Posieren“ vor der Kamera sind kein Problem, da dann (konkludente) Einwilligung vorliegt



# Sonderprobleme: Kamera-Attrappen?

- Kameraattrappen führen keinerlei Aufzeichnung oder Übertragung durch
  - Daher sind sie auch keine Videoüberwachung!
- Aber: § 16 ABGB Allgemeines Persönlichkeitsrecht
  - Siehe OGH Urteil 6 Ob 6/06k vom 28.3.2007
    - » Entscheidung: Unterlassung der „Überwachung“, aber kein Anspruch auf Beseitigung (da er sein eigenes Grundstück überwachen durfte)
    - » Dies wird gleich gelten: Nur auf das eigene Grundstück beschränkt darf man auch so „überwachen“ (=Zustimmung)



# Sonderprobleme: Google Street View?

---

- Keine „Video“-Überwachung, aber ev. Serienfotos
  - Aber: Es wird weder eine Person überwacht noch ein Objekt (außer man definiert ganze Stadt/Land als solches!)
  - Es werden auch keine Ereignisse festgestellt
  - Von jedem Ort/Ereignis gibt es immer nur ein einziges Bild!
- Ergebnis: Keine Videoüberwachung
  - „Nur“ ein „normales“ Datenschutzproblem!



# Verbleibende Probleme

- Grundprinzipien und Abwägung gehen immer vor
  - Beispiel: Eine Videoüberwachung eines Hauses kann plötzlich unzulässig werden, wenn dort eine Arztpraxis eröffnet wird oder eine politische Partei einzieht!
    - » In der Praxis wird das wohl kaum jemand prüfen/VÜ einstellen!
  - Müssten solche Umstände (oder deren Fehlen) in der Anmeldung genau aufgeschlüsselt werden?
    - » Achtung: Register ist öffentlich!
    - » Ist aber Vorabkontrollpflichtig, könnte also zumindest theoretisch bei der Registrierung geprüft werden!
- Kein Auskunftsrecht bei Echtzeitüberwachung
  - Nicht das eigene Bild, aber Zweck, Rechtsgrundlage etc.
    - » Würde Standardanwendung entsprechen: Auskunft ist auch jedem zu erteilen!
      - Könnte auch als „gesetzliche Standardanwendung“ gesehen werden



# Zusammenfassung

- Endlich durchführbare Regelung der Videoüberwachung!
- Scheint durchaus praxistauglich zu sein
- Potentielles Problem: Löschung nach 72 Stunden
  - Dauerhafte Archivierung nicht möglich
  - Für viele Kleinunternehmen wird die Organisation der Löschung komplex sein
    - » Einfachste Lösung: Fertiges System mit „Kreisaufzeichnung“ (autom. Überschreiben nach Zeitablauf) kaufen
- Problem: Hohe Missbrauchsgefahr
  - A anmelden, B machen
  - Illegale Auswertungen → Woher weiß man davon?
    - » Kein Beweisverwertungsverbot in Österreich!

F I M

# Fragen?

**Vielen Dank für Ihre Aufmerksamkeit!**