

Elektronische Leistungs- und Verhaltenskontrolle

„Big Brother“ im Betrieb?
Betriebsrätemesse
Berlin
27. September 2004
Claudia Schertel



Kurzvorstellung

- | | | |
|--|---|--|
| ▪ Selbstständige
Rechtsanwältin
mit
Schwerpunkt
Arbeitsrecht | ▪ Projektleitung
(ver.di)
OnForTe
Onlinerechte für
Beschäftigte | ▪ Lehrbeauftragte
an der FH
Frankfurt/M. für
Datenschutz und
Datensicherheit |
|--|---|--|



Kurzvorstellung

Wer oder was ist **OnForTe**?

- Online Forum Telearbeit,
- ein virtuelles ExpertInnennetzwerk,
- berät seit 1997 **arbeitnehmerorientiert** zu den Themen „**Arbeiten, Lernen und Kommunizieren im Netz**“



Arbeiten, Lernen und Kommunizieren im Netz



Basisinformation
Einzelfallberatung
Seminare, Workshops
Outboundaktionen

200 Veranstaltungen
400 Veröffentlichungen
20.000 Hotlineanrufe

www.onforte.de
01805-245678



Entwicklungen bei OnForTe

- Vom Projektstatus zum integrierten Bestandteil der ver.di-innotec gGmbH (seit Januar 04)
- ver.di-innotec gGmbH ist ein Kooperationsbüro
- schafft stabile Brücken für eine humane Arbeitswelt
Innovation – Humanität
Technik – Mensch



Geschäftsfelder von ver.di-innotec

- Wissenschaftsprojekte und Forschungskooperation
- Bildung und Weiterbildung
- Transfer von sozialen Gestaltungsansätzen
- Kommunikation und Öffentlichkeitsarbeit



Thema: Elektronische Leistungs- und Verhaltenskontrolle

1. Arbeitnehmerdatenschutz - worum geht es?
2. Rechtlicher Rahmen nach geltendem Recht
3. Praktische Auswirkungen
4. Fazit



1. Arbeitnehmerdatenschutz – Worum geht es?

- Wahrung der Persönlichkeitsrechte von Beschäftigten
- Vermeidung ausufernder Verhaltens- und Leistungskontrollen
- Schaffung eines ausgewogenen Interessenausgleichs zwischen Arbeitnehmern und Arbeitgebern

Schutz der Persönlichkeitsrechte – nicht unmöglich, aber....

- schwieriger
- im unterschiedlichen Maß durchsetzbar
- abhängig von der konkreten betrieblichen Situation
- abhängig von der Durchsetzungsmacht
 - der / des Einzelnen und
 - des Betriebsrats
- Trend hin zu weniger Rechten wird stärker

Konkret

- Aktuelle Situation: Spezifische gesetzliche Normen für einen effektiven Arbeitnehmerdatenschutz fehlen in der BRD noch immer
- Deshalb: Bewertung des bestehenden Schutzrahmens muss sich an (lückenhaften) allgemeinen
 - individuellen und
 - kollektiven Rechtsnormen
- orientieren

Probleme

- Bestehende gesetzliche Normen treffen auf die neuen betriebliche Sachverhalte nur teilweise zu
- In der Praxis bleibt damit oft nur der Rückgriff auf die Vorgaben der Rechtsprechung
- Diese ist nicht abschließend verbindlich, sondern wandelbar

Die Praxis – ein paar Beispiele aus der juristischen Diskussion

- Kontrolle von Inhalten / Mitlesen von E-Mails
- „Intranet Driven Company“
- Transnationale Datenverarbeitung
- Videoüberwachung
- Fleadboard /RFID
- usw.



Kontrolle von Inhalten / Mitlesen von E-Mails

- Immer mehr Arbeitgeber wollen
 - Inhalte von E-Mails lesen und
 - Zugriffe auf Internet / Intranet-Seiten protokollieren
- Problem: Klare gesetzliche Verbote des Mitlesens gibt es nicht – damit ist es in bestimmten Fällen aus juristischer Sicht nicht generell unzulässig!



Intranet Driven Company

- Bündelung bekannter "Organisationssoftware" zu einem einheitlichen System mit Basis Intranet (Internet)
- Folge: Neue Möglichkeiten – und neue Kontrollen wie etwa
 - Aufgabenmanagement
 - Dokumentensharing
 - Einheitliche Terminkalender
 - Protokollierte Chats usw.



Transnationale Datenverarbeitung

- Nationale Grenzen sind in der IT-Welt kein Hindernis mehr
- Beispiele aus dem HR-Bereich
 - Der zentrale Server steht noch in der BRD, wird aber aus dem europäischen Ausland von Mitarbeitern des Unternehmens gemanagt
 - Der zentrale Server steht in den USA – und wird von Mitarbeitern eines Schwesterunternehmens gemanagt (datenschutzrechtlich nach Meinung der zuständigen Aufsichtsbehörde bei Vorliegen entsprechender Verträge zulässig)
 - Der zentrale Server steht irgendwo - und wird von Mitarbeitern eines „IT-Outsourcers“ gemanagt



Weitere Beispiele...

- Videoüberwachung am Arbeitsplatz
- RFID-Chips (Funketiketten)
- Einsatz von Fleetboards - telematikgestützter Internetdienst /Flottenmanagement, der uneingeschränkten Zugriff auf Informationen und Dienste ermöglicht, zudem breites Spektrum an integrierten Diensten (Fahrweiseanalyse etc.)

2. Rechtlicher Rahmen nach geltendem Recht

- Die zentrale Regelung – das BDSG
- Daneben Spezialgesetze
- Relevanten Normen des BDSG sind insbes.
 - allgemeine Vorgaben wie § 4 Abs. 1 BDSG (keine Verarbeitung ohne gesetzliche Erlaubnistatbestände oder ohne freiwillige Einwilligung der Betroffenen)
 - § 3a BDSG (allgemeiner Grundsatz der Datenvermeidung oder Datensparsamkeit)
 - § 28 Abs. 1 BDSG (beispielhafte Erlaubnistatbestände wie z.B. Vorliegen eines Vertrags)

daneben Spezialgesetze

- In Abhängigkeit von der konkreten Ausgestaltung des Einzelfalls kommen Spezialnormen wie insbesondere
 - Telekommunikationsgesetz (TKG) und
 - Teledienstegesetz (TDG)
- zur Anwendung

Problemfeld: Internet

- Die Praxis: Die Auswirkungen / Wechselwirkungen der unterschiedlichen Gesetzesmaterien sind selbst für Juristen nicht immer überschaubar
- Der Grund: Mangels Arbeitnehmerdatenschutzrecht kommen allgemeine datenschutzrechtlichen Vorgaben zur Anwendung
- Die Folge: Es ist zu differenzieren
 - nach ausschließlicher dienstlicher Nutzung und
 - nach zugelassener Privatnutzung

Privatnutzung verboten

- Arbeitgeber kann Privatnutzung verbieten
- Aber: Auch im dienstlichen Bereich gibt es persönliche Kommunikation (etwa mit dem Betriebsarzt, dem Betriebsrat, dem betrieblichen Datenschutzbeauftragten)
- Hieraus folgt: Mitlesen aller E-Mails ist z.B. nicht zulässig.

Zugelassene Privatnutzung

- Ist die private Nutzung zulässig
 - kommen neben BDSG Sonderregelungen wie § 85 Abs. 2 TKG / § 3 Nr. 1 TDG zur Anwendung, weil der Arbeitgeber bezüglich des „Privatanteils“ zum „Provider“ wird
- Die Konsequenz
 - Verschärfte Datenschutzvorschriften gem. der §§ 85 ff. TKG
 - Anwendbarkeit des TDDSG

Folge

- Wird die private Nutzung eingeräumt, müssen vom Arbeitgeber die entsprechenden Datenschutzvorschriften beachtet werden
- Auswirkung:
 - z.B. Besondere technische Schutzmaßnahmen gem. § 87 TKG treffen oder
 - Beschränkte Nutzung anfallender Daten gem. § 6 TDDSG

Weitere Folge in der Praxis...

- Verbietet der Arbeitgeber die Privatnutzung nur halbherzig (augenzwinkernd),
- um die Anwendbarkeit des Telekommunikationsrechts zu unterlaufen, besteht
- im Streitfall für Arbeitnehmer ein erhebliches Beweisrisiko, falls sie tatsächlich privat nutzen ...

Konkret: Intranet/Internet

- Arbeitgeber kann
 - Nutzungsgrad / -tiefe vorgeben
 - Privatnutzung verbieten – dann nur ausnahmsweise zulässig
 - kann Maß der Privatnutzung festlegen (gelegentlich/zeitbeschränkt/immer)
- Arbeitgeber darf Inhalte
 - bei dienstliche Nutzung nur in bestimmten Fällen,
 - bei privater Nutzung nicht und
 - bei Vermischung dienstlicher / privater Nutzung nur in definierten Ausnahmefällen kontrollieren



Konkret: E-Mail

- Ähnlich wie bei Internet/Intranet Verbot der Privatnutzung möglich
- Arbeitnehmer können dann aber verlangen, dass ihr Namen nicht Bestandteil der Adresse wird
- Heimliche Kontrollen von dienstlichen und erst recht von privaten E-Mails sind unzulässig / Telekommunikationsgeheimnis gilt



Ergänzend zu beachten: Allgemeine Rechtsgrundsätze / Rechtsprechung

- Wo die Anwendbarkeit einschlägiger Gesetze endet, wird der Arbeitnehmerdatenschutz in der BRD durch Rechtsprechung (insbes. des BAG) bestimmt
- Ergebnis ist eine nur für Insider verständliche Regelungslandschaft
- Beispiel: Juristische Zulässigkeit von Inhaltskontrollen durch Arbeitgeber



Juristische Zulässigkeit

- Für die Zulässigkeit von Inhaltskontrollen sind neben datenschutzrechtlichen Normen insbesondere
 - arbeitsrechtliche und
 - verfassungsrechtlicheGrundsätzen bedeutsam.



Inhaltskontrollen – arbeitsrechtliche Grundsätze

- Kontrollen (Leistungs- und Verhaltenskontrollen) sind juristisch nicht grundsätzlich ausgeschlossen
- Sie müssen aber offen und für die Betroffenen nachvollziehbar sein
- Wichtig: Persönlichkeitsrechte und das BDSG gelten auch im Arbeitsverhältnis
- Folge: Widersprüchliche Interessen sind gegeneinander abzuwägen



Grundrechte – Verfassungsrechtliche Vorgaben

- Allgemeine Vorgaben sind zu beachten wie z.B.
 - R.I.S. = Befugnis des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen und
 - Allgemeines Persönlichkeitsrecht
- Folgen:
 - Totalkontrollen (etwa durch Video) sind unzulässig
 - Ständige Kontrolle ist in der Regel unzulässig



Grundrechte - Folgen

- Abwägung zwischen Interessen des Arbeitgebers und der Arbeitnehmer muss erfolgen
- Verhältnismäßigkeit muss beachtet werden
- Als Ergebnis sind nur die Eingriffe in Persönlichkeitsrechte zulässig, die unumgänglich sind

Zulässige Eingriffe - Beispiele

- Zulässig: z.B.
 - Überwachungsmaßnahmen, die Beschäftigte nur zufällig erfassen (sensible Industrieanlagen) oder
 - die in Gefährdungssituationen erfolgen
- Unzulässig: z.B.
 - alle Formen der Totalüberwachung, wenn diese ausschließlich der Beobachtung von Verhalten und Leistung dient

In jedem Fall unzulässig: Heimliches Kontrollieren von Inhalten

- Heimliches Mitlesen von E-Mails oder entsprechendes Protokollieren von Internet/Intranet-Aktionen verstößt gegen Persönlichkeitsrechte und ist unzulässig
- Beim Verdacht auf strafbare Handlungen kann nur die Justiz entsprechendes anordnen und durchführen

Dennoch

- es gibt keinen Grund für vorschnellen Optimismus.
- Die derzeitige Rechtssituation ist mit Blick auf die Herausforderungen im Bereich neuer Überwachungsmöglichkeiten am Ende ihrer Belastbarkeit angekommen.
- Denn

... das geltende Recht ist endlich

... und endet zu früh

■ Beispiele:

- Intranet Driven Company: Wichtige Punkte wie die Erteilung von Arbeitsanweisungen über das System (und die hiermit einhergehende elektronische Kontrolle) unterliegen allenfalls indirekt der Mitbestimmung
- Ansonsten könnten sich Beschäftigte nur persönlich zur Wehr setzen – was nicht karrierefördernd ist!
- Bei transnationaler Datenverarbeitung sind entweder komplexe Vertrags- und BV-Lösungen notwendig, um Rechte der Beschäftigten zu wahren
- oder der vertraute arbeitsrechtliche Standard ist nicht mehr realisierbar!

OnForTe
ARBEITEN, LERNEN,
KOMMUNIZIEREN IM NETZ



Hinzu kommen neue Problemfelder wie insbesondere ...

- der Umgang mit Einwilligungen der Arbeitnehmer in gesetzlich nicht zulässige Formen der Datenverarbeitung
- Gesetzlicher Ausgangspunkt: § 4 Abs. 1 BDSG
„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, sofern dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“

OnForTe
ARBEITEN, LERNEN,
KOMMUNIZIEREN IM NETZ



Freiwilligkeit der Einwilligung in Kontrollmaßnahmen des Arbeitgebers

- Grundsatz des § 4a BDSG: Wird eine nicht gesetzlich normierte Form der elektronischen Kontrolle vom Arbeitgeber gefordert, muss eine freiwillige Einwilligung der Arbeitnehmer vorliegen
- Damit stellt sich sofort die Frage: Was ist freiwillig?

„Freiwilligkeit von Einwilligungen“ im Arbeitsverhältnis – Stand der juristischen Diskussion

- Zur Diskussion stehen allgemeine Rechtsgüter wie
 - das allgemeine Persönlichkeitsrecht
 - das Recht am eigenen Bild und
 - das Recht auf informationelle Selbstbestimmung
- Die Rechtsprechung hierzu ist unklar

Position der Rechtsprechung

- Mittelbare Befassung mit dem Thema „Einwilligung“ in Entscheidungen des Bundesverfassungsgericht, des Bundesgerichtshofs in Straf- bzw. Zivilsachen und des Bundesarbeitsgerichts
- Zumeist zum Thema „Zulässigkeit des Mithörens von Telefongesprächen“
- D.h. Einzelentscheidungen etwa zur Frage „Kontrolle durch Videokameras“ u.ä.
- Unterschiedliche Entscheidungslinien

Entscheidungslinien I

- Bundesverfassungsgericht
 - Hohe Anforderungen an die Wirksamkeit einer Einwilligung
 - Bloße Kenntnis einer Abhörmöglichkeit beseitigt den bestehenden Grundrechtsschutz nicht
 - Folge: Einwilligung trägt Eingriff in Grundrechte nicht

Entscheidungslinien II

- Bundesgerichtshof
 - Reduzierte Anforderungen an die Wirksamkeit einer Einwilligung weil
 - Mithören von Telefongesprächen im Wirtschafts- und Geschäftsleben inzwischen gang und gäbe ist
 - Fernmeldegeheimnis keinem Gesprächspartner die Einbeziehung eines Dritten in den Kommunikationsvorgang verbietet (1999 !)
 - Vertraulichkeit durch ausdrückliche Aufforderung des anderen Kommunikationspartners erreicht werden kann



Entscheidungslinien III

- Bundesarbeitsgericht
 - Hohe Anforderungen an die Wirksamkeit einer Einwilligung entsprechend der Position des BVerfG
 - Vorherige Information unumgänglich
 - Recht am eigenen Wort besteht auch im Arbeitsverhältnis uneingeschränkt
 - Wer mithören will, muss dies aktiv offenbaren



3. Folgen

- Jeder schafft sich das Recht, das er gerade braucht
- Plastisches Beispiel:
 - Umgang mit individuellen Einwilligungen versus
 - Sicherung des Rechts auf informationelle Selbstbestimmung

Dennoch gibt es Grenzen des Zulässigen

- Bezüglich der Frage einer wirksamen Einwilligung tatsächlich kein Dissens in der Rechtsprechung
- Auch der BGH verlangt wirksame Einwilligung mindestens eines Partners der Kommunikation
- Heimliche Überwachungsmaßnahmen bleiben schon aus verfassungsrechtlicher Sicht im Regelfall unzulässig (auch in Call Centern, mit Spyware, im Bereich E-Mail, Internet, Intranet usw.)
- **Folge:** Der Arbeitgeber benötigt für gewollte Überwachungsmaßnahmen eine **wirksame** Einwilligung der Beschäftigten

Anforderungen an Einwilligungen

- Grundrechtsverzicht im Arbeitsverhältnis möglich, sofern Kernbereich gewahrt bleibt
- Verbindet sich
 - mit einer geforderten Einwilligung ein Eingriff in Grundrechte von Beschäftigten,
 - muss eine Abwägung der unterschiedlichen Rechtsgüter erfolgen.
- Einwilligung kann demgemäss nur verlangt werden, wenn Maßnahmen erforderlich und verhältnismäßig sind (=Beweislast liegt beim Arbeitgeber).
- Unumgängliche Eingriffe in Rechtsgüter der Beschäftigten müssen so gering und so schonend wie möglich sein



Wirksamkeit von Einwilligungen

- Freiwilligkeit (= kein „Druck“ oder keine „Zwangslage“) muss gegeben sein
- Die Einwilligung muss auf Basis ausreichender Kenntnis der Sachlage und der Konsequenzen des eigenen Handelns erfolgen
- Umfang und Ausmaß der Einwilligung müssen konkret festgelegt sein



Eindeutiges Ergebnis der juristischen Bewertung

- Greifen Überwachungsmaßnahmen im Arbeitsverhältnis in Grundrechte der Beschäftigten ein, sind an die Wirksamkeit einer Einwilligung hohe Anforderungen zu stellen
- Das Interesse des Arbeitgebers ist kein alleiniges Entscheidungskriterium
- Ziel ist vielmehr die Wahrung der Rechte der Beschäftigten
- Einwilligung kann nicht als Mittel zur Ausbehebung von Grundrechten verwendet werden

Aber: Probleme in der Praxis

- Vorrangig müssen Betroffene im Streitfall ihre Rechte selbst wahrnehmen – was nicht immer karrierefördernd ist
- Wo Betriebsräte bestehen, können diese Verhaltens- und Leistungskontrollen im Rahmen von § 87 Abs. 1 Ziff. 6 und 7 BetrVG regeln, nicht aber verhindern
- Hinzu kommen Änderung der gesetzlichen Grundlagen als Folge der Gesetzesänderungen nach dem 11. September (und hieraus folgend wahrscheinliche Änderungen der Rechtsprechung)

Zurück zur Ausgangsfrage

- Der Schutz der Persönlichkeitsrechte von Beschäftigten wird als Folge
 - der sich ändernden tatsächlichen Situation,
 - der veränderten gesetzlichen Grundlagen sowie
 - des Fehlens gesetzgeberischen Handelns
- immer schwerer.

Auf der individuellen Ebene

- werden direkte und indirekte Faktoren wie beispielsweise
 - die Internationalisierung der IT-Landschaften,
 - die Verarbeitung von Arbeitnehmerdaten in grenzüberschreitenden Systemen, aber auch
 - die „Deregulierung“ des Arbeitsrechts (z.B. immer ausuferndere Befristungsmöglichkeiten)
- dazu führen, dass die persönliche Wahrnehmung von Rechten für die Betroffenen ein zu großes Risiko wird.

Auf der kollektiven Ebene

- sehen sich Betriebsräte immer mehr „in die Ecke gedrängt“
- IT-Themen treten gegenüber anderen Problemen wie etwa Betriebsänderungen und/oder Stellenabbau in den Hintergrund
- Hinzu kommt, dass die Komplexität des Themas für viele Betriebsräte fachlich eine Überforderung beinhaltet, die zumeist nicht durch Schulungsmaßnahmen aufgehoben werden kann.



Konsequenz

- Der Schutz von Persönlichkeitsrechten der Beschäftigten wird in vielen Bereichen ausgehöhlt.
- Das Recht auf informationelle Selbstbestimmung wird in der Praxis an vielen Stellen beschnitten
- Dieser Trend wird sich mit jedem Technikschrift beschleunigen und verschärfen



4. Fazit: Gegenmaßnahmen

- Ausnutzen bestehender rechtlicher Möglichkeiten insbesondere auf der kollektiven Ebene
- Verankerung der neuen Risiken in den Köpfen der Betroffenen
- Wiederholung der Forderung nach einschlägigen und wirksamen gesetzlichen Regelungen.

