DVD Deutsche Vereinigung für Datenschutz e. V.

# Pathologie des Arbeitnehmerdatenschutzes

Karin Schuler, Deutsche Vereinigung für Datenschutz e.V.

Vortrag zur Sommerakademie 2009

Obwohl es im IT-Bereich recht gebräuchlich ist, Metaphern aus dem medizinisch-biologischen Sprachraum zu bemühen (man denke nur an Viren oder Würmer) haben derartige Vergleiche immer ihre Schwächen. Auch sind die Analogien meist nur von begrenzter Gültigkeit. Dies vorausschickend habe ich dennoch den ursprünglich von den Veranstaltern vorgeschlagenen Titel beibehalten: er ist einfach bestechend plakativ für ein Thema, das sich kaum noch emotionslos vortragen lässt – nach allem, was in den letzten Jahrzehnten passiert ist – oder eher: nicht passiert ist. Und so möchte ich Ihnen heute einige der aus meiner Sicht wesentlichen pathologischen, also krankmachenden Phänomene beschreiben, die dem Arbeitnehmerdatenschutz seit langem zusetzen und den Patienten immer mehr schwächen. Begreift man nämlich Pathologie auch als Mittel zur Qualitätssicherung – was ist schief gegangen und wie kann man das in Zukunft verhindern? – dann hat der Patient eine solche Betrachtung wirklich nötig.

Woran also krankt er? Seit nahezu 20 Jahren bin ich beruflich und ehrenamtlich auch mit Fragen des Arbeitnehmerdatenschutzes befasst: sowohl als Sachverständige für Betriebs- und Personalräte als auch bei der Unterstützung betrieblicher Datenschutzbeauftragter. Die in der Praxis auftretenden Probleme sind nicht nur mir, sondern vielen Kolleginnen und Kollegen nur allzu vertraut. Zur Unzulänglichkeit und Uneindeutigkeit gesetzlicher Vorgaben und Schutzmaßnahmen für Beschäftigte gibt es unzählige gute Erörterungen, Abhandlungen und systematische Arbeiten. Warum also, frage ich mich, scheinen sich

Gesetzesmacher –offizielle und andere- berufen zu fühlen, nur nach eigenem Kenntnisstand Gesetzentwürfe in die Gegend zu blasen, offenbar ohne auch nur das in teilweise langjähriger Diskussion entstandene Wissen zur Kenntnis zu nehmen?

Es ist schon eine merkwürdige Krankheit, an der der Arbeitnehmerdatenschutz da leidet. Im Folgenden einige, durchaus nicht vollständige Gedanken zu ihrem Wesen und wesentlichen Phänomenen. Ich stelle zu diesem Zweck derer sechs heraus, die mir besonders schädlich erscheinen. Ich weise vorsorglich darauf hin, dass ich trotz der teils etwas polemischen Zuspitzung anschließend gerne sachlich weiterdiskutiere.

1. Verschleppen und Verschlucken
2. Intrigieren und Verhindern
3. Ignorieren
4. Verbiegen, Vertuschen und Verniedlichen
5. Wegschauen und Wegschieben
6. Denkfaulheit!

## Verschleppen und Verschlucken

Seit Jahrzehnten wird von verschiedensten Akteuren auf die Notwendigkeit eines Arbeitnehmerdatenschutzgesetzes hingewiesen. Sogar über Norbert Blüm wird berichtet, er habe bereits an Gesetzentwürfen gearbeitet, diese jedoch nie vorgelegt. Mit dem Beginn der rot-grünen Koalition, die das Arbeitnehmer-Datenschutzgesetz in ihr Koalitionsprogramm aufgenommen hatte, waren viele Hoffnungen

verbunden, die sich jedoch im Nachhinein als vergeblich herausstellten. Verbände aller Couleur betonen und begründen seit Jahren, wie wichtig ein solches Gesetz sei. Der DGB hat ein Eckpunktepapier vorgelegt, die Deutsche Vereinigung für Datenschutz wiederholt Stellung zum Erfordernis eines solchen Gesetzes genommen, um nur zwei Organisationen von vielen zu nennen. Selbst der Bundesrat mahnte 2005 an, dass das Vorhaben endlich umgesetzt werden solle.

Die Stimmen, die ein solches Gesetz fordern sind so zahlreich, dass man sich irgendwann fragen muss: wenn doch derart viele Gruppen dafür sind – einschließlich einer immerhin zwei Legislaturen dauernden Regierung – warum, um Himmels willen, kommt dabei nichts Vernünftiges heraus? Andere Redner werden auf diese Frage heute vermutlich näher eingehen. Ich beschränke mich darauf, das Phänomen „Verschleppung“ als eine Auswirkung einer offensichtlich ungünstigen politischen Gemengelage zu konstatieren. Man könnte auch sagen, Generationen hochbezahlter Beamte und Politiker, die mit der Arbeit beauftragt warten, haben ihre Arbeit nicht getan. Eine beschämende und gleichermaßen erschreckende Bilanz, denn was man sich offensichtlich ohne Gehaltseinbuße und Arbeitsplatzverlust als Regierungsmitglied leisten kann – nämlich Arbeitsverweigerung- würde bei normalen Arbeitnehmern zu sofortiger Kündigung führen.

Unglücklicherweise heißt die andere Seite der Medaille „hektische Betriebsamkeit“ und diese kommt immer dann zum Einsatz, wenn Skandale zu öffentlicher Empörung führen. Um die Öffentlichkeit zu beruhigen und Handlungsfähigkeit zu demonstrieren werden dann Pseudoaktivitäten eingeleitet, die zwar niemandem wehtun, aber auch

keine Verbesserung bringen. Trostpflästerchen fürs Arbeitnehmervolk, gewissermaßen. Dass man sich an solchen Schnellschüssen regelmäßig verschluckt, lässt sich an der Historie des Flickenteppichs BDSG sehr schön bestaunen. Und die mit heißer Nadel gestrickten neuen Flicken setzen diese Tradition fort. Der §32 im neuen BDSG ist so ein Beispiel. Diesen Paragraphen kann man nur als lächerlich bezeichnen. Je nach Lesart ist er entweder entbehrlich – wenn man nämlich davon ausgeht, dass er lediglich konstatiert, dass das Beschäftigungsverhältnis als Vertrag die Zulässigkeitsgrundlage für die Verarbeitung der Mitarbeiterdaten durch den Arbeitgeber bildet – oder er ist vollkommen unpraktikabel, weil er, genau gelesen, die zulässigen Verarbeitungen durch den Arbeitgeber so einschränkt, dass weder die Protokollierung der Nutzung von Systemen, noch der Betrieb von Ticket-Systemen, noch von Kantinenabrechnungssystemen zweifelsfrei zulässig wären. Denn sie sind weder für die Durchführung noch die Beendigung des Beschäftigungsverhältnisses erforderlich. Und diese Aufzählung könnte man lange fortsetzen.

Warum auch soll es dem Gesetzgeber anders ergehen, als jedem anderen Menschen: wer zu lange geschlafen hat und nach dem Aufwachen zu große Brocken herunterschlingt, läuft Gefahr, sich im Halbschlaf zu verschlucken.

## Intrigieren und Verhindern

Die Frage, wie es sein kann, dass scheinbar wesentliche gesellschaftliche Kräfte ein Arbeitnehmerdatenschutzgesetz wollen, aber dennoch nichts passiert, bzw. Bemühungen seit Jahrzehnten immer

wieder im Sande verlaufen, führt einen direkt zu den Gegnern dieser Idee.

Die so genannten Interessensvertretungen der Wirtschaft versuchen mit offensichtlich gutem Erfolg, jegliche Bemühungen in diese Richtung zu torpedieren. Es ist bezeichnend, dass sie diese Auseinandersetzung weder inhaltlich noch organisatorisch mit offenem Visier führen.

Sachliche Argumente sind rar, stattdessen wird mit angstbesetzten Kampfbegriffen Panik in der eigenen Mitgliederschaft und bei Politikern geschürt. Angst vor der Einschränkung unternehmerischer Freiheit und Handlungsfähigkeit, Angst vor Überbürokratisierung und Angst vor Arbeitsplatzverlust. Wie gut und unmittelbar dieser durchsichtige Kunstgriff bei den angesprochenen Politikern wirkt, konnte erst kürzlich bei der Debatte im Innenausschuss um die Änderungen des BDSG wieder bestaunt werden.

Man ist erstaunt, welche Ängste die schlichte Forderung nach angemessenen Regelungen für die Persönlichkeitsrechte von Arbeitnehmerinnen und Arbeitnehmern in Teilen der Wirtschaft auslöst. Was sagt das über deren Verständnis von Arbeitnehmerrechten aus? Alles nur Verhandlungsmasse?

Ich schenke mir Deutungsversuche der weitgehend argumentationsfreien Angstkampagnen, die einige Wirtschaftsverbände veranstalten. Da es aber keine weiteren Gegner zu geben scheint, muss man wohl annehmen, dass diese Gruppe es einerseits schafft, Regierungen und starke gesellschaftliche Teile in Schach zu halten und

dass sie das Ziel andererseits größtenteils durch verdeckte Lobbyarbeit und aufwändige Einzelbearbeitung von Abgeordneten verfolgt.

**Ignorieren**

Wie es viele Unternehmen schaffen, die Persönlichkeitsrechte ihrer Beschäftigten schlichtweg zu ignorieren, haben wir im letzten Jahr zur Genüge in der Presse verfolgen können. Auch Frau Prof. Däubler-Gmelin wird hierzu sicherlich noch tiefere Einblicke gewähren. Aus meiner beruflichen und ehrenamtlichen Tätigkeit habe ich inzwischen ein Bild gewonnen, wonach mich a) diese medial aufbereiteten Skandale nicht wirklich erstaunt haben (wie übrigens viele meiner Kolleginnen und Kollegen) und b) mir die den Skandalen zugrundeliegenden Verhaltensweisen und Einstellungen weit verbreitet und die daraus resultierenden datenschutzrechtlichen Grauzonen in Unternehmen gang und gäbe scheinen.

Das Unrechtsbewusstsein in allen Führungsebenen ist, vorsichtig formuliert, stark unterentwickelt und es ist eher schon der Normalfall, dass man als Mitglied der Führungsebene über die Grundlagen des Datenschutzes allgemein und des Arbeitnehmerdatenschutzes im Besonderen nicht viel weiß. Insbesondere weiß man häufig nicht, dass man als Vorstand oder Geschäftsführer für die Einhaltung des Datenschutzes verantwortlich ist – und eben nicht der Datenschutzbeauftragte oder gar der IT-Leiter.

Wer in deutsche Unternehmen fragt, welche der Führungsmitglieder regelmäßig durch ihren Datenschutzbeauftragten geschult werden, wird meist keine erfreulichen Antworten erhalten. Hier kann ich auch Teile

meiner eigenen Zunft nicht von der Kritik ausnehmen. Wie soll die geforderte Unterweisung jemand leisten, der als externer DSB anbietet, ein mittelständisches Unternehmen für 100 EUR im Monat zu betreuen? Aber auch für engagierte Datenschutzbeauftragte ist es natürlich nicht immer angenehm, darauf zu bestehen, dass auch der Chef, die Geschäftsführung, der Vorstand bitteschön zur Unterweisung anzutreten haben. Genau das aber sieht das Gesetz vor und die Unterweisungen sind, das ist meine Erfahrung, gerade in den oberen Etagen, meist auch bitter nötig. Auch wenn ich mir damit im Arbeitnehmerlager nicht nur Freunde mache: Einen sehr großen Anteil an Datenschutzverstößen gegenüber Beschäftigten hat die Ignoranz – fast mehr als der böse Wille. Was nicht die Auswirkungen der Verstöße mindert – aber die Möglichkeiten, solche in Zukunft zu vermeiden, denn Ignoranz ist heilbar, böser Wille nur schlecht. Und ich rede da ausdrücklich von den Unternehmen selbst, nicht von deren Verbänden.

Wozu Ignoranz führen kann, lässt sich landauf landab in Betrieben besichtigen: Nicht nur die Datenschutzvorschriften des BDSG werden ignoriert, sondern auch ein weiterer wesentlicher Baustein des Arbeitnehmerdatenschutzes: die Mitbestimmung. Dass gerade durch die Zustimmungserfordernis der Arbeitnehmervertretung die Persönlichkeitsrechte von Beschäftigten gewahrt werden, gehört jedoch leider nicht zum Allgemeinwissen.

Auch betriebliche Datenschutzbeauftragte bekleckern sich in diesen Fragen nicht immer mit Ruhm: Dass sie Verfahren, in denen Mitarbeiterdaten verarbeitet werden, als unzulässig einstufen müssten, wenn die Mitbestimmung nicht gewahrt wurde, weil die Voraussetzung

der Rechtmäßigkeit nicht gewahrt wurde, scheint den wenigsten bewusst zu sein.

Natürlich sind die Skandale des vergangenen Jahres teilweise empörend. Man gewinnt – vermutlich zu Recht- den Eindruck, je größer ein Unternehmen ist, desto mehr scheint es sich Rechtsbegriffe nach eigenem Geschmack zurechtzubiegen. Aber das Problem ist nur in der Öffentlichkeit auf einmal besonders deutlich geworden. Begonnen hat es schon vor vielen, vielen Jahren und in Fachkreisen ist niemand wirklich erstaunt über die Vorgänge, die jetzt als Skandale gehandelt werden.

Viele Kolleginnen und Kollegen bestätigen mir meine eigenen Beobachtungen, die im übrigen zu den diesjährigen, soeben gesichteten Nominierungen für die BigBrotherAwards passen: die Skandale stellen nur die Spitze des Eisbergs dar. In Unternehmen aller Größenordnungen stellen Persönlichkeitsrechte von Beschäftigten keine signifikante Größe für die Unternehmensführung dar.

Ich bin beileibe nicht die einzige, die regelmäßig gefragt wurde: schön, Frau Schuler, so wäre es also vorbildlich...und was kostet es uns, wenn wir das nicht machen und wie wahrscheinlich ist es, dass die Aufsichtsbehörde das prüft? Mit dem Betriebsrat werden wir uns schon einig.

Aber auch Länder und Gesetzgeber ignorieren seit Jahren hartnäckig Umsetzungsdefizite. Obwohl immer mehr grundlegende und weit verbreitete Fehlentwicklungen in Unternehmen sichtbar wurden, wird nichts getan, um die Ausstattung und Arbeitssituation der Aufsichtsbehörden zu verbessern.

Es scheint mir beispielsweise eher die Regel als die Ausnahme zu sein, dass Unternehmen ab einer gewissen Größenordnung innerhalb ihres Konzerns Arbeitnehmerdaten hin- und herschieben ohne die damit datenschutzrechtlich verbundene Übermittlung überhaupt als solche wahrzunehmen und entsprechende Zulässigkeitsprüfungen durchzuführen. Einen Schritt weiter gehen regelmäßig internationale Unternehmen, die wie selbstverständlich Arbeitnehmerdaten aus Personalakten, Bewertungssystemen, Zeiterfassung etc. an eine außereuropäische Mutter liefern – und zwar ohne dass es hierzu Verträge gemäß Standardvertragsklauseln, genehmigte corporate binding rules oder safe-harbor- Mitgliedschaft gäbe. Ob die Mutter in USA, Japan oder Russland sitzt: häufiger treffe ich auf Unternehmen, die bestenfalls seit Jahren an einer Lösung herumdoktern – oder das zumindest behaupten, um den Betriebsrat ein wenig in Schach zu halten. Seltener sind diejenigen, die tatsächlich eine Zulässigkeitsgrundlage für Ihre außereuropäische Datenübermittlung geschaffen haben. Wenn solches Herumdoktern aber jahrelang möglich ist, ohne dass eine Aufsichtsbehörde dies auch nur mitbekommt, geschweige denn kontrollieren oder beanstanden kann, dann stimmt mit der Kontrollinstanz ganz offensichtlich etwas nicht. Eine Behörde, deren Existenz man derart ungestraft ignorieren kann, ist ganz offensichtlich hoffnungslos unterbesetzt und von Gesetzgeber und Land mit ihren vielen Aufgaben alleine gelassen.

## Verbiegen, Vertuschen, Verniedlichen

Und damit wäre man bei den Auswirkungen von Ignoranz und –in einigen Fällen sicher auch– bösem Willen. Beides führt in der Praxis zu rechtlich nicht haltbaren aber umso phantasievolleren „Interpretationen“ der Gesetzeslage. Aber: wo kein Kläger, da kein Richter! Und wer könnte schon der Kläger sein? Die Aufsichtsbehörden sind, wie bereits dargestellt, seit Jahren chronisch unterbesetzt – gemessen an den ihnen zukommenden Aufgaben- und überlastet. Die personelle Besetzung bewegt sich von wenigen Mitarbeitern pro Land (im einstelligen Bereich) bis zu maximal 50 Mitarbeitern in wenigen besser ausgestatteten Bundesländern. Die meisten Länder müssen mit einem Stab von um die 20 Personen zurechtkommen. Selbst wenn man wohlwollend annimmt, dass eine Aufsichtsbehörde im Schnitt pro Jahr ca. 1000 Unternehmen besucht und prüft, dann müsste bei den in Deutschland laut Angaben des Statistischen Bundesamtes ca. 3,5 Mio. Unternehmen jedes Unternehmen statistisch gesehen alle 218 Jahre mit einer Prüfung rechnen müssen. Die Wahrscheinlichkeit, dass man geprüft wird, lässt sich also fast ignorieren. So ungern ich da sage (denn manche Unternehmen bekommen hier aus offensichtlichen Gründen sofort leuchtende Augen): in den 20 Jahren meiner Berufstätigkeit, in denen ich für rund hundert Unternehmen aller Größenordnungen (vom internationalen Großkonzern bis zum örtlichen Sportverein) tätig war, habe ich ein einziges Mal eine Vor-Ort-Prüfung einer Aufsichtsbehörde und ca. fünfmal schriftliche Aufklärungswünsche der Behörde erlebt. Dies suggeriert den Unternehmen jedenfalls nicht, dass der Persönlichkeitsschutz Beschäftigter und sonstiger Betroffener vom

Gesetzgeber selbst sehr ernst genommen würde. Wer sich niemals für die gemäß gesetzlicher Vorschriften nötigen Abwägungen, Verfahrensverzeichniseinträge oder die datenschutzgerechte Gestaltung seiner Prozesse verantworten muss, neigt dazu, Interpretationsspielraum unangemessen zu seinen Gunsten zu nutzen.

Und dann werden Verarbeitungszwecke so allgemein definiert, dass letztlich alles erlaubt ist, Löschfristen im Verfahrensverzeichnis bewusst vage gehalten, Personaldaten überhaupt nie gelöscht, Aufträge gemäß § 11 BDSG mit erbarmungswürdigen Vertragstexten erteilt, wenn überhaupt schriftlich und so könnte man weiter aufzählen.

Ein besonderes Phänomen ist zu beobachten, wenn Gesetze, die mit dem Datenschutz konkurrierende Ziele vorgeben, klarer formuliert sind als dieser: sie werden ohne weitere Abwägung buchstabengetreu befolgt. Dies geschieht unter anderem bei der Einrichtung von Whistleblowing-Systemen, bei der Korruptionsbekämpfung, bei Sicherungsmaßnahmen gemäß SOX (hier ist zusätzlich ein wirtschaftliches Interesse die Triebfeder!) und einigen anderen.

Reichen weder Ignorieren noch Verbiegen aus und werden Datenschutzverstöße innerbetrieblich moniert oder gar öffentlich angeprangert, wird gerne Zuflucht zur Vertuschung genommen: Am besten sollten Vorfälle gar nicht ans Licht kommen („das ist betriebsintern und geht keinen was an“). Einige Unternehmen gehen dabei nicht zimperlich mit so genannten „Nestbeschmutzern“ um. Die Nominierenden einiger BBA-Preisträger können davon ein Lied singen.

Lassen sich Vorfälle trotz aller Bemühungen nicht mehr unter der Decke halten, tritt man in die Phase der Verniedlichung („es ist doch nichts passiert“, „die anderen machen es doch auch so“).

Alles in allem ein Teufelskreis, denn die mangelnde Einsicht verhindert, dass aus Fehlern und Vorfällen gelernt und die Überprüfung eigener Prozesse eingeleitet wird.

**Wegschauen und Wegschieben**

Und zuletzt – zumindest als Anregung – haben auch Öffentlichkeit und die Betroffenen selbst zumindest einen gewissen Anteil an der langen Leidensgeschichte des Patienten.

Es reicht eben nicht, einmal im Jahr zur Verleihung der BigBrotherAwards zu gehen, mit dem Finger auf die Preisträger zu zeigen und sich dann wieder in die wohlige Datenschutzapathie zurückfallen zu lassen.

Sicher ist die Erfolgsgeschichte BBA auch eine Erfolgsgeschichte des Datenschutzes (und inzwischen sind die Nominierungen aus der Arbeitswelt zahlreich) aber nachhaltige Änderungen sind nur durch zähen, solidarischen Einsatz für die eigenen Rechte und die der Kolleginnen und Kollegen zu erzielen. Das ist oft weniger glamourös als die BBA-Gala, aber unverzichtbar für die Sache.

Es kann nämlich auch bedeuten, dass man als Administrator die Zivilcourage aufbringen muss, dem Chef die Auswertung der E-Mail-Konten zu verwehren oder den Betriebsrat über die heimlich installierte Schnüffelsoftware zu informieren.

Die bisher aufgeführten Krankheitsphänomene, so ärgerlich sie sind, werden durch ein aus meiner Sicht unverzeihliches Phänomen in den Schatten gestellt, nämlich

**Denkfaulheit**

Ich bezeichne damit die geradezu seuchenartige Erscheinung, sich mit gut klingenden Phrasen zufrieden zu geben und Dinge nicht zu Ende zu denken.

Die Unbestimmtheit mancher im Gesetz verwendeter Begriffe mag der Jurist gewohnt sein. Sie ist in der Praxis jedoch nur dann akzeptabel, wenn die Auslegung nicht zum alleinigen Recht einer einzelnen Partei wird. Im betrieblichen Alltag geschieht jedoch genau das, wie bereits zuvor dargestellt: phantasievolle Auslegung allerorten und kein Gegengewicht, das allzu dreiste Eskapaden begrenzen würde. Warum ein Gesetz sich zu schade sein soll, Begriffe, die es einführt und an zentraler Stelle nutzt, auch sauber zu definieren, bleibt ein Geheimnis.

Die Anträge unterschiedlicher Fraktionen zum Arbeitnehmerdatenschutz, die in der letzten Legislaturperiode gestellt wurden, sprechen da leider eine deutliche Sprache: eine derartige Häufung nicht hilfreicher, gar kontraproduktiver Forderungen lässt sich angesichts der jahrzehntelangen Fachdiskussion kaum noch erklären. Die Alibi-Anhörung des Ausschusses für Arbeit und Soziales im Mai dieses Jahres (immerhin eine ganze Stunde!) war dann auch erwartungsgemäß eher Zeitverschwendung als dass sie in irgendeiner Weise zum Erkenntnisgewinn beigetragen hätte – wenn man von der Erkenntnis absieht, dass sich die Fronten und Lager nicht wesentlich verschoben

haben und die so genannten Interessensvertreter der Wirtschaft sich nach wie vor darauf beschränken, statt Sachargumente auszutauschen, Ängste zu schüren.

Zur Illustration der Denkfaulheit hier einige Beispiele.

Am Begriff der „Zweckbestimmung“ lässt sich seit Jahrzehnten verfolgen, wie das Gesetz sich um Konkretisierung herumdrückt und weder Aufsichtsbehörden noch Datenschutzbeauftragte eine wirklich tragfähige Definition dessen geben (können), wie die Zweckbestimmung eines Verfahrens zu beschreiben ist. Zugegebenermaßen ist dies auch wirklich keine triviale Angelegenheit, aber in über 30 Jahren hätte man schon mal ein wenig Energie in die Entwicklung einer sauberen Definition stecken können.

In der betrieblichen Praxis führt dieses Defizit häufig zu unakzeptabler Definitionsjonglage des Arbeitgebers. Wenn die Zweckbestimmung bestimmter Daten oder einer Anwendung zu definieren ist, sind wir uns bei einem „extremen Ausreißer“ schnell einig: „Zu unseren Geschäftszwecken“ ist sicher nicht ausreichend. Aber was ist ausreichend? Wird beispielsweise erst einmal so etwas Schwammiges wie „Optimierung von Abläufen“ als Zweckbestimmung akzeptiert, so lassen sich hernach alle auf dieser Grundlage gesammelten Beschäftigtendaten (Tastenanschläge, minutiöse Überwachung von Außendienstmitarbeitern, sogar die Zahl der Toilettengänge) für fast alle denkbaren Auswertungen einsetzen, ohne, formal gesehen, den ursprünglich definierten Zweck zu ändern.

Was genau muss also in einem Verfahrensverzeichnis an der Stelle „Zweckbestimmung“ stehen, damit zum Beispiel auch der Betriebsrat etwas mit den Angaben anfangen kann?

Noch ein Beispiel: der § 31 BDSG zur besonderen Zweckbindung. Dass Daten, die nur für Zwecke der Datenschutz-Kontrolle, Datensicherung oder zur Sicherstellung ordnungsgemäßen Betriebs erhoben werden, dann auch nur für diese Zwecke genutzt werden dürfen, wird durch AG regelmäßig ausgehebelt. Dies geschieht beispielsweise durch die simple Festlegung, dass die Daten von vorneherein auch für Zwecke der Abrechnungskontrolle (Telefonvermittlungsrechner-Protokolle), des Abgleichs mit Zeitwirtschaftsdaten (Firewall- oder Zutrittskontrollprotokolle) gedacht sind. Der §31 ist in der Praxis ein zahnloser Tiger, weil er nicht, was zugegebenermaßen etwas mehr Nachdenken erfordert hätte, definiert, welche Daten hierunter fallen, sondern die Geltung von der beliebigen Anfangsentscheidung des Arbeitgebers abhängig macht. Jedes Systemprotokoll, das man „eigentlich“ eher als Hilfsmittel für den ordnungsgemäßen Betrieb verstehen würde, lässt sich auch noch für etwas Anderes, meist Arbeitnehmerüberwachung, nutzen. Wenn man nur die Weitsicht besitzt, dies von vorneherein zu definieren, ist der Schutz von § 31 wirkungslos. Es bleibt daher weitsichtigen Betriebsräten überlassen, dafür zu kämpfen, bestimmte Protokolle per Betriebsvereinbarung dem Schutz des § 31 zu unterwerfen.

Ein ähnlich schwammiger, augenwischerischer Begriff geistert seit einiger Zeit durch Gesetzentwürfe und Arbeitspapiere zum Arbeitnehmerdatenschutz: das Datenschutzkonzept. Hört sich gut an

und es gibt auch durchaus gut organisierte Unternehmen, die sehr gute Datenschutzkonzepte besitzen. Nur ist die Situation eben eine etwas andere, wenn dies plötzlich als Anforderung in einem Gesetz auftaucht. Will man alle Betriebe zwingen (möglicherweise auch ohne eigene Einsicht) ein solches Konzept vorzulegen, dann muss man schon definieren, was dessen Inhalt sein soll – wenn man nicht einen weiteren Papiertiger schaffen will, der sich nur auf den ersten Blick gut anhört, sich aber bei genauerem Nachdenken als Luftnummer entpuppt. Wie dick darf's denn sein? Reichen drei Seiten (schließlich ist ja nur ein Konzept, keine Richtlinie)? Oder müssen es doch 5 oder gar zehn Seiten sein? Sie finden meine Fragen albern und spitzfindig? Das sind jedoch genau die Fragen, die mir Unternehmen stellen, die eigentlich gar kein Datenschutzkonzept wollen, aber auf einmal vielleicht aus gesetzlichen Gründen ein solches erstellen müssen.

Dies Phänomen kennen wir übrigens schon: vom Verfahrensverzeichnis. Offen ungeliebte, gesetzliche Verpflichtung, die aus Prüfsicht (der Aufsichtsbehörde) vor allem einen Vorteil hat: man kann sofort erkennen, wenn es überhaupt keines gibt – und auch da gibt es noch mehr als genug Unternehmen, die diese Pflicht einfach ignorieren. Fragt der Betriebsrat im Rahmen eines Mitbestimmungsvorgangs zu einem EDV-System nach dem Verfahrensverzeichnis, sieht man nicht selten lange oder verständnislose Gesichter auf der anderen Seite. Andere Unternehmen haben der Form nach ein Verfahrensverzeichnis – häufig eines, das auf zwei DIN A-4-Seiten passt und das sie manchmal sogar noch als besonderes Zeichen ihrer Datenschutzfreundlichkeit im Internet veröffentlichen. Was man da allerdings zu sehen bekommt, ist häufig

das Papier nicht wert, auf das es geschrieben steht. Da werden in großen Unternehmen ganze fünf Datenkategorien identifiziert, die insgesamt drei Zwecken dienen und, wenn überhaupt „entsprechend gesetzlicher Löschfristen“ gelöscht werden. Beliebiger und inhaltsfreier geht’s nimmer!

Und leider kann man den Aufsichtbehörden hier eine unselige Beförderung dieses Trends nicht ganz absprechen: Das Formular, das seit Jahren als Ausfüllhilfe kursiert, ignoriert geflissentlich, dass die im gesetzlichen Katalog geforderten Angaben nicht alle auf gleicher logischer Ebene angesiedelt sind, sondern eine Matrix bilden. Es sind nämlich gerade für **jede Datenkategorie** die nachfolgenden Angaben zu Empfängern, Löschfristen, Zugriffsberechtigten etc. zu machen. Alles andere wäre auch vollkommen unsinnig.

Dies sind nur einige klassische Beispiele für Denkfaulheit bei Grundkonzeptionen, die allerdings weitreichende Folgen haben.

Dies schädliche Phänomen kann man nur durch solide Konkretisierung der Datenschutzprinzipien bekämpfen, im Bereich der Persönlichkeitsrechte von Beschäftigten durch ein Arbeitnehmerdatenschutzgesetz. Ein solches Gesetz muss auf den Grundlagen des BDSG aufbauen und durch konkrete, betriebsorientierte Regelungen einen Mehrwert für den Arbeitnehmerdatenschutz erzielen. Es muss sich an der betrieblichen Praxis orientieren und festlegen, wie beispielsweise die Prinzipien „Verbot mit Erlaubnisvorbehalt“, „Erforderlichkeit“, „Zweckbindung“ und „Transparenz“ in Bezug auf den Umgang mit Arbeitnehmerdaten umzusetzen sind. Dabei muss nicht

zuletzt auch solide, tragfähige Definitions- und Abgrenzungsarbeit geleistet werden. Ein zweites BDSG, bei dem nur die Worte „Betroffener“ durch „Beschäftigte“ und „verantwortliche Stelle“ durch „Arbeitgeber“ ersetzt würden, wäre nicht wünschenswert

Eine andere Auswirkung der Denkfaulheit zeigt sich in den vielfältigen Kollisionen der Datenschutzvorschriften mit anderen gesetzlichen Normen. Ein vertrautes Beispiel: Generationen von Betriebsräten schlagen sich, in Ratlosigkeit mit den Unternehmen vereint, mit den Implikationen privater Nutzungserlaubnis dienstlicher Internet-Zugänge herum. Bei Zulässigkeit privater Nutzung wird das Unternehmen nach den Buchstaben des Gesetzes zum Diensteanbieter und muss in der Folge strenge Vorgaben zum Umgang mit Verbindungsdaten und Inhaltsdaten beachten. Eine Situation, die weder inhaltlich angemessen, noch in der Praxis rechtssicher und gleichzeitig technisch akzeptabel zu lösen ist. Denn der sichere Betrieb einer IT-Infrastruktur in einem Unternehmen erfordert Schutzmechanismen, Protokollierungen und Sicherungskopien, die mit dem Fernmeldegeheimnis nicht vereinbar sind. Die eigentlich als Schutz gedachte Norm führt so im geschlossenen Umfeld eines Unternehmens dazu, dass entweder juristische Absicherungen zu treffen sind, deren Wirksamkeit je nach Bundesland unterschiedlich beurteilt wird (Einwilligungen der Arbeitnehmer) oder, viel häufiger, dass formal die private Nutzung untersagt wird. Was aber in der Regel nicht verhindert, dass dennoch z.B. private Mails geschickt werden. Erforderlich und zu Ende gedacht wäre daher eine Klarstellung, dass ein Unternehmen gerade nicht als Telekommunikationsdiensteanbieter im Sinne des TKG gilt, dass aber für

die transparente Gestaltung der Netzüberwachung und die betriebsöffentliche Dokumentation der Überwachungsmaßnahmen strenge, willkürverhindernde Vorschriften gelten, bzw. im Rahmen der Mitbestimmung vereinbart werden müssen.

Meine lange aber lange nicht vollständige Liste hat Ihnen hoffentlich einige Anregungen zur späteren Diskussion gegeben. Ich schließe mit der Hoffnung, dass der Patient noch nicht tot sein möge!