

info Sicherheit

Beiträge zu Fragen der Sicherheit in der Wirtschaft

03/2010

Die Zukunftsfragen der Sicherheit



**Russischer Agentenring-
die wahre Geschichte
Seite 5 .**

**Wirtschaftsspionage
aus Sicht von Innenminister
Uwe Schünemann
Seite 31 .**

**Unternehmenssicherheit
auf dem Prüfstand
Seite 34**

**Informationsschutz-
was ist zu tun?
Seite 40**

**Private Sicherheit-
quo vadis?
Seite 46**

**Datenschutz darf kein
„Tatenschutz werden“
Seite 48**

*Kriminalität und Spionage sind ein ernstes Thema für Deutschlands Unternehmen. Werden künftig die Möglichkeiten, sich gegen solche Angriffe zu schützen, in nicht akzeptabler Weise eingeschränkt?
Foto: Agentur Klarpunkt*

**Verband für Sicherheit in der
Wirtschaft Norddeutschland e. V**

**VSW
VSW
NORDDEUTSCHLAND**

VSWN- Vorsitzender Dau: Wer 5000-Meter-Lauf fordert, darf nicht zugleich Beine amputieren



1. Vorsitzender des VSWN und Vorstandsmitglied der ASW: Rolf-Wilhelm Dau. Foto: wm

Man könne von niemandem einen 5000-Meter-Lauf verlangen, wenn man ihm gleichzeitig beide Beine amputiert. Mit diesem plastischen Vergleich brachte der 1. Vorsitzende des Verbandes für Sicherheit in der Wirtschaft Norddeutschland e.V. (VSWN) und Vorstandsmitglied der Arbeitsgemeinschaft für Sicherheit in der Wirtschaft e.V. (ASW), Rolf-Wilhelm Dau, seine Bedenken gegen den am

25. August 2010 vom Bundeskabinett beschlossenen Entwurf eines Beschäftigtendatenschutzes auf den Punkt. „Sind gerade in den letzten Jahren Regelwerke wie KonTraG, Compliancevorgaben und Whistleblower in der Wirtschaft zum Selbstverständnis erhoben worden, um Transparenz und Regelkonformität zu fördern, so werden auf der anderen Seite aber die Durchsetzungsmöglichkeiten erschwert“, erklärte er wörtlich. Dieser Widerspruch werde leider bei vielen Betrachtungen völlig übersehen.

Das Thema habe eine große Bedeutung für die ASW, betonte Rolf-Wilhelm Dau. Unverständnis äußerte Rolf-Wilhelm Dau darüber, dass die ASW im Vorwege „nicht in der Form angesprochen worden war, wie es wünschenswert gewesen wäre“. Dies steht im Widerspruch zu den Aussagen des Bundesinnenministeriums, dass die „betroffenen Verbände und Sozialpartner (...) Gelegenheit (hatten), sich im Rahmen einer Anhörung zu dem Gesetzentwurf zu äußern“.

Im Gesetzgebungsverfahren, das der Einbringung des Gesetzentwurfes durch die Bundesregulierung nunmehr folgt, werde die ASW klar und eindeutig Position beziehen, machte der 1. Vorsitzende des VSWN und Mitglied des ASW-Vorstandes deutlich. Auf seine Initiative hin werde innerhalb der Arbeitsgemeinschaft für Sicherheit in der Wirtschaft eine Tischvorlage erarbeitet, die allen ASW- und VSWN-Vertretern eine Fakten- und Argumentationssamm-



Ein reales Beweisfoto: Der Täter bereitet seine Diebestour vor (links). Ein sichernder Blick. Täter handeln heimlich und verdeckt, die Überwachung aber soll offen sein. Zwei Sachverhalte, die nicht zusammenpassen können (rechts). Fotos: Agentur Klarpunkt

lung in die Hand gegeben werden soll. Spätestens bei der „Security Essen“ (5. bis 8. Oktober 2010), werde dieses Papier aller Voraussicht nach auf dem gemeinsamen Stand der ASW, den VSWn und des Secumedia-Fachverlages vorgestellt und allen Interessierten zur Verfügung gestellt werden.

Gegenüber info Sicherheit trat Rolf-Wilhelm Dau hinsichtlich der internen Ermittlungsmöglichkeiten in Unternehmen für rechtlich absolut saubere Lösungen ein. Dies dürfe aber nicht mit einem pauschalisierenden Verbot von Ermittlungsansätzen wie der verdeckten Videoüberwachung bei hinreichendem Verdacht auf besonders schwere Straftaten zum Nachteil des Unternehmens gleichkommen.

Ein solches Verbot war nach Information von info Sicherheit weder inhaltlicher Bestandteil des 2009 vom damaligen Bundesarbeitsminister Olaf Scholz (SPD) vorgelegten Gesetzentwurf noch der ursprünglichen Fassung aus dem Hause Thomas de Maizière (CDU) gewesen. Erst in der Abstimmung zwischen den einzelnen Ressorts hatte sich Bundesjustizministerin Sabine Leutheusser-Schnarrenberger (FDP) mit ihrem Votum für ein Totalverbot durchgesetzt. Die sich als „Anwältin der Bürgerrechte“ positionierende Linksliberale ist für ihre konsequente Haltung bekannt. Am 17. Januar 1996 trat sie wegen des FDP-Mitgliederentscheids zum „Großen Lauschangriff“ unter Tränen von ihrem schon damals ausgeübten Amt als Bundesjustizministerin zurück. SPIEGEL-online portaitierte die Politikerin als „Bundesbedenkenträgerin“, die sich „auch heute (...) der Rückendeckung durch die eigene Partei nie ganz sicher sein“ könne.

Kritik an dem Gesetzentwurf übte auch Reinhard Göhner, Hauptgeschäftsführer des Bundesverbands der Arbeitgeber. Die Überwachung von Lagerräumen ohne Wissen der Arbeitnehmer müsse auch künftig bei Verdacht auf Straftaten möglich sein, sagte er. In solchen Fällen müssten die betroffenen Unternehmen in der Lage sein, den Fall selbst aufzuklären, ohne sofort die Polizei einzuschalten.

Ähnlich argumentiere Thomas Bade, Arbeitsrechtsexperte des Hauptverbands des Deutschen Einzelhandels. Die verdeckte Videoüberwachung bezeichnete er als oft letzten Weg, um einen Straftäter im Unternehmen zu ermitteln. Umkleiden und Sanitäreinrichtungen seien davon selbstredend ausgenommen. ■ -khg

SICHERHEIT RUND UM DIE UHR



SICHERHEITS- UND WACHDIENST GMBH



Werk- und Objektschutz



Revierdienst, Kontrolldienst



Alarmverfolgung, Intervention



Messe- und Veranstaltungsschutz



Personenschutz, Detektei



Videoüberwachung



Hausnotruf, Alarmzentrale



Geldtransport, Kurierdienste



Reinigungs- und Hausmeisterdienst

Borsigstrasse 10, 49661 Cloppenburg

Tel 0 44 71 - 93 09 15, info@siwa-sicherheit.de

www.siwa-sicherheit.de

J. Pawlack: „Vorlage ohne vernünftige Einbindung der Arbeitgeberorganisationen“



2. Vorsitzender des Verbandes für Sicherheit in der Wirtschaft Norddeutschland e.V.: Jochen Pawlack. Foto: P.

Fragen an den 2. Vorsitzenden des Verbandes für Sicherheit in der Wirtschaft Norddeutschland e.V. (VSWN) und Vorstandsmitglied der ASW, Jochen Pawlack

Info Sicherheit: Können Sie als Vertreter des VSWN die Proteste auf Arbeitgeberseite nachvollziehen?

Jochen Pawlack: Generell begrüße ich jede neue gesetzliche Regelung und die Novellierung bestehender Rechtsnormen, die geeignet sind zum einen den gesellschaftlichen Interessen gerecht zu werden und zum anderen einen konkreten Handlungsrahmen „abzustecken“.

Als im Jahr 2009, infolge der öffentlichen Reaktionen auf die „Datenschutzskandale“ bei Lidl, der Bahn und Telekom, eine neue Regelung für den Beschäftigtendatenschutz angekündigt wurde, habe ich damit gerechnet, dass Lücken bei den bestehenden Regelungen geschlossen werden und ausgewählte „Regelungsbereiche“ zusätzlich eine Verschärfung erfahren.

Die Novellierung des BDSG mit konkreten Pflichten für die Unternehmen war ein erster Schritt, der auf allgemeine Akzeptanz gestoßen ist. Als 2009 ein erster Arbeitsentwurf für ein Beschäftigtendatenschutzgesetz im Arbeitsministerium erarbeitet wurde, konnten die dort aufgeführten Änderungen in den Unternehmen als praxistauglich bewertet werden. Das öffentliche Interesse an der weiteren Ausgestaltung des Schutzes der Privatsphäre und des Datenschutzes wurde, ebenso wie das Interesse der Unternehmen an Handlungsoptionen, für die Aufklärung von Wirtschaftskriminalität und Straftaten gegen Unternehmen in wesentlichen Teilen berücksichtigt.

Überraschend ist nun, dass die Beschlussvorlage des BMI ohne eine vernünftige Einbindung der Arbeitgeberorganisationen, Spitzen- und Interessenverbände erfolgt ist. Die aktuell vorliegende Fassung des Entwurfes enthält leider einige Regelungen, die eine wirkungsvolle und angemessene Aufklärung von Kriminalität innerhalb eines Unternehmens erschweren, zumal eine klare Deutung „was ist unter welchen Bedingungen (noch) erlaubt“ schwer fällt.

Durch eine Einbindung der signifikanten Arbeitgeberorganisationen und anderen Fachverbänden, hätte man die unternehmensbezogenen Interessen bei der Bekämpfung der Wirtschaftskriminalität besser berücksichtigen können. Dabei ist zu berücksichtigen, dass vom BMI, dem BKA und den LKA's immer wieder gefordert wird, dass die Unternehmen aktiv zur Aufhellung des Grau- und Dunkelfeldes bei den Straftaten innerhalb der Unternehmen beitragen, um den Ermittlungsbehörden ein reales Lagebild zu vermitteln.

Betrachtet man heute die öffentliche Diskussion und die Kommentierungen zum Gesetzentwurf, so entsteht ein subjektives Bild, dass lediglich Korruption und Ladendiebstahl die gravierenden Probleme in den Unternehmen darstellen.

Info Sicherheit: Existieren aus Ihrer Sicht im Entwurf Regelungsbereiche die „nachjustiert“ werden sollten, um auch den kritischen Stimmen aus den Unternehmen gerecht zu werden?

Aus praktischen Erwägungen und hier muss angemerkt werden, dass die, die im Unternehmen mitverantwortlich sind für die Aufklärung und Prävention von Wirtschaftskriminalität und gegen das Unternehmen gerichtete kriminelle Delikte, insbesondere im Verbot des Einsatzes von verdeckter Videotechnik eine restriktive Vorschrift im Gesetzentwurf sehen.

Bei konsequenter Beachtung und Anwendung aller bisher geltenden Rechtsvorschriften für die Maßnahme „verdeckte Videotechnik“ war nach meiner Auffassung ein Missbrauch ausgeschlossen. Mir sind nur Maßnahmen bekannt, mit denen auf Einzelfälle nach Voruntersuchungen und entsprechendem Verdacht reagiert wurde.

In Unternehmen aller Branchen sind Eigentumsdelikte hinsichtlich der Häufigkeit und der Schadensbilanz ein relevantes und kritisches Phänomen. Die Abwehr der Schäden und die Entwicklung einer effizienten Risk Management-Organisation liegt nicht nur im Interesse des Unternehmens sondern wird vom Gesetzgeber gefordert.

Praktisch bedeutet das Verbot des generellen Einsatzes von „verdeckter Videotechnik“, dass dieses bisher in den meisten Unternehmen zweckgebundene rechtlich konform eingesetzte Arbeitsmittel, nicht mehr zur Anwendung kommen kann.

In der Praxis können nun Unternehmen bei Straftaten wie Diebstahl, Produktsabotage, Datenausspähung Datenmissbrauch oder Computermanipulation keine Vorermittlungen im Vorfeld der strafrechtlichen Ermittlungen realisieren.

Die Komplexität der Unternehmensprozesse hat in der Praxis dazu geführt, dass bei signifikantem Tatverdacht unternehmensintern, in Abstimmung mit anderen Fachbereichen und dem Betriebsrat ausgewählte Ermittlungen zielführend umgesetzt wurden. Im weiteren Verlauf wurde durch die Bereitstellung von Beweismitteln und fundierten Informationen die nachfolgende Ermittlungsarbeit der Strafverfolgungsbehörden unterstützt. Videodokumentationen zu strafbaren Handlungen waren in der Vergangenheit bei den Ermittlungsbehörden ein wichtiges Instrument um das Ermittlungsverfahren erfolgreich abzuschließen und gegebenenfalls Anklage zu erheben.



Wie steht es mit dieser Art von Beweissicherung in einer Echtlage? Müssen etwa auf der Straße Hinweisschilder "Vorsicht Video" aufgestellt werden? Foto: Agentur Klarpunkt

Praktisch bedeutet es, dass der Einsatz von verdeckter Videotechnik in den Unternehmensbereichen den Strafverfolgungsbehörden vorbehalten bleibt. Angesichts fehlender Kapazitäten in den Ermittlungsbehörden und einer weiteren Zunahme der Kriminalität würden kriminelle Handlungen in den Unternehmen zukünftig seltener aufgeklärt. Das hat wiederum zur Folge, dass der Regelkreislauf zwischen Prävention und Repression nicht bedient wird. Das heißt auch, dass durch die Unternehmen in den Fällen, wo Strafverfolgungsbehörden kapazitätsbedingt nicht unterstützen können, weiterer entstehender Schaden hingenommen und getragen werden müsste.

Das geringe Entdeckungsrisiko für tatmotivierte Personen und die ausbleibenden öffentlichkeitswirksamen Sanktionen durch die zukünftig eingeschränkte Aufklärung von Straftaten führt wiederum zu einer Zunahme der Belastung durch Kriminalität.

Vorsorglich möchte ich nochmals anführen, dass bei den mir bekannten Unternehmen der Einsatz verdeckter Videotechnik eines der letzten Mittel nach Ausschöpfen anderer Ermittlungsansätze war. Ich möchte nochmals betonen, dass die konsequente Anwendung der bisherigen Rechtsvorschriften, das beinhaltete u. a. auch die Mitbestimmung durch den Betriebsrat, einen Missbrauch der Maßnahme „verdeckte Videotechnik“ ausgeschlossen hatte.

Info Sicherheit: Warum wurde möglicherweise bei einigen Passagen der Handlungsbedarf der Unternehmen bei realen kriminellen Bedrohungen nicht berücksichtigt.



Auch GPS Tracking steht auf der Verbotsliste des Beschäftigtendatenschutzes. Selbst bei konkreten Verdachtslagen soll dieser Ermittlungsansatz künftig nicht mehr anwendbar sein. Foto: Agentur Klarpunkt

Jochen Pawlack: Wie schon anfangs angemerkt, hätte eine Einbindung der Arbeitgeberverbände, der ASW und anderer Fachgremien bei der Erarbeitung des Gesetzentwurfes zum Beschäftigtendatenschutz dazu geführt, dass man die Positionen und den Handlungsbedarf in der Wirtschaft kritisch, aber auch konstruktiv betrachtet hätte. Hier stellt sich die Frage, sind bei der Erarbeitung des Entwurfes tatsächlich die Bedrohungslage und die realen Szenarien in den Unternehmen berücksichtigt worden? Hat man mit aller Konsequenz auch die Folgen für ausgewählte restriktive Vorschriften, wie das Verbot der verdeckten Videoüberwachung und anderer technischer Systeme betrachtet?

Unbestritten wird ein Arbeitnehmerdatenschutzgesetz gefordert, allerdings gewinnt man den Eindruck, dass die bisherige rechtlich konforme Untersuchungstätigkeit in den Unternehmen hinsichtlich realer Kriminalitätsbekämpfung und den Erfordernissen kaum im notwendigen Umfang betrachtet wurde.

Kritisch angemerkt werden muss, dass die bisherige passive Kommunikation zur Entwicklung von Straftaten innerhalb der Unternehmen eine neue Qualität annehmen muss. Die Existenz eines Grau- und Dunkelfeldes führt mit Sicherheit zu einer nicht angemessenen Beurteilung der realen Bedrohungsszenarien. Die Unternehmen sind deshalb zunehmend gefordert mit den verantwortlichen Ministerien über ihre Fachgremien aktiv zusammenzuarbeiten.

Die Bereitstellung von Informationen zur Kriminalitätsentwicklung in der Wirtschaft hätte zur Folge, dass eine angemessene Lagebeurteilung vonseiten der Behörden erfolgt und Rückschlüsse auf notwendige Maßnahmen der Kriminalitätsbekämpfung gezogen werden können.

Info Sicherheit: Welche Konsequenz hätte die Verabschiedung des Gesetzes Ihrer Meinung nach für die betroffenen Verantwortungsbereiche?

Jochen Pawlack: Sollte es zu einer Verabschiedung des Gesetzes in der vorliegenden Fassung kommen, hat das wohl nur geringfügige Auswirkungen, da eine offene, mitbestimmte und beschilderte Videoüberwachung auch im Sinne der Prävention die geeignetere Maßnahme darstellt.

Zu einem Kernbereich gehört die Ausgestaltung von Präventionsmaßnahmen, die mittel- und langfristig die Sicherung der Unternehmensziele unterstützt. Die Repression von Straftaten ist letztendlich Teil der Präventionsstrategie.

Durch die enge Zusammenarbeit der Bereiche Corporate Security, Compliance, Rechtsabteilung, Personal etc. sowie die Einbindung des Betriebsrates in die Maßnahmen der Kriminalitätsbekämpfung wurden strenge Maßstäbe in der praktischen Umsetzung von betrieblichen Ermittlungen im Vorfeld oder parallel zur Tätigkeit der Strafverfolgungsbehörden verwirklicht.

Nach Compliance-Vorgaben werden alle Maßnahmen der privatrechtlichen Untersuchungen im Unternehmen mit der notwendigen Transparenz geplant und ausgeführt. Alle Phasen der Realisierung werden hinreichend dokumentiert, um rechtssicher den geforderten gesetzlichen Ansprüchen und den unternehmensinternen Festlegungen gerecht zu werden.

Bei Verdachtsfällen wurde die konkrete Verdachtslage dokumentiert, unkritische Prüfungshandlungen vorgenommen und nach einer Interessenabwägung geeignete, erforderliche und verhältnismäßig geeignete kriminalistische Einzelmaßnahmen auf der Grundlage geltender Gesetze und Unternehmensvorschriften umgesetzt.

Beim Kernthema „verdeckte Videoüberwachung“ war bisher eine konkrete Straftat oder eine schwere Verfehlung eines Arbeitnehmers bzw. ein eng eingegrenzter lokaler Bereich ein Kriterium für den Einsatz dieser kriminalistischen Sondertechnik. Vorher sollten bereits alle zur Verfügung stehenden Mittel ausgeschöpft sein.

Mir sind keine Fälle bekannt, bei denen ein sorgfältig begründeter Vorschlag zum Einsatz von verdeckter Videotechnik durch Betriebsräte abgelehnt wurde.

Darüber hinaus ist der Einsatz der „verdeckten Videotechnik“ in jenen Einzelfällen darauf ausgerichtet, die angestrebten Beweismittel für eine Nutzung im späteren Strafverfahren zu verwenden. Im Unternehmen hat es sich bewährt, eine enge Zusammenarbeit mit den Strafverfolgungsbehörden zu leben.

Nach Verabschiedung des Gesetzes in der heutigen Fassung wäre der Einsatz der verdeckten Videotechnik ausgeschlossen und alternative rechtskonforme Arbeitsmittel müssten zum Einsatz kommen. Ohne Frage wird die Bedeutung der klassischen Observation, unter Beachtung der neuen Regelungen, wieder zunehmen. Sicherlich muss man dabei unterstellen, dass die wesentlich höheren Kosten für eine solche Maßnahme zusätzlich ein effizientes Vorgehen erschweren.

14 Tage Videoobservation sind mit einem Kostenbudget verbunden, bei dem ich vergleichsweise eine fachlich fundierte Observation für einen bis maximal drei Tage finanzieren könnte.

Neben dem Thema „Video“ werden weitere Vorgaben für die Dokumentationspflichten in den Arbeitsbereich hineinwirken. Prüfungssicher müssen alle mit der Datenerhebung zu Beschäftigten bezogenen Prozesse und Maßnahmen umfassend dokumentiert werden.

Die Löschung von erhobenen Daten wird unmittelbar nach Erreichen des Zwecks der Ermittlungen erfolgen müssen. Das bedeutet nach meiner Lesart nicht, dass ein Ermittlungsvorgang mit allen Dokumenten vollumfänglich vernichtet werden muss. Hier würde eine „allgemeine Aktenvernichtung“ mit Compliance-Prinzipien und den gesetzlichen Vorschriften für die Aufbewahrung und Dokumentationspflichten kollidieren.

Im Umkehrschluss bedeutet die Forderung nach einer Löschung, dass geeignete Maßnahmen notwendig sind, die zum einen die geforderte Löschung der erhobenen Daten und zum anderen die Dokumentation des Geschäftsvorfalles sichert.

Eine weitere Konsequenz ist die verstärkte Inanspruchnahme der Ermittlungsbehörden bei Eigentumsdelikten, um bei registrierten Schadenfällen und Verlusten eine konsequente Reaktion auf die kriminellen Angriffe zu sichern. Inwieweit die verantwortlichen Stellen in der Lage sind mit ihren Ressourcen die Situation innerhalb der Unternehmen zu bewältigen, bleibt abzuwarten.

In der Vergangenheit wurde praktisch sichtbar, dass die schon seit Jahren vom BMI bei den Unternehmen einge-

forderte Mitverantwortung bei der Kriminalitätsbekämpfung und durch zahlreiche Unternehmen gelebte Sicherheitspolitik von den zuständigen Ermittlungsbehörden in der Praxis dankend angenommen wurde.

Info Sicherheit: Sehen Sie mit der Regelung einen Anstieg der kriminellen Bedrohung und eine Zunahme der Risiken für die Unternehmen?

Jochen Pawlack: Die Globalisierung, die Komplexität der Wertschöpfungsketten, das Wirken sozialökonomischer Faktoren und die Pluralisierung des Wertesystems, hatten in den letzten Jahren kontinuierlich zu einem Anstieg der Kriminalität gegen Unternehmen geführt. Diese Tendenz ist auch für die nächsten Jahre zu prognostizieren.

Im nationalen Bereich wirken sich Einschränkungen für die unternehmensinterne Kriminalitätsbekämpfung natürlich auf die Lage in den Unternehmen aus.

Die betrieblichen Schutzorganisationen würden beim Einsatz einiger Arbeitsmittel eingeschränkt und könnten Maßnahmen der Informationserarbeitung zu den Verdachtsmomenten und die Beweismittelsicherung nur bedingt eigenständig wahrnehmen. Ein umfassender effizienter Ausgleich durch den Einsatz der Strafverfolgungsbehörden wird durch knappe Ressourcen und fehlende Handlungs- und Ermittlungsoptionen der Ermittlungsoptionen bei bestimmten Indizienlagen eher nicht stattfinden.

Ein Beispiel aus der Praxis: Konnte noch einem Hinweisgeber auf innerbetriebliche Straftaten durch die Fachabteilungen Vertraulichkeit und Anonymität zugesichert werden, so kann eine Strafverfolgungsbehörde in der Regel diesen Schutz nicht gewähren. Damit steht kein Hinweisgeber und darauf aufbauend kein begründeter Verdacht für die Einleitung eines Ermittlungsverfahrens zur Verfügung. Unternehmensintern wäre man in der Vergangenheit diesem Hinweis durch abgestufte Prüfungshandlungen nachgegangen. Zukünftig würden aber die Möglichkeiten für operative Maßnahmen eingeschränkt und Straftaten blieben zunehmend unerkannt oder würden erst nach Eintritt eines erheblichen Schadens identifiziert werden können.

Ich gehe aber davon aus, dass infolge der aktuellen Diskussion im aktuellen Entwurf des Beschäftigtendatenschutzgesetzes einige Korrekturen vorgenommen werden.

Info Sicherheit: Herr Pawlack, vielen Dank für das Gespräch. ■

Fachanwalt Nau: „Die kritischen Stimmen auf Arbeitgeberseite kann ich gut nachvollziehen“



Rechtsanwalt Stefan Nau (Berlin). Foto: pr.

Zum Entwurf des Gesetzes zum Arbeitnehmerdatenschutz (Beschluss des Bundeskabinetts) führte info Sicherheit mit dem Wirtschaftsanwalt und Fachanwalt für Arbeitsrecht Stefan Nau (Berlin) ein ausführliches Interview.

Info Sicherheit: Der Entwurf des Arbeitnehmerdatenschutzgesetzes wird aktuell diskutiert – können Sie als Wirtschaftsanwalt die Diskussion auf Arbeitnehmerseite und die Proteste auf Arbeitgeberseite nachvollziehen?

RA Stefan Nau: Grundsätzlich erachte ich es für sehr positiv, dass Gesetzgebungsverfahren in der breiten Öffentlichkeit diskutiert werden. Gesetze sollen ja gerade die Praxis und nicht die Theorie regeln, so dass die Meinungen und Anregungen der von der gesetzlichen Regelung Betroffenen von großer Bedeutung sind. Es bleibt nur zu hoffen, dass die dabei auftretende Meinungspluralität bei der abschließenden Gesetzesvorlage dann auch wirklich Berücksichtigung findet. Diese Diskussion vermittelt jedoch den Eindruck, als ob die Daten der Beschäftigten bis dato ungeschützt waren. Damit wird jedoch die Tätigkeit der Gerichte verkannt, die diesen Schutz bislang und in guter Weise gewährleistet haben. Die kritischen Stimmen auf Arbeitgeberseite kann ich insofern gut nachvollziehen, als der Gesetzesentwurf wohl als Nachwirkung zu dem Fall „Emily“ hauptsächlich auf Ladendiebstahl etc. abstellt und deren Aufklärung auch noch erschwert, aber

Wirtschaftsstrafataten von größerem Ausmaß nicht im Fokus zu stehen scheinen.

Info Sicherheit: Zahlreiche gesetzliche Vorschriften, wie das novellierte BDSG oder auch das Betriebsverfassungsgesetz haben neben den allgemeinen Strafrechtsnormen das Thema bisher reguliert – sind solche restriktiven Einschränkungen, wie das Verbot der verdeckten Videoüberwachung, tatsächlich geeignet, alle Interessen zu berücksichtigen?

RA Stefan Nau: Das generelle Verbot mag die Interessen der Straftäter decken, aber nicht die der betroffenen Arbeitgeber. Ein Schutz der Persönlichkeitsrechte und der Arbeitgeberinteressen wird nur durch eine differenzierte Betrachtung erreicht. Ein absoluter Schutz der Intimsphäre muss ohne weitere Diskussion natürlich gewährleistet sein, wie auch ein relativer Schutz der Privatsphäre, wohingegen eine Überwachung des sog. Sozialbereiches bei begründetem Verdacht zulässig sein sollte.

Info Sicherheit: Die praktische Interpretation des Entwurfes wird recht unterschiedlich wahrgenommen – welche signifikanten Änderungen sind für die Aufklärung von Wirtschaftsstrafataten und Betriebskriminalität für die Unternehmen zu beachten?

RA Stefan Nau: Es erfolgt eine eindeutige Verlagerung der Aufklärungsarbeit auf die Strafverfolgungsbehörden. Soweit man den dortigen „Bearbeitungsstau“ und die technische Ausstattung betrachtet, bleibt dann nur zu hoffen, dass dem durch erhöhte Budgetzuweisung Rechnung getragen wird. Andernfalls bleiben die Unternehmensinteressen auf der Strecke.

Info Sicherheit: § 32 d, Absatz 3 des Entwurfes lässt bei schwerwiegenden Pflichtverletzungen oder zur Aufdeckung von Straftaten eine Datenerhebung und Nutzung der Daten zu. Ist aber die ausdrückliche Nennung der Tatbestände „Untreue, Bestechlichkeit, Bestechung, Vorteilsnahme“ nicht eine einseitige Ausrichtung auf die Aufklärung von Korruption?

RA Stefan Nau: Auf andere Weise lässt sich der Gesetzestext leider nicht interpretieren. Zumal auch die Begründung des Gesetzesentwurfes keine Erklärung enthält, warum gerade diese Straftatbestände besonders hervorgehoben worden sind. Man darf gespannt sein, wie die Gerichte die Konkurrenz in

§ 32d Absatz 3 des Gesetzentwurfes zwischen einerseits dem allgemeinen Verweis auf „Aufdeckung von Straftaten“ am Anfang des Absatzes und der nachfolgenden Konkretisierung auf die „Korruptionstatbestände“ bewerten werden; möglicherweise liegt aber auch lediglich ein redaktioneller Fehler vor.

Info Sicherheit: Sehen Sie Defizite in der fehlenden Integration von weiteren Straftatbeständen, die signifikant für die Unternehmen Bedeutung haben? Insbesondere die Bedrohung durch Datenausspähung, Datenmanipulation, Datenmissbrauch, Produktsabotage und Industriespionage?

RA Stefan Nau: Wenn und soweit die Hervorhebung der „Korruptionstatbestände“ einen besonderen Zweck erfüllen sollte, dann wird dadurch der Schutz vor den Wirtschaftsstraftaten, die auf das Know-how und den Betrieb des Unternehmens abstellen, deutlich erschwert. Der Gesetzgeber muss meiner Meinung nach die Hervorhebung streichen und damit unterstreichen, dass das Unternehmen sich mit den zulässigen Mitteln der Aufdeckung jeglicher Straftat zuwenden kann.

Info Sicherheit: Im § 32 e des Entwurfes (Datenerhebung ohne Kenntnis des Beschäftigten) sind einige Optionen und Einschränkungen aufgeführt. Welche praktischen Auswirkungen hat dieser Paragraph für die betriebliche Ermittlungspraxis?

RA Stefan Nau: Die Voraussetzungen zur Datenerhebung ohne Kenntnis des Beschäftigten, so nämlich ein begründeter Verdacht und auch die Erforderlichkeit der Datenerhebung zur Aufdeckung bzw. Verhinderung von Straftaten, sind auch bisher und sollen nach meiner Ansicht weiterhin zwingend sein. Der hierzu in Absatz 3 festgehaltene Grundsatz der Verhältnismäßigkeit der Mittel ist so verständlich und richtig, wie aber auch so undefiniert. Die Versuche der Bundesregierung, die Auslegung dieses Grundsatzes zu vereinfachen, stellen aber die Ermittlungspraxis vor nahezu unlösbare Fragen, so zum Beispiel die Frage, wie lang die Dauer der Maßnahme sein kann, bis sie das Maß des Unerlässlichen übersteigt.

Info Sicherheit: Wie kann man die vom Gesetzgeber genutzte Formulierung „schwerwiegende Pflichtverletzung“ als ein Grund für eine Datenerhebung ohne Kenntnis des Betroffenen interpretieren?

RA Stefan Nau: Es handelt sich um einen sog. „unbestimmten Rechtsbegriff“, der der Auslegung bedarf. Mangels anderweitiger Anhaltspunkte darf man sich wohl bezüglich seiner Interpretation an der Auslegung zu § 626 BGB (fristlose Kündigung aus wichtigem Grund) ausrichten. Die im Raum stehende und die Datenerhebung veranlassende schwerwiegende Pflichtverletzung muss also dazu führen, dass eine Fortsetzung des Arbeitsverhältnisses im Bestätigungsfalle unzumutbar sein muss.

Im Absatz 5 des gleichen Paragraphen wird die Information des Betroffenen geregelt.

Info Sicherheit: Ist das praktisch ohne Störung des Betriebsfriedens möglich? Welche Handlungsorientierung sehen Sie für die verantwortlichen Bereiche (z.B. Compliance, Revision, Sicherheitsabteilung, Rechtsabteilung)?

RA Stefan Nau: Wenn sich ein Verdacht nicht bestätigt hat, wird aller Erwartung nach natürlich die nachfolgende Information des Betroffenen zu erheblichen Störungen in der Zusammenarbeit führen. Um so wichtiger ist es, auch die, sich aus dem gleichen Absatz ergebenden, Dokumentationspflichten genauestens einzuhalten, um dem Betroffenen einen, den Verdacht begründenden, Sachverhalt en detail vor Augen führen zu können. Nur damit kann Verständnis auf Seiten des Betroffenen erzielt werden, wie auch eventuellen Beschwerden begegnet werden kann.

Info Sicherheit: In § 32 der Regelung zur Datenerhebung vor Begründung eines Beschäftigungsverhältnisses wird im Absatz 6 u. a. geregelt, dass eine Erhebung von Daten nur über den Jobbewerber erfolgen kann oder der Bewerber über eine Erhebung von Daten informiert wird. Welche Konsequenzen hat das in der Praxis für die Überprüfung der Bewerber in sensiblen Bereichen?

RA Stefan Nau: Unverständlich ist für mich der Ausschluss der Erhebung von allgemein zugänglichen Daten über den Bewerber; zumindest dies müsste als zulässig eingestuft werden. Soweit die Erhebung weiterer Daten von der Zustimmung des Betroffenen abhängig gemacht wird, so muss dann darauf geachtet werden, dass nicht nur partiell eine Zustimmung erteilt wird, sondern eine generelle Zustimmung erfolgt.

Info Sicherheit: Es ist doch unumstritten, dass dienstlich genutzte PC-Systeme und Speichermedien der Arbeitnehmer im Rahmen einer Sonderfallüberprüfung „Korruptionsverdacht“ durch die jeweiligen zuständigen Fachabteilungen zur Beweismittelsicherung beschlagnahmt werden. Da private Daten unabdinglich auf den Speichermedien enthalten sind, dürfte doch auch hier Handlungsbedarf vorliegen. Welche Lösungsansätze sehen Sie?

RA Stefan Nau: Es wäre wünschenswert, wenn der Gesetzgeber sich auch mit dieser Thematik näher beschäftigt hätte. So verbleibt die Regelung des Zugriffs auf private Daten, so deren Speicherung auf dienstlich genutzten PC-Systemen überhaupt gestattet werden sollte, bei dem Arbeitgeber bzw. einer Regelung im Arbeitsvertrag.

Info Sicherheit: Herr Nau, wir bedanken uns für das Gespräch. ■

„Gegenwärtiger Entwurf an einigen Stellen wenig praxistauglich und rechtsklar“



Sicherheitsberater und Geschäftsführer: Klaus-Dieter Baier. Foto: P.

Fragen an Klaus-Dieter Baier, Sicherheitsberater und GF der „DESA Investigation and Risk Protection“, einer auf Prävention und Schadenaufklärung spezialisierten Unternehmensberatung.

Info Sicherheit: Der Entwurf des Arbeitnehmerdatenschutzgesetzes liegt vor. Wie lautet Ihre Bewertung?

Klaus-Dieter Baier: Es liegt mir fern, den legislativen Prozess zu kritisieren, dennoch sehe ich Defizite in der fehlenden Beteiligung der Arbeitgeberverbände oder anderer spezialisierter Stellen. Insbesondere die mit hoher Akzeptanz bei den Einrichtungen des Bundes und der Länder bekannte ASW ist ein geeigneter Ansprechpartner im Rahmen eines Gesetzgebungsverfahrens.

Meine Kritik richtet sich gegen inhaltliche Ausführungen, da der gegenwärtige Entwurf an einigen Stellen wenig praxistauglich und rechtsklar ist.

Info Sicherheit: Können Sie das erläutern?

Klaus-Dieter Baier: Die vorliegende Fassung des Gesetzentwurfes führt zu einer Behinderung einer durch nationale und internationale Gesetzgebungen geforderten Korruptions- und Kriminalitätsbekämpfung. Durch zahlreiche Regelungen wird die betriebliche Gestaltung des Arbeitnehmerdatenschutzes zwischen Unternehmensführung und Betriebsrat faktisch abgeschafft. Der Handlungsspielraum für ein differenziertes und gebotenes Handeln wird erheblich eingeschränkt.

Im Gesetzentwurf werden Rechtsbegriffe genutzt, die eine weitere Rechtsunsicherheit in der Praxis schaffen.

Info Sicherheit: Privatermittler und andere auf die Aufklärung von Wirtschafts- und Betriebskriminalität spezialisierte Dienstleister gehen in die Kritik und werfen dem BMI eine fehlende Berücksichtigung der Erfordernisse bei der Kriminalitätsbekämpfung vor.

Klaus-Dieter Baier: Ich habe Verständnis für sachlich begründete Kritik an einzelnen Passagen des Gesetzentwurfes. Insbesondere die restriktiven Einschränkungen zum Einsatz der Videoüberwachungstechnik sehe ich als sehr bedenklich an. Das Verbot des Einsatzes von verdeckter Videotechnik ist dabei eine Kernfrage und hat unmittelbare Auswirkung auf die Situation in den Unternehmen. Zum einen wird die Anwendung von verdeckter Videotechnik als Mittel der Beweissicherung für die „zivilen“ Institutionen innerhalb des Unternehmens umfassend ausgeschlossen und zum anderen wird angesichts der komplexen Unternehmensprozesse die zielgerichtete Aufklärung nicht nur erschwert sondern in vielen Fällen unmöglich gemacht.

Damit bedienen wir eine gefährliche Spirale. Ohne die Aufklärung von kriminellen Handlungen und die Sanktionierung über strafrechtliche oder zivilrechtliche Maßnahmen kann eine wirkungsvolle Prävention nicht umgesetzt werden. Wir stehen hier vor den gleichen Problemen wie außerhalb der Unternehmen.

Natürlich fordert der Gesetzentwurf – falls nicht notwendige Korrekturen vorgenommen werden – von den betroffenen Unternehmen, den verantwortlichen Fachbereichen und nicht zuletzt den externen Dienstleistern neue Lösungsansätze und eine alternative rechtskonforme Umsetzung von operativen Ermittlungen im Umfeld der Unternehmen.

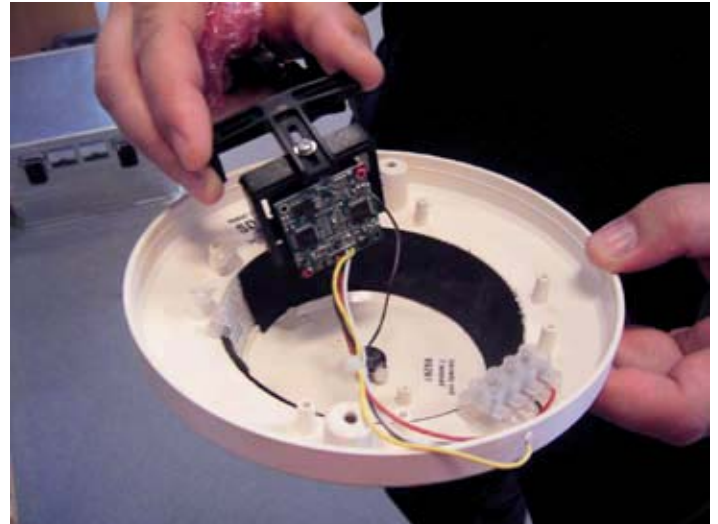
Info Sicherheit: Können Sie Beispiele aufzeigen, wie sich die Änderungen im Beschäftigtendatenschutz auf die Praxis auswirken könnten?

Klaus- Dieter Baier: Thema: „Verdeckte Videoüberwachung“. Natürlich hat uns der wissenschaftliche Fortschritt fast zwanzig Jahre ein geeignetes Arbeitsmittel in die Hand gegeben, mit der man zum Teil kosteneffizient und für die kriminalistische Praxis sehr tauglich Beweismittel erarbeiten konnte.

Hier muss aber klargestellt werden, dass auch vor dem Einsatz der Videotechnik als „Arbeitsmittel“ Eigentumsdelikte und andere unternehmensschädigende Delikte durch private Sicherheitsorganisationen in den Unternehmen aufgeklärt wurden. Zukünftig werden wir uns alternativer rechtskonformer kriminalistischer Methoden besinnen müssen, wenn bei einem dringenden Tatverdacht eine Aufklärung gefordert ist. Neben den technischen Hilfsmitteln aus dem Repertoire der Kriminaltechnik wird zukünftig der personelle Einsatz von Ermittlern im Vordergrund stehen.

Info Sicherheit: Heißt das, die Zeiten „verdeckte Videotechnik“ und „GPS-Ortungssysteme“ sind vorbei und nun muss ausschließlich mit Fernglas und Fotoapparat, wie im Entwurf festgeschrieben, der Täter gefasst werden?

Klaus- Dieter Baier: Eine solche Situationsbeschreibung würde verkennen, dass in zahlreichen Unternehmen schon nahezu eine identische Situation vorgeherrscht hat. Bei einer konsequenten Berücksichtigung der bestehenden Rechtsnormen wie BDSG, Betriebsverfassungsgesetz, StGB und Nebenstrafgesetze, sowie bei Berücksichtigung der aktuellen Rechtsprechung zu den relevanten Aspekten waren schon in der Vergangenheit die Hürden für den Einsatz der genannten Spezialtechnik sehr hoch.



Eine gebräuchliche "Vercontainerung": Videotechnik im Rauchmelder. Künftig nur noch Vergangenheit? Foto: Agentur Klarpunkt

Darüber hinaus wurde in vielen Fällen der Einsatz von verdeckter Videotechnik oder GPS-Ortungstechnik nicht in Erwägung gezogen, um die geforderte Mitbestimmungspflicht des Betriebsrates nicht in Anspruch zu nehmen. In solchen Fällen wurden aufwendige Observationsmaßnahmen oder andere meist kostenintensive Alternativen für die Aufklärung des jeweiligen Tatverdachts herangezogen.

Info Sicherheit: Können Sie das noch näher erläutern?

Klaus- Dieter Baier: Insbesondere bei Eigentumsdelikten, wie klassischer Diebstahl innerhalb des Unternehmens, kann man den Schaden häufig zeitnah identifizieren, und die Tat ist den verantwortlichen Stellen im Unternehmen bekannt. In einem solchen Fall werden die vorhandenen internen Möglichkeiten geprüft, um geeignete Informationen zum Tatverdacht zu erarbeiten. Dazu gehört unter anderem die Auswertung von Daten zu bestimmten internen Prozessen und den tatrelevanten Abläufen. Zum Beispiel eine Auswertung der Daten des Zutrittskontrollsystems für den betreffenden Handlungsbereich, dem Tatort. Die klassische Spurensicherung und die Befragung von Zeugen gehört in einem solchen Fall zu den Kernaufgaben, und diese Einzelmaßnahmen wurden in der Praxis mittlerweile sehr gut von den innerbetrieblichen Ermittlungsorganisationen bewältigt.

Erst nach Ausschöpfen aller zur Verfügung stehenden Mittel wurde der Einsatz geeigneter technischer Arbeitsmittel in Erwägung gezogen und geprüft. Mittlerweile gehört es in zahlreichen Unternehmen zur Praxis, dass die Zweckbindung dieser Maßnahmen und die Parameter der Umsetzung umfassend dokumentiert werden. Darüber hinaus wurde der jeweilige Betriebsrat wegen der geforderten Mitbestimmungspflicht beteiligt. Mir sind auch Unternehmen bekannt, bei denen schon in der Phase der Prüfung zum möglichen Einsatz von



Nicht gestellt- Betriebskriminalität live: Bei dem abgebildeten Mann handelt es sich um einen realen Brandstifter, der durch diese Aufnahme überführt werden konnte. Foto: Agentur Klarpunkt

technischen Mitteln zur Tataufklärung eine solche „operative Maßnahme“ von vornherein ausgeschlossen wurde. Gründe waren unter anderem unkommentierte Entscheidungen der Unternehmensführung oder das Abwägen von Risiken für den Betriebsfrieden durch Einschaltung des Betriebsrates und der Kenntnisnahme einer solchen Maßnahme für die Belegschaft.

In einem solchen Fall mussten die externen Dienstleister ein alternatives Vorgehen planen und umsetzen. Die Konsequenz waren meist Maßnahmen mit einem hohen Personalaufwand. Observationen lassen sich letztendlich auch in Unternehmensbereichen nur durch mehrere Mitarbeiter, mit weitaus höheren Kosten als bei einer Videoüberwachung, realisieren.

Zukünftig wird auch, wie vor den neunziger Jahren, die klassische Observation eine zunehmende Bedeutung erlangen.

Info Sicherheit: Können Sie noch etwas detaillierter auf das Thema „GPS-Ortung“ eingehen?

Klaus- Dieter Baier: Im Wesentlichen hat sich das Verbot für den Einsatz von GPS-Ortungstechnik und adäquater Technik schon erübrigt. Bei konsequenter Beachtung der jüngsten Rechtsprechung war der Einsatz von GPS-Technik für Unternehmen in den letzten Jahren schon ein erhebliches Risiko.

Mir persönlich sind in den letzten zwei Jahren bundesweit mindestens acht Fälle bekannt geworden, bei denen der GPS-Einsatz öffentlich bekannt geworden ist. Einige Fälle endeten trotz der augenscheinlich geeigneten Ausgangssituation für den Dienstleister in Strafverfahren. Dabei wurden

datenschutzrechtliche Aspekte und die Verletzung der Privatsphäre in den Fokus der staatsanwaltlichen Ermittlung gerückt.

Zivilrechtliche Forderungen des durch die Maßnahme Geschädigten oder ein Schadenersatz für polizeiliche Maßnahmen waren die Folge für den Privatermittler oder die eingesetzte Detektei.

Wegen der Mitbestimmungspflicht bei in Erwägung gezogenen GPS-Einsätzen wurde in der jüngsten Vergangenheit immer seltener der Einsatz von GPS-Systemen in der Unternehmenspraxis registriert.

Info Sicherheit: Sehen Sie auch Möglichkeiten, die geplanten Bestimmungen bei der Aufklärung von Straftaten gegen Unternehmen rechtskonform zu berücksichtigen und gleichzeitig kritische Prozesse zu bewältigen? Als Beispiel hier das Thema „Hintergrundüberprüfungen“ bei Personaleinstellungen.

Klaus- Dieter Baier: Ich gebe Ihnen Recht, augenscheinlich erweisen sich die geplanten Vorschriften bei der Überprüfung von Bewerberkandidaten als Hemmnis. Generell werden Hintergrundüberprüfungen aber nicht ausgeschlossen. Durch Ergänzung bestimmter organisatorischer Maßnahmen können allerdings notwendige ausgewählte Prüfungshandlungen dennoch absolviert werden. In der Praxis bedeutet es, dass Arbeitsanweisungen und Verfahrensanweisungen existieren müssen, durch die das Procedere der Bewerberauswahl und Bewerberüberprüfung geregelt wird.

Eine Voraussetzung für Hintergrundüberprüfungen ist es dabei, eine schriftliche Zustimmung des Bewerbers einzuholen. Konsequenz ist aber in der Praxis, dass der Bewerber später Recht auf Einsicht in die Unterlagen erhält und so Kenntnis über die Art und Weise der Datenerhebung und deren Inhalt erhält. Hier entstehen neue Spannungsfelder für die Unternehmen.

Info Sicherheit: Haben die gesetzlichen Bestimmungen zur Durchsetzung des Datenschutzes nicht ausgereicht?

Klaus- Dieter Baier: Das lässt sich weder mit einem einfachen „Ja“ noch mit einem einfachen „Nein“ beantworten. Hier muss man differenzieren und die Zielsetzungen der einzelnen Punkte des Entwurfes betrachten.

Nehmen wir den Punkt „verdeckte Videotechnik“. Bei Anwendung aller Rechtsvorschriften wäre ein Missbrauch dieser Maßnahme im Gros der deutschen Unternehmen weitestgehend ausgeschlossen. Insbesondere das Mitbestimmungsrecht nach Betriebsverfassungsgesetz war ein intakter Regulator.

Betrachten wir die „echten Skandalfälle“ - vieles wurde von der Presse ungeprüft herbeigeredet und zum Teil subjektiv interpretiert, haben die bekanntgewordenen Missbrauchsfälle für den Einsatz von verdeckter Videotechnik meist in Unternehmen, die über keinen oder keinen arbeitsfähigen Betriebsrat verfügten, stattgefunden.

Gerade beim geplanten Verbot des Einsatzes von verdeckter Videotechnik durch zivile Institutionen innerhalb der Unternehmen gewinnt man den Eindruck, dass man bei den federführenden Referenten lediglich die öffentliche Meinung, geschaffen und transportiert durch die Medien, als Maßstab herangezogen hat. Hier hat man in Unkenntnis der realen Situation in den Unternehmen ein Datenschutzziel formuliert, welches für die Kriminalitätsbekämpfung und damit für eine gesamtgesellschaftliche Aufgabe ein Hemmnis darstellt. Konsultationen mit den verantwortlichen Spitzenverbänden hätten hier Abhilfe verschafft.

Andere Regelungsbereiche, wie die Einschränkungen bei der Erhebung von Daten im Rahmen der Bewerberverfahren kann ich durchaus aus Sicht der Allgemeinheit nachvollziehen. Hier sehe ich durchaus Ansätze, Regeln für die Datenerhebung bei Einstellungsüberprüfungen zu entwickeln.

Allerdings generiert der Entwurf neue Fragen, die nicht hinreichend beantwortet werden. Weder im Gesetz noch in den kommunizierten Hintergrundinformationen. Widersprüchlich ist zum einen der angestrebte Wunsch eine Datenerhebung in sozialen Netzwerken, die maßgeblich für die Kommunikation sind, zu verbieten und zum anderen Recherchen in anderen sozialen Netzwerken zuzulassen.

Soziale Netzwerke sind alle gerade durch den hohen Grad der Kommunikation gekennzeichnet. Deshalb ist es nicht nachvollziehbar, dass das Netzwerk XING als „Jobbörse“ in einer Hintergrundinformation des BMI als nicht relevant bewertet wird. Andere Netzwerke, wie StudiVZ, Stayfriends und Facebook werden als relevant eingestuft. Hier wird es in der Praxis erhebliche *Verunsicherung* geben.

Info Sicherheit: Nun melden sich einzelne Stimmen und geißeln den Gesetzentwurf als unternehmensfeindlich und ungeeignet um Interessen der Unternehmen zu berücksichtigen.

Klaus- Dieter Baier: In der Tat hat der Entwurf als Ganzes an vielen Stellen aufgezeigt, dass der reale Bedarf der Unternehmen an der Sicherung der Unternehmensprozesse, damit auch im Interesse der Gesellschaft, unbeachtet geblieben ist. Persönlich bin ich für eine klare Regelung bestimmter Eingriffe in die Persönlichkeitsrechte und die Schaffung gesetzlicher Normen, die einen durch die Gesellschaft geforderten Datenschutz verwirklichen.

Unverständnis habe ich allerdings wenn negative Einzelfälle

nicht im Kontext mit der Gesamtsituation bewertet werden und infolge der Fehlbewertung Verbote und Einschränkungen folgen, die mit anderen Zielen unserer Gesellschaft kollidieren.

Info Sicherheit: Wo sehen Sie konkrete Kollisionen bei den Rechtsvorschriften?

Klaus- Dieter Baier: Auf der einen Seite verpflichtet der Gesetzgeber die Unternehmen, wirkungsvolle Risk Management-Systeme zum Schutz der Unternehmen und zur Absicherung der Unternehmensziele zu implementieren und fortzuschreiben. Hier unterstelle ich auch das gesamtgesellschaftliche Interesse an der Sicherung der Wirtschaft und der Abwehr von Gefahren. Zusätzlich wird durch Bundes- und Landesbehörden die Eigenverantwortung und Zusammenarbeit der Wirtschaft bei der Bekämpfung von Unternehmenskriminalität eingefordert.

An der Stelle, wo aber die praktische Realisierung von Risk-Management-Systemen im Raum steht, werden restriktive Vorschriften erlassen, die nicht nur eine Aufklärung krimineller Delikte erschweren, sondern zusätzlich mit anderen Vorschriften möglicherweise kollidieren.

Info Sicherheit: Die Publikumspresse berichtet in einer Überschrift, dass Wanzen nicht mehr erlaubt seien...

Klaus- Dieter Baier: Danke für dieses Beispiel einer unsachlichen Presseberichterstattung. Der Einsatz von Wanzen für Privatpersonen und damit für betriebliche Ermittlungsorganisationen ist schon durch das Strafgesetz seit je her geregelt und verboten. Hier kann man aber erkennen, dass selbst fachlich hoch qualifizierte Journalisten sich mit dem Thema ungenügend auseinandersetzen. Es werden Nachrichten adaptiert, die vermeintlich öffentliche Meinung wird als Gradmesser für eine Beurteilung herangezogen und nachfolgende „abgeurteilt“ oder „fachkompetent“ bewertet. Man konnte in den letzten Tagen bei der öffentlichen Berichterstattung und insbesondere bei der Kommentierung erkennen, dass die Interessenlage der Wirtschaft nur ungenügend berücksichtigt wurde. Gelegentlich hatte man das Gefühl, dass „Schwarz-Weiß-Interpretationen“ oder das „Feindbild Arbeitgeber“ medial bedient wurden.

Wenn im ZDF-Morgenmagazin der Moderator dem Vertreter des Arbeitgeberverbandes auf seine Kritik zu den fehlenden Möglichkeiten der Kriminalitätsbekämpfung entgegnet wird, dass für diese Aufgaben die Polizei zur Verfügung steht, offenbart dieses Interview wie viel Unkenntnis in den Medien vorherrscht und damit ein „falsches Bild“ mit fatalen Folgen an die breite Öffentlichkeit vermittelt wird.

Info Sicherheit: Herr Baier, vielen Dank für das Gespräch. ■