

Vortrag

zum Thema

„Datenschutz in der Privatwirtschaft“

am Dienstag,

dem 31. August 2010

zur Veranstaltung

Zu Gast in der Staatskanzlei:

Datenschutz – Ein verkannter Freund?

Sperrfrist: Redebeginn!

Es gilt das gesprochene Wort!

Meine Damen und Herren,

I. Einleitung

1. Herzlichen Dank, Herr Ministerpräsident, für die freundliche Begrüßung und die Gelegenheit, hier bei Ihnen in der Staatskanzlei über Fragen des Datenschutzes reden und diskutieren zu können. Ich freue mich sehr, dass mit Ihrer Hilfe, Herr Dr. Schwager, und der Unterstützung der ZIRP so viele Gäste für unsere Veranstaltung interessiert werden konnten, vor allem auch aus der rheinland-pfälzischen Wirtschaft. Es zeigt, dass der Datenschutz längst kein Nischenthema mehr ist, sondern breite Kreise der Bevölkerung interessiert, und zwar nicht nur wegen der vielen Skandale, sondern weil die Menschen zu verstehen beginnen, dass beim Datenschutz nicht irgendwelche Daten geschützt werden, sondern sie selbst. Das gilt auch beim Datenschutz in der Privatwirtschaft, unserem heutigen Thema.

2. In der vergangenen Woche, meine Damen und Herren, erhielt ich von einem Mainzer Geschäftsmann die Nachricht, er sei aufgrund einer Sicherheitslücke bei einem E-Mail-Dienstleister in den Besitz des E-Mail-Verteilers und der Kundenliste einer großen deutschen Drogeriekette mit 7 Millionen E-Mail-Adressen und 150 000 Datensätzen mit weiteren Angaben gelangt, die jetzt verschlüsselt auf dem PC seines Mitarbeiters gespeichert seien und dort abgeholt werden könnten. Er ist ein alter Bekannter von uns. Vor einiger Zeit hatte er uns darüber informiert, schon zwei Jahre lang im Besitz von 16 Millionen Kundendaten der T-Mobile GmbH zu sein. Auch diese Daten konnten wir sicherstellen. Manchmal erfahren wir auch von 16jährigen Gymnasiasten, dass sie den Datenspeicher von schülerVZ geplündert hätten, nicht in krimineller Absicht, sondern nur um festzustellen, ob sie oder die Techniker von schülerVZ in Sicherheitsfragen versierter seien.

Das sind keine Einzelfälle, meine Damen und Herren. Sie werfen vielmehr ein Schlaglicht auf unser digitales Zeitalter, in dem nicht nur unvorstellbar große Mengen von Daten gespeichert werden, sondern auch der

Datendiebstahl und der sog. Identitätsdiebstahl an der Tagesordnung sind. Vor allem in den USA, aber auch in der Bundesrepublik Deutschland macht der Datendiebstahl dem Drogenhandel mittlerweile den Rang als lukrativstes Verbrechen streitig, auch deshalb, weil von Teilen der Wirtschaft viel zu wenig in die Sicherheit ihrer Daten investiert wird.

Als 1974, meine Damen und Herren, das rheinland-pfälzische Landesdatenschutzgesetz erlassen wurde und wir, sehr geehrter Herr Prof. Rudolf, im Dezember 1983 die noch druckfrische Entscheidung des Bundesverfassungsgerichts zur Volkszählung in den Händen hielten und darin erstmals von einem Datenschutzgrundrecht lasen, dem informationellen Selbstbestimmungsrecht der Bürgerinnen und Bürger, waren wir von solchen Verhältnissen noch digitale Generationen entfernt, zumal es damals auch gar nicht um Wirtschaftsunternehmen ging, sondern um den Staat und um unsere Sorge, er würde mit Hilfe der elektronischen Datenverarbeitung aus seinen Bürgerinnen und Bürgern gläserne Untertanen machen.

Dass es so nicht gekommen ist, haben wir vor allem dem Bundesverfassungsgericht zu verdanken, das in einer Kette von Entscheidungen immer und immer wieder große Informationsvorhaben des Staates stoppte: Am Anfang war es – wie gesagt – die Volkszählung, zuletzt – Sie wissen es – die Vorratsdatenspeicherung, demnächst – vielleicht – das ELENA-Verfahrensgesetz.

Mittlerweile sind aber andere dabei, die von Georg Orwell eigentlich dem Staat zugedachte Rolle des Big Brother zu übernehmen, vor allem die Internet-Oligarchen unserer Tage, etwa der Vorstandsvorsitzende von Google, Eric Schmidt und sein Kollege von Facebook, Mark Zuckerberg. Auch der frühere Vorstandsvorsitzende der Deutschen Bahn, Hartmut Mehdorn, und einige leitende Mitarbeiter, etwa der Deutschen Telekom, haben sich an dieser Rolle versucht, wie die entsprechenden Daten-skandale der vergangenen Jahre belegen, die im Übrigen auch mit den Namen Lidl, Schlecker und Daimler, aber auch mit Begriffen wie Datenklau, Datenhandel und Callcenter verbunden sind und alle die Privatwirtschaft betroffen haben.

Diese Skandale und Datenpannen haben den früheren Präsidenten des Bundesverfassungsgerichts Hans-Jürgen Papier vor 2 Jahren dazu ver-

anlasst, vor einem drohenden „S u p e r g a u des Datenschutzes“ in der Privatwirtschaft zu warnen und diese Warnung mit der Aufforderung zu verbinden, der S t a a t solle sich endlich schützend vor seine Bürgerinnen und Bürger stellen. Wenn man den im Februar vom Telekom-Vorstand Manfred Balz vorgelegten Untersuchungsbericht über die Bespitzelungsmaßnahmen des Konzerns liest, kann man Prof. Papier nur zustimmen. Denn in diesem Bericht wird frank und frei eine „Unkultur des Misstrauens“ und ein „hysterisches Sicherheitsverständnis“, eingestanden.

Mittlerweile, meine Damen und Herren, wurde das Bundesdatenschutzgesetz an der einen oder anderen S t e l l e novelliert. Aber einen Konsens über den S t e l l e n w e r t des Datenschutzes in Staat und Gesellschaft, in der Wirtschaft und im Privatleben haben wir noch längst nicht erzielt. Mehr denn je pendeln wir zwischen zwei weit auseinander liegenden Positionen. Auf der einen Seite das Bundesverfassungsgericht, das unter Hinweis auf die Menschenwürde in Art. 1 GG Privatsphäre und Datenschutz mit Nachdruck und großer Eindringlichkeit verteidigt. Auf der anderen Seite die Internetapologeten unserer Zeit, welche Privatsphäre und Datenschutz eher als Relikt einer untergegangenen Welt deklarieren, als Versteck für jene, die etwas zu verbergen haben. Wo die Gesellschaft hinsteuern wird, scheint ungewiss. Deshalb bewegen wir uns zurzeit – gerade auch in Datenschutzfragen – auf unsicherem Gelände. Damit meine ich Sie als Vertreter der Wirtschaft, aber auch uns Datenschützer und nicht zuletzt den Staat, der mit demselben Problem zu kämpfen hat, aber stärker als die Wirtschaft durch das Rechtsstaatsprinzip gebunden ist.

Das, meine Damen und Herren, ist der Hintergrund, vor dem ich Ihnen einen kurzen Überblick über die Situation des Datenschutzes in der Privatwirtschaft geben will.

II.

Datenschutz in der Privatwirtschaft

1. Zunächst: Es gibt nicht nur Negatives zu berichten. Denn Teile der Wirtschaft haben natürlich aus den Datenskandalen der vergangenen Jahre Konsequenzen gezogen. Die Telekom hat einen eigenen Vorstand

für Datenschutzfragen installiert, Vodafone mit der früheren Vizepräsidentin des Deutschen Bundestages, Renate Schmidt, eine Ombudsfrau für den Datenschutz bestellt und die Schufa den früheren Vizepräsidenten des Bundesverfassungsgerichts, Prof. Hassemer, als Datenschutzbevollmächtigten eingesetzt. Die Deutsche Bahn hat ihrem betrieblichen Datenschutzbeauftragten mehr Personal zugestanden und Lidl alle Videokameras abgebaut, auch in den Verkaufsräumen ihrer Filialen, was datenschutzrechtlich gar nicht notwendig gewesen wäre. Aber so buchstabiert man eben Vertrauensbildung: einen Schritt mehr zu tun, als man eigentlich tun müsste.

Leider ist diese Haltung nicht überall verbreitet. Viele Unternehmen wollen sich – wenn überhaupt – eher mit einem datenschutzrechtlichen Minimum begnügen, womit die Bürgerinnen und Bürger aber offenbar nicht ganz einverstanden sind. Nach einer Allensbach-Umfrage vom Mai des vergangenen Jahres misstrauen 82 % der Befragten den Unternehmen beim Schutz ihrer Daten. Die Gründe liegen auf der Hand. Um Defizite beim Verbraucherdatenschutz geht es vor allem bei den Internetgroßmächten wie Google, Facebook, Amazon, eBay und ihren kleinen bundesdeutschen Brüdern. Um zuweilen unzureichenden Arbeitnehmerdatenschutz vor allem bei vielen klein- und mittelständischen Betrieben und Handelsketten. Erlauben Sie mir dazu jeweils ein paar Anmerkungen, wobei ich in meinem Vortrag dem Verbraucherdatenschutz etwas mehr Raum widmen möchte, da wir in der anschließenden Podiumsdiskussion sicherlich stärker auf den Beschäftigtendatenschutz zu sprechen kommen werden.

2. Google, Facebook und Co., meine Damen und Herren, sind unsere neuen digitalen Götter oder besser gesagt: die goldenen Kälber unseres digitalen Zeitalters, um die Millionen und Abermillionen von Menschen hier und in aller Welt tanzen, rund um die Uhr, immer länger, immer häufiger, immer ausgelassener. Facebook hat weltweit mittlerweile 500 Millionen Mitglieder, Google 620 Millionen Nutzer pro Tag, die täglich sieben Milliarden Mal alleine die Suchmaschine nutzen. Immer hemmungsloser werden dabei persönliche Daten preisgegeben, zum Teil bewusst, zum Teil unbewusst, zufällig zuweilen, aber in allen Fällen zwangsläufig.

Die Internetdienstleister lassen sich durch die damit verbundenen datenschutzrechtlichen Fragen kaum beeindrucken. Sie betreiben eine aggressive Kommerzialisierung der Privatsphäre. Frank Schirrmacher, der Herausgeber der FAZ, spricht sogar von deren Industrialisierung. Was meint er damit? Er meint den Versuch von Google, Facebook und Co., die Menschen virtuell abzubilden, einen digitalen Klon herzustellen, um diesen wirtschaftlich auszubeuten.

Diese Entwicklung hat viele problematische Seiten. Natürlich betreffen sie in erster Linie die Onliner, also die Nutzer und Verbraucher selbst. Sie betreffen aber auch die Gesellschaft, weil sich die Grenze zwischen Privatsphäre und Öffentlichkeit, zwischen Geheimnis und Offenheit verschiebt, ja aufzulösen beginnt und wir nicht wissen, welche Konsequenzen dies haben wird. Diese Entwicklung geht aber auch an der Wirtschaft nicht spurlos vorbei, und zwar schon deshalb nicht, weil sich viele junge Onliner nicht nur privat sorglos in den Netzwerken bewegen, sondern dies auch tun, wenn sie dieselben Webdienste beruflich in ihrer Firma nutzen.

Mit anderen Worten: Wer seine persönlichen Geheimnisse leichtfertig offenbart, achtet möglicherweise auch nicht allzu sehr auf die Betriebs- und Geschäftsgeheimnisse anderer. Diese Schlussfolgerung legt jedenfalls eine Studie der Beratungsgesellschaft Accenture aus dem vergangenen Jahr nahe, die sich mit den sog. „Millennials“ befasste, also der Internetgeneration der Jahrgänge 1977 bis 1994, die bereits in das Berufsleben eingetreten sind oder es in absehbarer Zeit tun werden.

Die Ergebnisse dieser Studie sollten Sie besorgt machen. Denn diese „Millennials“ schleppen ihre gewohnten Anwendungen und Geräte in die Unternehmen ein und bringen dabei ein eher geringes Sicherheitsbewusstsein mit. Sie nutzen Social Networks, Instant Messaging und Smart Phones. Sie bloggen, twittern und chatten, nicht nur privat, sondern auch im beruflichen Kontext, und hinterlassen auf diese Weise viele Informationen über ihr Unternehmen, dessen Mitarbeiter und Kunden im Netz.

Dies ist für Konkurrenten eine Fundgrube, aber für Kriminelle auch, vor allem wenn sie sich im Wege des social engineering Zugang zu Firmengeheimnissen verschaffen und diese wirtschaftlich verwerten. Eine Bil-

lion Euro Schaden soll der globalen Wirtschaft jedes Jahr durch solche Attacken entstehen.

Umso wichtiger ist es, dass sich die Wirtschaft darauf einrichtet, dass ihre jungen Mitarbeiter eine bestimmte Einstellung zu den sozialen Medien haben und diese Einstellung auch nicht ablegen, wenn sie durch das Werks- oder Firmentor gehen.

Die Frage, wie die Wirtschaft dies tun soll, wird aber überwiegend nicht gestellt und, wenn doch, nicht einheitlich beantwortet. Manche sind der Auffassung, dass eine Art betriebliche Umerziehung in regelmäßigen Schulungen ausreiche. Andere plädieren eher für den Erlass von einschlägigen Richtlinien und Verhaltensregeln, in denen der Einsatz von sozialen Medien zu beruflichen und betrieblichen Zwecken vorgeschrieben werden müsse. In der betrieblichen Praxis findet sich aber offenbar weder das eine noch das andere.

Was die Richtlinien anbelangt, so lässt die Studie von Accenture vermuten, dass weitaus weniger als die Hälfte der Unternehmen über entsprechende Verhaltensregeln verfügt. In einer Untersuchung der Universität Leipzig ist gerade einmal von 19 % der Unternehmen die Rede. Das ist problematisch genug. Es wird aber dadurch noch verschlimmert, dass die vorhandenen Muster-Richtlinien – es gibt sie etwa vom Bundesverband der digitalen Wirtschaft – an der datenschutzrechtlichen Problematik der Angelegenheit völlig vorbeigehen.

Sie sehen also, meine Damen und Herren, es wäre zu kurz gedacht, die Entwicklung auf dem Felde des Internet im Allgemeinen und der sozialen Netzwerke im Besonderen ausschließlich als privates oder gesellschaftliches Problem zu begreifen, mit dem sich die Wirtschaft nicht weiter beschäftigen müsste. Sie steckt selbst mitten im digitalen Prozess.

Ich will es bei diesem Exkurs belassen und zurückkehren zu der Frage, wie Staat, Gesellschaft und vielleicht auch die Wirtschaft mit dem aus Sicht des Verbraucherdatenschutzes so wichtigen Problem der Industrialisierung der Privatsphäre umgehen sollen, ja umgehen müssen.

Natürlich ist der Gesetzgeber gefragt. Die Probleme, die wir zurzeit mit Street View haben, zeigen, dass die aus der Vorinternetzeit

stammenden Bestimmungen des Bundesdatenschutzgesetzes nicht einfach pauschal auf die virtuelle Realität übertragen werden können. Da das Internet eine *e i g e n e* Welt darstellt, brauchen wir für sie auch ein *e i g e n e s* Gesetz, das die Spielregeln enthält, die in dieser Welt beachtet werden müssen, wobei ich natürlich weiß, dass die Regelungsmöglichkeiten nationaler Gesetzgeber im World Wide Web notwendigerweise begrenzt sind. Aber das begründet eine erhöhte Verantwortlichkeit der Wirtschaft, die auch in der Pflicht zur Selbstregulierung zum Ausdruck kommt, welche aber allzu oft nicht wahrgenommen wird.

Regelungen des Gesetzgebers oder Selbstregulierungen durch die Wirtschaft reichen aber nicht aus. Sie müssen durch *t e c h n i s c h e* *M a ß n a h m e n* ergänzt werden. Was der Airbag und die Anschnallgurte im Straßenverkehr sind, müssen im Internet, das ja bekanntlich nichts vergisst, der digitale Radiergummi und das virtuelle Verfallsdatum sein. Beides ist technisch machbar, wie wir gerade von der Universität Saarbrücken erfahren haben, wo ein Verfahren entwickelt wurde, mit dessen Hilfe man Dateien und Bilder mit einem Verfallsdatum versehen kann, bevor man sie ins Internet stellt. Allerdings ist die Umsetzung eines solchen Verfahrens noch lange nicht in Sicht, auch deshalb nicht, weil sich die *W i r t s c h a f t* davon offenbar keinen Gewinn verspricht.

Umso wichtiger ist es, den Datenschutz – der Verkehrserziehung entsprechend – auch als Erziehungsaufgabe zu verstehen, zumal das Datenschutzbewusstsein der Verbraucherinnen und Verbraucher – wie gesagt – nicht besonders widerstandsfähig ist. Die Kommerzialisierung der Privatsphäre durch die Wirtschaft findet deshalb in vielen Verbraucherinnen und Verbraucher bereitwillige Mitspieler.

Wir könnten diese Entwicklung achselzuckend hinnehmen, wenn die Betroffenen immer wüssten, was sie eigentlich tun. Aber das ist nicht der Fall. Dem durchschnittlichen Onliner bleibt immer häufiger verborgen, welche digitalen Aktivitäten welche Datenspuren hinterlassen und wer diese zu Lesen in der Lage ist. Das gilt für Erwachsene, aber erst recht für Jugendliche und ganz sicher für Kinder, die sich ja ebenfalls zu Tausenden im Netz bewegen, auch in den sozialen Netzwerken, ohne dass sie dort ausreichend geschützt wären. Gerade deshalb, meine Damen und Herren, muss der Datenschutz als Bildungs- und Erziehungsaufgabe begriffen werden, und zwar als gesamtgesellschaftliche Bildungsauf-

gabe, die nicht nur den Schulen aufgebürdet werden darf, sondern auch von der Wirtschaft wahrgenommen werden muss, zumal sie die Probleme schafft, mit denen wir uns heute auseinandersetzen müssen. Es geht dabei nicht nur um Schulungen zum betrieblichen Datenschutz, sondern mehr noch darum, den Mitarbeitern Regeln für den verantwortungsvollen Umgang mit den eigenen Daten und den respektvollen Umgang mit den Daten anderer zu vermitteln.

Ich will es bei diesen Anmerkungen zum Verbraucherdatenschutz zunächst einmal belassen und zum nächsten Thema übergehen: dem Arbeitnehmerdatenschutz.

3. Beim Arbeitnehmerdatenschutz stehen ganz andere Fragen im Vordergrund. Hier geht es um den sachgerechten Ausgleich zwischen den Persönlichkeitsrechten der Arbeitnehmer einerseits und den Informationsrechten der Arbeitgeber andererseits, vor allem um die Grenzziehung zwischen berechtigter und unzulässiger Kontrolle der Arbeitnehmer durch die Arbeitgeber.

Diese Grenzziehung, meine Damen und Herren, hat schon immer Schwierigkeiten bereitet und tut es auch heute noch. Dies zeigen die bereits erwähnten Datenskandale. Die Deutsche Bahn hatte zweimal rund 200 000 Mitarbeiter auf Korruptionsvergehen hin überprüft, die Deutsche Telekom u.a. einige Vorständler und Journalisten wegen eines möglichen Verrats von Betriebsgeheimnissen durchleuchtet. Lidl hatte seine Mitarbeiter mit Videokameras überwacht, aber auch Telefongespräche abgehört, EDEKA hatte Detektive eingesetzt.

Dem ersten Schreck nach Bekanntwerden der Skandale folgte meistens der treuherzige Versuch, die Verantwortlichen als Schwarze Schafe und die Vorfälle als Einzelfälle abzutun, die man nicht verallgemeinern dürfe. Das klingt ganz nett, trifft aber nicht zu, wie Sie leicht feststellen können, wenn Sie durch die Fußgängerzonen unserer Innenstädte schlendern und mit etwas Aufmerksamkeit die zahllosen Videokameras entdecken können, die in sehr vielen Geschäftsräumen angebracht sind, in der Regel zur Überwachung von Mitarbeitern, etwa an den Kassen oder in sonstigen Servicebereichen. Die meisten Anlagen verstoßen gegen Datenschutzrecht, weil es keinen Anlass für eine Überwachung gibt, weil sie unverhältnismäßig ist oder weil die Mitarbeiter nicht unterrichtet

wurden. Klar geregelt ist dies aber alles nicht, so dass man entweder Datenschutzvorschriften heranziehen muss, die für andere Sachverhalte gedacht sind, oder nach Entscheidungen der Arbeitsgerichte zu suchen hat, die vielleicht passen könnten.

Das soll – wie Sie sicherlich wissen – künftig anders werden. Aus Sicht des Datenschutzes ist es deshalb außerordentlich zu begrüßen, dass das Bundeskabinett in der vergangenen Woche einen Gesetzentwurf für ein Beschäftigungsdatenschutzgesetz beschlossen und auf den parlamentarischen Weg gebracht hat, auf dem sich seit ein paar Monaten auch schon ein entsprechender Gesetzentwurf der SPD-Bundestagsfraktion befindet.

Auf den Gesetzentwurf der Koalition möchte ich etwas näher eingehen, weil er die Grundlage der kommenden Beratungen des Bundestags sein wird. Er enthält eine Reihe von bemerkenswerten Verboten:

- das Verbot der heimlichen Videoüberwachung,
- das Verbot von heimlichen Abhörmaßnahmen, z. B. von Wanzen,
- das Verbot der heimlichen Mitarbeiterortung durch GPS-Systeme,
- das grundsätzliche Verbot, Daten aus sozialen Netzwerken in Bewerbungsverfahren zu verwenden und
- das Verbot von medizinischen Einstellungsuntersuchungen, es sei denn der künftige Verwendungszweck der Bewerber macht eine solche Untersuchung zwingend erforderlich.

Wo ausnahmsweise heimliche Überwachungsmaßnahmen zugelassen werden, gelten enge Voraussetzungen und die Pflicht, die betroffenen Arbeitnehmer zumindest nachträglich über die heimlichen Kontrollen zu informieren.

Das bedeutet aber nicht, dass der Gesetzentwurf den Arbeitgebern die Kontrolle ihrer Beschäftigten über die Maßen erschweren oder gar unmöglich machen würde. Erlaubt wird z. B. das sog. Mitarbeiterscreening, also der automatische Abgleich von Beschäftigtendaten, dann nämlich, wenn auf diese Weise Straftaten, insbesondere Korruptionsvergehen, aufgeklärt werden sollen.

Manches wird **k o n t r o v e r s** beurteilt, etwa das Verbot, Daten aus sozialen Netzwerken für Bewerbungsverfahren zu verwenden, weil die Einhaltung eines solchen Verbotes nicht kontrolliert werden könne. Das trifft zwar zu, gilt aber auch für manch andere Vorschrift, die bei der Durchführung von Bewerbungsverfahren zu beachten ist, aber nicht beachtet wird. Außerdem trägt ein solches Verbot dazu bei, die längst fälligen Spielregeln für soziale Netzwerke zu etablieren, die man ja immer noch als den „Wilden Westen des 21. Jahrhunderts“ bezeichnet.

Im Übrigen gibt es aus der Sicht des Datenschutzes sicherlich einige Ansatzpunkte für eine Verbesserung des Gesetzentwurfs. Der Entwurf der SPD-Bundestagsfraktion enthält dazu die eine oder andere Anregung. Aber der Datenschutz ist nicht der Nabel der Welt und auch nicht die einzige Grundrechtsposition. Andere Rechte müssen auch zum Zuge kommen. Die gesellschaftliche Akzeptanz des Datenschutzes lebt deshalb vom guten Kompromiss. Sie lebt davon, dass er nicht überzieht. Deshalb muss auch nicht jede denkbare Verbesserung des Gesetzentwurfs der Regierungskoalition zur Machtfrage erhoben werden.

Andererseits, meine Damen und Herren, darf der Datenschutz aber auch nicht unter Wert gehandelt, diskreditiert oder gar diffamiert werden. Das geschieht aber, wenn Arbeitgeberpräsident Dr. Hundt den Gesetzentwurf als eine Art von Täterschutzgesetz bezeichnet, weil ihm die heimlichen Kontrollrechte der Arbeitgeber nicht weit genug gehen. Das ist in jeder Hinsicht unangemessen. Unangemessen ist das Gerede vom „Datenschutz als Täterschutz“, weil es ganz einfach nicht zutrifft und weil es immer noch weit verbreitete Vorbehalte und Vorurteile gegen den Datenschutz schürt. Unangemessen ist aber auch die Forderung nach mehr heimlicher Kontrolle, weil sie das **V e r t r a u e n** aufs Spiel setzt, von dem der Arbeitnehmerdatenschutz lebt.

Denn der Arbeitnehmerdatenschutz liegt letztlich in den Händen der Arbeitgeber. **S i e** haben sicherzustellen, dass auch die Arbeitnehmer zu **i h r e m** Recht kommen. Das ist eine verantwortungsvolle Aufgabe. Sie wird nur gelingen, wenn die Arbeitnehmer darauf **v e r t r a u e n** können, dass ihre Rechte von den Arbeitgebern auch respektiert werden. Das ist ja gerade das Ziel des Gesetzentwurfes, dazu beizutragen, dass ein vertrauensvolles Arbeitsklima zwischen Arbeitgebern und Arbeitnehmern am Arbeitsplatz besteht bzw. entstehen kann.

Ob das gelingt, hängt auch davon ab, wie beide Seiten in dem jetzt anstehenden Gesetzgebungsverfahren miteinander umgehen. Es sollte nicht soweit kommen wie bei der Novellierung der BDSG-Vorschriften zum Adressdatenhandel vor zwei Jahren, als eine intensive Lobbyarbeit am Ende nur noch ein abgenagtes Regelungsgerippe des ursprünglichen Gesetzentwurfs übrig gelassen hat.

Übertreiben wir also nicht den Gruppenegoismus, das Verbandsinteresse und die Lobbyarbeit. Wenn wir das Gemeinwohl etwas mehr bedenken, werden wir feststellen, dass der Gesetzgeber weder ein Täterschutzgesetz geschaffen hat, noch dass das Gesetz ein „miserables Regierungswerk“ ist, wie von Gewerkschaftsseite behauptet wird. Er ist alles in allem ein ausgewogener Kompromiss und deshalb eine gute Grundlage für die anstehende parlamentarische Beratung.

III. Schlussbemerkung

„Datenschutz in der Privatwirtschaft – Ein verkannter Freund?“ so lautet der Titel unserer Veranstaltung. Ich hoffe, dass ich Ihnen verständlich machen konnte, was ich mit diesem Titel zum Ausdruck bringen wollte. Man kann den Datenschutz als Kostenfaktor begreifen, als bürokratische Last oder als Luxusproblem einer überregulierten Gesellschaft. Man kann so tun, als käme Cyber-Kriminalität nur in Science Fiction-Romanen vor und als sei Facebook kein großangelegtes soziales Experiment, sondern nur ein harmloser Weg, den Dialog mit Mitarbeitern und Kunden zu intensivieren. Man kann also den Datenschutz als eine quantité négligeable betrachten oder ihn sogar ignorieren.

Die Folgen lägen auf der Hand. Es würde zu weiteren Datenskandalen kommen und zu noch mehr öffentlichem Druck. Darunter würde das Firmenimage leiden, Kunden würden abwandern. Bußgeldzahlungen wären dann noch das Geringste.

Es gibt eine gute Alternative dazu: einen offensiv betriebenen Datenschutz. Er gibt Ihnen die Möglichkeit, etwas für Ihr Firmenimage zu tun, das Vertrauen zwischen Arbeitnehmern und Arbeitgebern zu stabilisieren

und sich insgesamt besser im digitalen Zeitalter zurechtzufinden. Ich möchte sie deshalb gerne dazu einladen, sich gemeinsam mit Ihrem betrieblichen Datenschutzbeauftragten und meiner Behörde auf einen Datenschutz mit Augenmaß einzulassen.

Herzlichen Dank für Ihre Aufmerksamkeit, meine Damen und Herren.