Privacy at workplace – Kontrolle und Überwachung der Arbeitnehmer

Interview mit Herrn Prof. Dr. Caspar, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit (HmbBfDI)

Das Projekt ist durch das Programm Grundrechte und Unionsbürgerschaft von der Europäischen Union kofinanziert.

A. Über die gesetzlichen Regelungen und die Selbstregulierung

I. Gesetzliche Regelungen

1. Aktuelle Rechtslage

Herr Professor, von den bereichsspezifischen Regelungen einmal abgesehen, beurteilt sich die Zulässigkeit des Umgangs mit Arbeitnehmerdaten häufig nach dem BDSG. Trotz der immensen Bedeutung des Beschäftigtendatenschutzes fehlte es im deutschen Recht bis 2009 an einer expliziten gesetzlichen Regelung. Wie stehen Sie zu der damals eingeführten Generalklausel des § 32 BDSG?

Wir haben aufgrund von Datenskandalen diverser Firmen wie etwa LIDL, Telekom oder der Deutschen Bahn eine Diskussion bekommen, die wir im Grunde zwar schon hatten, die aber durch die missbräuchliche Verwendung von Arbeitnehmerdaten noch stärker wurde. Eine Diskussion, die aufgezeigt hat, dass wir mit den gegenwärtigen Regularien einen Arbeitnehmerdatenschutz nicht sicherstellen können. Insofern hat sich der Gesetzgeber dann sehr schnell, – vielleicht auch zu schnell – daran gemacht, § 32 BDSG zu schaffen. Im Grunde genommen hat er damit eine Zauberformel – § 28 BDSG war ja insoweit mehr oder weniger anwendbar – durch eine Generalklausel ersetzt, die im Wesentlichen auch kein Mehr an Rechtsklarheit gebracht hat. Man muss also sagen, es handelt sich hierbei größtenteils um symbolische Gesetzgebung, eine politische Maßnahme, um den Druck aus der Diskussion zu nehmen. So hat sich bereits frühzeitig gezeigt, dass die Schaffung des § 32 BDSG Inkonsequenzen zur Folge hatte, insbesondere solche systematischer Natur mit Blick auf das Verhältnis zwischen § 28 BDSG und § 32 BDSG. In diesem Kontext sind verschiedene Probleme aufgetreten. Insbesondere war ungewiss, ob präventive Maßnahmen zur Gefahrenabwehr im Betrieb künftig möglich sind oder nicht, was durch die Formulierung des § 32 BDSG nicht hinlänglich sichergestellt wurde. So tat sich die Frage auf, ob man auf § 28 BDSG zurückgreifen kann. Durch den neuen Paragraphen hat man damit am Ende also möglicherweise noch weniger Rechtssicherheit als zuvor. Aber insofern war auch klar – und das wurde im politischen Kontext auch sehr schnell kommuniziert, dass man bei dieser Norm des § 32 BDSG nicht hätte stehen bleiben können. Es hat sich also herausgestellt, dass ein Regelungsbedürfnis bestand, dem man jetzt damit Abhilfe schaffen will, eine Vollregelung zu installieren.

Welche Probleme bringt § 32 BDSG in der Praxis mit sich?

Genau genommen, finden wir bei § 32 BDSG die gleichen Strukturen wieder, die wir schon von § 28 BDSG kennen. Strukturprobleme treten vor allem deshalb auf, weil wir es jetzt gerade mit zwei Normen zu tun haben, die alternativ zur Anwendung gelangen bzw. eine Generalklausel der Generalklausel, die als Auffangvorschrift gelten kann. Gerade mit Blick auf Bereiche, die nicht unmittelbar in § 32 BDSG behandelt sind, ist ein Rückgriff auf § 28 BDSG wieder möglich. Unklar ist insofern, was der Gesetzgeber eigentlich mit der Schaffung des § 32 BDSG gewollt hat.

2. Gesetzesentwurf zum Beschäftigtendatenschutz

Bislang hat der Arbeitnehmerdatenschutz im deutschen Recht noch keine befriedigende Regelung erfahren. So wundert es nicht, dass der Gesetzesentwurf zum geplanten neuen Beschäftigtendatenschutz nach den §§ 32 ff. BDSG dieser Tage heiß diskutiert wird. In seiner Stellungnahme (noch zu dem ursprünglichen Regierungsentwurf) erklärte der Bundesdatenschutzbeauftragte Peter Schaar, es handele sich um einen „tragfähigen Kompromiss" für Beschäftigte und Arbeitgeber, der eine „substantielle Verbesserung" im Umgang mit Beschäftigtendaten darstelle.[1] Sehen Sie das ähnlich?

Wir müssen zunächst sehen, dass wir drei konkurrierende Entwürfe im Bundestag haben: das ist zum einen der Regierungsentwurf, zum anderen ein Entwurf einer Vollregelung jenseits des BDSG von Bündnis 90/Die Grünen und zuletzt einen Entwurf von der SPD, der eine Änderung des BDSG vorsieht. Dies alles sind Möglichkeiten einer neuen Struktur des Bundesdatenschutzrechts. Die Bewertung muss man aber im Einzelnen vornehmen. Ich bin aber durchaus auch mit Herrn Schaar der Auffassung, dass zunächst einmal ganz entscheidend ist, dass wir Regelungen bekommen. Der Teufel liegt dabei aber im Detail. Wenn wir uns die Regelungen angucken, auch gerade die Regelungen im Regierungsentwurf, werden wir Kritik äußern können und natürlich hier und da aus Datenschutzsicht natürlich Nachbesserungsbedarf anmelden.

Die neuen §§ 32 ff. BDSG-E deckt ein weites Spektrum ab: Von der Datenverarbeitung vor Begründung eines Beschäftigungsverhältnis bis zu der Frage der Zulässigkeit einzelner Überwachungsmaßnahmen im Arbeitsverhältnis selbst werden zahlreiche Aspekte angesprochen. Dennoch können abstrakt-generelle Regelungen per se nicht alle Einzelfragen erfassen. Wo liegt Ihrer Meinung nach Regelungs- und Verbesserungsbedarf im Bereich der geplanten Neuregelungen des BDSG zum Beschäftigtendatenschutz?

Das ist wirklich ein sehr weites Feld. Dazu müsste man sich die ganzen Spezialregelungen einmal angucken. Vom Grundsatz der Vollständigkeit haben wir aber sicherlich noch Spielraum nach oben. So haben wir bislang etwa nicht die Personalaktenführung sowie den Bereich des Konzerndatenschutzes geregelt. Auch fehlen Reglungen über den Einsatz von RFID-Chips am Arbeitsplatz, was insbesondere naheliegt, wenn man andere technische

[1] „Regierungsentwurf bringt substanzielle Verbesserungen beim Beschäftigtendatenschutz", Bundesbeauftragter für Datenschutz und Informationsfreiheit, 25. August 2010, abrufbar unter: http://www.bfdi.bund.de/cln_136/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2010/36_KabinettbeschlussArbeitnehmerDatenschutz.html.

Fragestellungen mit aufruft. Es gibt in vielen Bereichen Vorschriften, die sehr stark abwägunsspezifisch sind und nicht die nötige Klarheit haben, die man schaffen könnte.

Begrüßenswert wäre es, die Dinge noch etwas mehr auf die Praxisrelevanz hin zu formulieren. Das sind Schlaglichter, die man sicherlich anbringen kann. Letztlich ist klar: Die Diskussion im Detail über den Arbeitnehmerdatenschutz hat die gesamte Problematik des Arbeitnehmerrechtsschutzes insgesamt aufgeworfen – es ist die Fragestellung der Abwägung zwischen Kapital und lohnabhängiger Arbeit. Das ist aber nur die eine Seite. Auf der anderen Seite haben wir das Problem des Verhältnisses von Recht und Technik. Und zwar insofern, als dass die Gesellschaft immensen technischen Innovationszyklen unterliegt und daneben einen Zug zur Ökonomisierung von personenbezogenen Daten kennt. Dieses beides bedeutet natürlich, dass wir uns in einem sehr schwierigen Abstimmungsprozess auf politischer Ebene befinden. Eine Antwort zu finden, ist eben nicht nur von dem Vorverständnis des Verhältnisses von Arbeitgeber und -nehmer abgängig, sondern auch von diversen anderen Fragen. Welche Technik darf ich einsetzen? Wo ist eine Technik möglicherweise aus rechtsethischen Gründen nicht mehr zulässig? Wo kommen wir an Grenzen mit Blick auf das informelle Selbstbestimmungsrecht der Beschäftigten vor Ort? Ein wichtiger Kritikpunkt am Regierungsentwurf ist die Regelung der Videoüberwachung in den Betrieben. Die Entscheidung, dass man eine heimliche Videoüberwachung nicht zulassen will, ist in der Tat eine Strukturentscheidung, die ich sehr begrüße. Heimliche und verdachtlose Datenerhebung am Arbeitsplatz bringt Probleme mit sich und hat sehr kritisch kommentiert zu werden. Es bedarf also in diesen Fällen einer sehr schwerwiegenden Verhältnismäßigkeitsprüfung. Wenn sich der Gesetzgeber völlig gegen eine heimliche Videoüberwachung ausspricht, so finde ich das sehr konsequent. Im Gegenzug dazu steht seine Entscheidung, die offene Videoüberwachung sehr weitgehend zuzulassen und eine Regelung zu schaffen, bei der die Videoüberwachung schon fast zur Normalität im Betrieb wird. Hier wird die Videoüberwachung künftig nicht nur zum Schutz von betrieblichen Beschäftigten und Eigentum des Betriebes möglich sein, sondern etwa auch zur Qualitätskontrolle, was letztlich bedeutet, dass jeder an seinem Arbeitsplatz videoüberwacht werden kann. Sogar in Pausenräumen, die nicht überwiegend zu privaten Zwecken verwendet werden, soll eine Videoüberwachung eingeführt werden. Das geht mir deutlich zu weit. Man muss sich fragen: Ist hier am Ende der gläserne Arbeitnehmers aufgerufen? Wird jeder Handschlag letztlich digitalisiert und rekonstruierbar? Das kann es nicht sein. Hier müssen wir an eine menschengerechte Umsetzung von Regelungen zur informellen Selbstbestimmung drängen. So weitgehend darf die Videoüberwachung nicht gehen.

II. Selbstregulierung

Wie stehen Sie zum Thema Selbstregulierung im Bereich des Arbeitnehmerdatenschutzes? Was für Fälle sind Ihnen aus der Praxis im Hinblick auf Selbstregulierung bekannt und wie wird das Thema in der Praxis gehandhabt?

Ein aktuelles Beispiel für die Selbstregulierung haben wir mit dem Kodex der BITKOM zu Panoramadiensten im Internet. Im Zuge der Entwicklung von Google Street View hat unsere Behörde mit Google verhandelt und bestimmte Vorgaben vereinbart, die eingehalten werden können und müssen. Google hat sich dabei mit uns insoweit verständigt, dass die Betroffenen Hauseigentümer ein Vorabwiderspruchsrecht hinsichtlich der Veröffentlichung von Bildern haben. Dies fand ich sehr sinnvoll. Der Kodex der BITKOM sieht ein solches Vorabwiderspruchsrecht nicht vor. Und so stellt sich die Frage: Sind

Selbstregulierungsmaßnahmen, ist also die regulierte Selbstregulierung in dem Bereich, in dem es darum geht, unterschiedliche Interessen zu harmonisieren, wirklich in der Lage, annehmbare Strukturen zu schaffen? Wir haben jedenfalls von der Seite der Aufsichtsbehörden klargestellt, dass wir diese Art der Selbstregulierung nicht akzeptieren. Weder als eine Art antizipierte Sachverständigengutachten noch als Verwaltungsvorschrift, die wir dann zu Rate ziehen, wenn es darum geht, die entscheidenden Paragraphen anzuwenden. Insoweit sind wir also der Meinung, diese Form der Selbstregulierung liegt deutlich hinter den gesetzlichen Anforderungen. Deswegen bin ich insgesamt auch skeptisch. Nicht nur zuletzt aus dieser Erfahrung heraus, glaube ich, dass Selbstregulierung immer da eine Rolle spielt, wo ein Eigeninteresse der Betriebsleitung daran besteht, bestimmte Dinge zu optimieren. Regulierte Selbstregulierung ist da interessant, wo ich etwa den Datenschutz als Maßnahme zur Wettbewerbsverbesserung, als Standortvorteil einsetzen kann, also dort, wo ich mir Vorteile bei Kunden verspreche. Wenig Sinn macht es dort, wo es darum geht, dass unterschiedliche Interessen entschieden oder Rechtseingriffe festgelegt werden. Hier wird man ohne rechtliche Regelungen kaum auskommen.

B. Überwachungsmaßnahmen

Welche Überwachungsmaßnahmen kommen vorwiegend in der Praxis zum Einsatz? Gibt es neuere Tendenzen?

Zunächst einmal muss man sicherlich die Videoüberwachungstechnologie sehen, die mehr und mehr um sich greift und bei der es auch schwer ist, klare Zuschreibungen zu machen. Denn oft wird auch nach außen hin überwacht, etwa zum Schutze des Eigentums. Gerade in öffentlich zugänglichen Bereichen. Hier ist danach zu fragen, ob man nicht eine Regelung für die Arbeitnehmerüberwachung in öffentlichen Bereichen braucht, die über den § 6b BDSG hinausgeht. Eben weil es eine Schutzrichtung ist, die noch tiefer greift. Das BAG stellt ja vollkommen zu Recht fest, dass eine analoge Anwendung des § 6b BDSG in diesen Bereichen nicht zulässig ist – eben weil es eine andere Interessenlage gibt: im Gegensatz zum Kunden, der bestimmte Bereiche meiden kann, steht dem Arbeitnehmer nicht die Möglichkeit offen, seinen Arbeitsplatz nach Belieben zu verlassen, weil er nicht videoüberwacht werden will. Ein weiterer Punkt ist der Einsatz der RFID-Technologie, die es hochgradig ermöglicht, durch Dritte Daten abzufangen, ohne dass dem – ohne entsprechende Vorkehrungen zu treffen – Einhalt zu gebieten ist. Es geht aber auch um die Frage der Standortdaten, die beim Arbeitgeber landen, wie etwa bei GPS. Das fängt beim Dienstwagen an, den man möglicherweise über den Beruf hinaus auch privat nutzt, und hört beim Dienst-Handy auf, das man auch mit entsprechenden Ortungsmöglichkeiten nutzt.

Wie lautet ihr Vorschlag hinsichtlich einer Best Practice zu dem Umgang mit den neuen Technologien?

Erst einmal ist es ganz entscheidend, bei dieser Entwicklung der neuen Technologie von einer höchstmöglichen Transparenz bei ihrem Einsatz auszugehen. D.h. es muss jedem Mitarbeiter auf jeden Fall klar sein, was da eigentlich passiert. Dass etwa seine Standortdaten angegeben werden, wenn er bestimmte Dinge nutzt. Es muss aber auch der Einsatz dieser Technologie einen rechtlichen Rahmen haben. Es kann nicht sein, dass die Anwendung der Technologie im Belieben des Arbeitgebers steht. Wir brauchen vielmehr klare Vorgaben für den Einsatz

dieser modernen Technologien. Betroffen hiervon sind die nicht nur die RFID-Technologie und die Ortung mit Handy und Dienstwagen. Weiterhin spielt der Bereich der biometrischen Daten in der Praxis auch eine erhebliche Rolle. Für all dies brauchen wir klare Regelungen. Diese dürfen nicht als Generalklausel verstanden werden und müssen eine nach wie vor ohnehin transparente Praxis legitimieren. Die Möglichkeiten, moderne Technologien einzusetzen, bestehen und man darf sich jetzt auch nicht auf den Standpunkt stellen, sie dürfen von Arbeitgebern generell nicht genutzt werden. Natürlich ist es erforderlich, mit der neuen Technik umzugehen. Aber es muss klar sein, dass nur Daten erhoben und Informationen generiert werden dürfen, wenn ein zulässiger Zweck vorliegt, etwa die Sicherung des Eigentums. Wo steht der Lastwagen, wenn ich ihn abgestellt habe? Ist er dort noch vorhanden? In welcher Wiese kann ich disponieren, wenn ich eine Ware von A nach B transportiere? Es muss immer klar sein, dass es hier darum geht, vorgegebene Strukturen rechtlich umzusetzen und eben keine Totalüberwachung des Arbeitnehmers vorzunehmen, die auch in die Freizeit hinein diffundiert.

C. Bewusstsein über den Datenschutz

Was denken Sie über das Bewusstsein der Arbeitnehmer und -geber hinsichtlich des Datenumgangs? Findet ein Wandel im Denken statt oder fehlt es Ihrer Einschätzung nach an der Sensibilität der Involvierten?

Ich glaube, es ist durchaus schwer, zu verallgemeinern. Wir haben viele Einsatzbereiche von Videotechnik in kleinsten Betrieben, wo es darum geht, dass die Technik exzessiv einzusetzen, um Sicherheitsbedürfnisse des Arbeitgebers zu erfüllen. Teilweise fehlt es also an jeglicher Sensibilität mit Blick auf das informationelle Selbstbestimmungsrecht der Arbeitnehmer. Oft gibt es Kleinbetriebe, in denen Wildwuchs herrscht und in denen es ohne Reflexion zur Sache geht. In den größeren Betrieben haben wir die Diskussion schon allein durch das Bestehen von Betriebsräten und betrieblichen Datenschutzbeauftragten. Da kommt dann eine ganz andere Kultur der Diskussion zustande. Auch wenn letztlich Vieles aus datenschutzrechtlicher Sicht möglicherweise nicht hinreicht. Ich erinnere an die Diskussion, ob die Möglichkeit besteht, durch Beschlüsse des Betriebsrates über das hinauszugehen, was datenschutzrechtlich zulässig ist. Hierzu sage ich ganz klar: Das darf nicht sein. Auch innerbetriebliche Beschlüsse müssen sich an die gesetzlichen Rahmungen halten und auch die Arbeitnehmervertreter dürfen nicht über das hinweggehen, was der Einzelne erwarten darf.

Wo sehen Sie im Hinblick auf die stetig voranschreitende technische und technologische Fortentwicklung die die Hauptgefahren in der nunmehr stark digitalisierten Arbeitswelt?

Man kann schon im Vorwege des Arbeitsvertrags ansetzen. Wenn wir uns die Situation bei der Bewerberauswahl angucken, haben wir ein ganz klares Problem in der digitalisierten Welt. Wir haben viele Menschen, die bereits, ohne dass man etwas Geschriebenes von ihnen erhalten hat, bekannt sind, da man sie im Internet über Personensuchmaschinen aufruft oder etwa über die sozialen Netzwerke recherchiert. Dies eröffnet neue Möglichkeiten, sich Informationen über Personen zu beschaffen, die im Zusammenhang mit einem Arbeitsrechtsverhältnis sehr nachteilig sein können.

Herr Professor, Sie engagieren sich im Rahmen Ihres aktuellen Projektes „Meine Daten kriegt ihr nicht!“ für die Aufklärung von Schülern, um diese zu sorgsamem Umgang mit eigenen und fremden Daten anzuhalten. Wenn Sie statt der Schüler nun Arbeitnehmer vor sich sitzen hätten, was würden Sie diesen raten?

Dieser Ansprache käme möglicherweise schon zu spät, muss man sagen. Denn die heutigen Schüler sind die Arbeitnehmer von morgen und wenn wir uns angucken, wie lange sich Daten heute im Internet halten und wie schwer es ist, sie wieder rauszubekommen, muss man früher ansetzen. Um einen gute Ausbildungsstelle und einen guten Arbeitsplatz zu erhalten, ist es natürlich erforderlich, dass man die personenbezogen Daten, die man von sich preis gibt, auch reflektiert und nicht in einem jugendlichen Überschwang Dinge von sich preis gibt, die man nachher bereut.

Käme der Rat für die Arbeitgeber auch zu spät?

Im Regierungsentwurf zum Arbeitnehmerdatenschutz wird die Nutzung von sozialen Netzwerken mit Blick auf Bewerber streng reguliert. Die Frage lautet aber, ob sich Arbeitgeber an eine solche Regelung halten würden, würde sie Gesetz werden. Letztlich ist jeder Arbeitgeber natürlich in der Lage, im Internet zu recherchieren, ohne dass es jemand von außen erfährt. Ich plädiere aber dafür, dass man – wenn man sich schon ein Bild über Menschen, möglicherweise auch gerade von jungen Menschen anhand ihrer im Internet öffentlich zugänglichen Daten machen will – dies nicht als persönliches K.O.-Kriterium wertet, sondern mit einer gewissen Liberalität zu sehen. Dies impliziert letztlich, dass man auch Menschen, die sich möglicherweise digital tätowieren, ja stigmatisiert haben, aufgrund einer Präsentation im Internet nicht bereits deshalb aus dem Kreis von Bewerbern ausschließt. Mittlerweile gibt es so viele Dinge, die man über einzelne Menschen weiß, dass es letztlich auch vielleicht. gar nicht mehr den Nagel auf den Kopf trifft, wenn man sagt „Wir wollen keine Leute, die sich zu sehr nach außen bewegen.“. Oft sind es ja auch sehr kommunikative Menschen, für die es konkrete betriebliche Verwendungen gibt. Im Gegensatz zu den Anhängern der Post-Privacy-Ideologie glaube ich aber auch nicht, dass eine stärkere Offenstellung unserer Daten im Internet dazu führt, dass wir nicht mehr in diskriminierender Weise damit umgehen. Auch wenn die Daten alle offen sind, wenn also alles für Arbeitgeber und -nehmer insgesamt transparent ist, wird immer noch der Einzelne dahingehend beurteilt, wie er sich dort darstellt. Für Arbeitnehmer ist es tendenziell nicht tunlich, sich so darzustellen, dass es möglicherweise den Eindruck einer Pflichtvergessenheit oder einer größeren persönlichen Labilität erweckt.

D. Technologische Aspekte

Wo sehen Sie angesichts der stetig zunehmenden Technologisierung die größten Gefahren für Arbeitnehmer?

Diese Frage kann man nicht mit einer technologischen Entwicklung wie etwa der der Videotechnik oder der RFID-Technologie erfassen. Die große Gefahr besteht aus der Kombination aller technischen Möglichkeiten und aus der jederzeitigen Rekonstruierbarkeit von Abläufen innerhalb betrieblicher Sphären. Wenn alles, was wir tun, dokumentiert werden kann, etwa durch Bilder oder durch Bewegungsprofile, die erstellt werden, dann gibt es keine Möglichkeit des devianten Verhaltens mehr, ohne, dass man Angst haben muss, dass dies garantiert rauskommt. Wir fordern ja kein Recht des Einzelnen auf deviantes Verhalten mit Blick auf Pflichtvergessenheit am Arbeitsplatz. Was gefordert werden muss, ist dass es keine absolute Kontrolle von Menschen am Arbeitsplatz gibt, die so intensiv und so dicht ist, dass jeder Handschlag rekonstruiert werden kann. Das ist eine Grenze. Diese Grenze ist natürlich schwer quantifizierbar, weil es immer Bereiche gibt, in denen man eine Nachkontrolle haben wird. Aber es muss eben auch Bereiche geben, in denen diese Kontrolle nicht statt findet. Insofern ist ganz wichtig, dass der Einsatz von Technologie in einer menschengerechten Weise erfolgt und nicht zu einer totalen Überwachung am Arbeitsplatz.

Wie kann man diesen Gefahren Ihrer Einschätzung nach am besten begegnen? Was würden Sie diesbezüglich vorschlagen?

Ganz wesentliche Voraussetzungen sind insgesamt, möglichst keine Daten auf Vorrat zu erheben, möglichst keine heimlichen Daten zu erheben und da, wo Daten erhoben werden, dies transparent werden zu lassen.

Was war der bedeutendste Fall, mit dem Sie sich in punkto Arbeitnehmerdatenschutz bislang beschäftigt haben?

Wir haben in unserer Behörde eine Reihe von Fällen gehabt. Bei einem Fall ging es um Bluttest einer großen, international agierenden Firma. Bei den Untersuchungen stellt sich heraus, dass – scheinbar freiwillig – im Bewerbungsverfahren Gesundheitsvorsorgeuntersuchungen angeboten wurden. Diese Untersuchungen wurden für sämtliche Bereiche durchgeführt, also etwa auch für die Verwaltung und nicht etwa bloß für besondere Gefährdungsbereiche. Die Untersuchungen wurden mit Einwilligung der Bewerber vorgenommen. Dies zeigt prägnant, dass die Möglichkeit, aus freiwilligen Stücken in Bewerbungsverfahren in solche Gesundheitsvorsorgeuntersuchungen einzuwilligen, eigentlich faktisch gar nicht besteht.

Haben Sie sich in der Praxis bisher mit Privacy Enhancing Technologies beschäftigt?

In der Praxis sind wir sehr stark damit beschäftigt, die Eingaben abzuarbeiten. In den vergangenen Jahren hat sich unser Arbeitsaufwand etwa verdreifacht. Von daher ist die Tätigkeit der Aufsichtsbehörden oft nicht präventiv ausgerichtet. Wir nutzen aber auch die Möglichkeit, bei Vorhaben, in denen wir früh genug in die Planung einbezogen werden, datenschutzfreundliche Technik zu implementieren.

Was sind die derzeit gängigsten Technologien?

Im Bereich des privaten Datenschutzes spielt sicherlich die Videoüberwachung eine wesentliche Rolle. Die Technik wird immer billiger, die Kameras immer hochauflösender. Den Verwendern stehen damit große Optionen zur Überwachung zu, was insbesondere deshalb gefährlich ist, weil sie oft über kein ausreichendes Wissen über die Handhabung der Technik verfügen.

Arbeiten Sie in diesem Bereich an Lösungsmöglichkeiten?

Unser Ziel ist es, Wissen zu etablieren und klare Vorgaben zu schaffen. Das Thema ist jedoch sehr komplex. Insofern fällt es schwer, Grundsätze herauszugeben, die von den Bürgerinnen und Bürgern ohne Weiteres umgesetzt werden können. Oft handelt es sich um Einzelfälle, denen ein schwieriger Abwägungsvorgang zugrunde liegt.

E. Abschließende Fragen, statistische Daten und interessante Fälle aus der Praxis

Haben Sie selbst schon Untersuchungen hinsichtlich der Thematik des Beschäftigtendatenschutzes eingeleitet?

Wir dürfen uns nicht der Illusion hingeben, sämtliche Sachverhalte im Vorfeld regeln zu können. Vielmehr kann präventive Steuerung in diesem Umfang aufgrund der Komplexität der Materie nicht ausreichend ermöglicht werden. Aktuell arbeiten wir jedoch an einem großen Projekt, das sich mit der Videoüberwachung in Hamburg durch öffentliche Stellen beschäftigt. Gegenwärtig wird deren Zulässigkeit überprüft. Dazu schreiben wir die öffentlichen Stellen an, die uns dann zur Dokumentation über ihre Videoüberwachungsmaßnahmen verpflichtet sind. Dies beansprucht unsere Arbeitskraft in erheblichem Maße. Die Ergebnisse sind wiederum abhängig vom Einzelfall. Darüber hinaus führen wir eine Umfrage bei mehreren Hundert Unternehmen im nicht-öffentlichen Bereich durch, die sich mit der Einstellung betrieblicher Datenschutzbeauftragter beschäftigt. Dabei prüfen wir, ob die Unternehmen ihre Bestellpflicht einhalten. Der betriebliche Datenschutzbeauftragte als Mann des Datenschutzes vor Ort stellt das Bindeglied zwischen betrieblicher Leitung, den Beschäftigten und der Datenschutzbehörde dar. Dadurch gewinnt er an immenser Bedeutung für den Datenschutz im Betrieb. Gleichzeitig fungiert er als starkes Instrument zur Verhinderung von Datenschutzverstößen. Ich sehe in diesem Testfall der regulierten Selbstregulierung und Ausdruck der Autonomie ein großes Potential für den Datenschutz.

Gibt es diesbezüglich Kooperationen mit anderen Datenschutzbeauftragten?

Zum einen gibt es den Düsseldorfer Kreis, in dem die obersten Aufsichtsbehörden als informelle Clearing-Instanz die Einhaltung des Datenschutzes im nicht-öffentlichen Bereich überwachen. Als Pendant hierzu beschäftigt sich die Datenschutzkonferenz mit datenschutzpolitischen Fragen und dem Datenschutz im öffentlichen Bereich.

Welchen prozentualen Anteil ihrer Fälle machen solche mit Zusammenhang zum Arbeitnehmerdatenschutz aus?

Derartige Fälle stammen vorwiegend aus dem Privatsektor und machen eher einen kleinen Teil der Eingaben aus, schätzungsweise etwa 10 % des gesamten Aufkommens. Wir verzeichnen eine Spitze im Bereich der Telemedien/Telekommunikation. Nahezu die Hälfte der Eingaben stammt aus diesem Bereich. Im Gegensatz dazu stammen – entgegen den Befürchtungen vieler – wenige Fälle aus dem Bereich der Eingriffsverwaltung.

Welche Entwicklung nahm der Bereich in den letzten fünf Jahren?

Betriebe sind immer mehr dazu übergegangen, auf die Daten der Arbeitnehmer zuzugreifen. Letztlich kommt es zu einer Ökonomisierung von Daten.

Sehen Sie einen Zusammenhang zwischen den bislang unzulänglichen gesetzlichen Vorgaben und der Anzahl der eingegangenen Beschwerden?

Ich sehe vielmehr einen Zusammenhang zwischen der öffentlichen Diskussion um den Datenschutz und den derzeitigen Bestrebungen, klare Regelungen zu finden.

Was prognostizieren Sie im Hinblick auf die Anzahl der Eingaben für die Zukunft?

Ich rechne mit mehr Eingaben, da das Bewusstsein der Arbeitnehmer im Hinblick auf den Datenschutz gestärkt wird. Im ursprünglichen Gesetzesentwurf war vorgesehen, dass sich der Beschäftigte nur an die zuständige Datenschutzbehörde wenden konnte, wenn er sich zuvor an seinen Arbeitgeber gewendet hat. Dies war sowohl im Hinblick auf die Datenschutzrichtlinie als auch auf das Petitionsrecht nicht rechtskonform. Viele Arbeitnehmer würden, was menschlich ist, von einer Verfolgung der Verstöße absehen. Die Vorabmitteilung war oft also mit einem Rechtsverzicht verbunden. Jetzt ist der Gesetzgeber hingegen auf der sicheren Seite.

Effektiver Datenschutz ist oft leider auch eine Frage der zur Verfügung stehenden Mittel. Wie wollen Sie zukünftig die Flut von Datenschutzrechtsverstößen in den Griff bekommen?

Durch eine Umschichtung und Umstrukturierung. Jedoch sind die Steuerungsmaßnahmen begrenzt, schlimmstenfalls können bei Anwachsen der Zahl der Eingaben keine Präventionsmaßnahmen vorgenommen werden, sondern nur noch Fälle abgearbeitet werden. Wir werden aber unser Potential effektiv zu nutzen wissen und die betriebliche

Eigenverantwortung stärken. Gerade die verstärkte Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten, die wir als natürlichen Verbündeten empfinden, wird hierbei sehr hilfreich sein. Moderner Datenschutz erfordert auch zukünftig einen hohen Bedarf an Eigenverantwortung.