Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes

- Gutachten -

Stand: 08.04.2016

Karin Schuler
Kronprinzenstr. 76, 53173 Bonn
schuler@netzwerk-datenschutzexpertise.de

Dr. Thilo Weichert
Waisenhofstr. 41, 24103 Kiel
weichert@netzwerk-datenschutzexpertise.de

www.netzwerk-datenschutzexpertise.de

Inhalt

1 Vorbemerkung

Der vorliegende, im Netzwerk Datenschutzexpertise erarbeitete Hintergrundtext befasst sich mit der Frage, welche nationalgesetzlichen Regelungen nach der Einigung über eine Europäische Datenschutz-Grundverordnung (EU-DSGVO)[1] zur Verbesserung des Beschäftigtendatenschutzes in Deutschland erforderlich sind. Dabei werden die europäischen Regelungen, die bisherigen Gesetzgebungsbestrebungen in Deutschland, der technische Stand der Digitalisierung in Betrieben, die betrieblichen Erfahrungen von Beschäftigtenvertretungen und Datenschutzbeauftragten und die Rechtsprechung in diesem Bereich berücksichtigt. Der Text schlägt die **Schaffung eines Beschäftigtendatenschutzgesetzes** als Spezialregelung sowohl des allgemeinen Datenschutzrechts als auch des Arbeitsrechts vor, in dem die beschäftigungsspezifischen Fragestellungen des Datenschutzes geregelt werden. Zur normativen Konkretisierung sollen zwischen gesetzlichen und betrieblichen Regelungen wie Betriebsvereinbarungen auch überbetriebliche Kollektivvereinbarungen zwischen der Arbeitnehmer- und der Arbeitnehmerseite etabliert werden, die von der zuständigen Datenschutzaufsichtsbehörde zu genehmigen sind.

Im Folgenden wird einheitlich der Begriff „Beschäftigtendatenschutz“ und nicht der auch gebräuchliche **Begriff „Arbeitnehmerdatenschutz“** verwendet, wenn keine Originalzitate verwendet werden. In der öffentlichen Debatte werden diese beiden Begriffe weitgehend synonym verwendet. Bisher verwendet das Bundesdatenschutzgesetz (BDSG) wie nun auch die EU-DSGVO den Begriff „Beschäftige“ (§ 3 Abs. 11 BDSG, Art. 88 EU-DSGVO, Art. 82 in der Entwurfsfassung). Damit sind nicht nur Arbeitnehmerinnen und Arbeitnehmer erfasst, sondern eine Vielzahl weiterer abhängig Beschäftigter (Auszubildende, arbeitnehmerähnllich Beschäftigte, Beamte …) sowie sich bewerbende Personen. Die folgenden Ausführungen sollen grds. für sämtliche in § 3 Abs. 9 BDSG genannten Personen gelten.

2 Der Regelungsrahmen der Europäischen Union

Auf Ebene der **Europäischen Union** (EU) gab es bisher nur begrenzte Aktivitäten im Bereich des Beschäftigtendatenschutzes. Die derzeit noch geltende Europäische Datenschutzrichtlinie 95/46/EG (EG-DSRl) von 1995 trifft zu Beschäftigungsverhältnissen keine speziellen Aussagen. Eine von der EU-Kommission initiierte Konsultation zum Arbeitnehmerdatenschutzrecht in den Jahren 2001/2002 hatte keine weiteren Initiativen zur Folge. Ein Grund hierfür dürfte auch gewesen sein, dass zu dieser Zeit selbst auf nationaler Ebene in den meisten EU-Mitgliedstaaten kein Regelungsbedarf gesehen wurde. Vereinzelte nationale Gesetze, etwa in Finnland, waren nicht dazu geeignet, Beschäftigte wirksam zu schützen,

[1] Rat der EU, Interinstitutionelles Dossier 2012/0011(COD) 5419/16 06.04.2016, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=DE.

sondern eröffneten der Arbeitgeberseite weite Spielräume für die Kontrolle ihrer Beschäftigten.[2]

Schon seit längerem ist durch die Rechtsprechung des Europäischen Gerichtshofes (EuGH) wie des Europäischen Gerichtshofes für Menschenrechte (EGMR) anerkannt, dass aus der Europäischen Menschenrechtskonvention und den nationalen Grundrechtsgarantien ein gemeinsamer Standard zum Datenschutz abgeleitet werden kann. Mit der **Europäischen Grundrechte-Charta** von 2009 (EuGRCh) wurde dies normativ bestätigt. Sie gewährleistet in Art. 8 EuGRCh ein Grundrecht auf Datenschutz. Die Reichweite dieses Grundrechts ist trotz einer Vielzahl einschlägiger Urteile noch nicht umfassend geklärt. So ist in der EuGRCh neben dem Grundrechtsschutz als Abwehr gegen staatliche Eingriffe auch eine institutionelle Gewährleistung sichergestellt. Wie weit jedoch der Schutzauftrag des Staates im Verhältnis von Bürgern zu mächtigeren Wirtschaftsunternehmen geht und ob eine entsprechende Gewährleistungsfunktion besteht, ist – anders als in der Rechtsprechung des BVerfG[3] – noch nicht eindeutig erkennbar. Insbesondere ist bisher nicht geklärt, inwieweit Grundrechte eine Ausstrahlung auf private Unternehmen haben, die sich in einer strukturellen Machtbeziehung zu abhängigen Personen befinden, so wie dies im Verhältnis von Beschäftigten zu ihrem Arbeitgeber der Fall ist.

Angesichts dieser Vorgeschichte durfte man keine übertriebenen Erwartungen an die **Europäische Datenschutz-Grundverordnung** (EU-DSGVO) haben, zu der die EU-Kommission am 25.01.2012 den Aufschlag machte. Nach Art. 288 Abs. 2 S. 2 des Vertrags über die Arbeitsweise der EU (AEUV) ist eine Verordnung in all ihren Teilen verbindlich und – anders als eine Richtlinie – direkt anwendbar. Der Vorschlag zur EU-DSGVO eröffnete in Art. 82 (jetzt 88) den Mitgliedstaaten die Möglichkeit, „in den Grenzen dieser Verordnung per Gesetz“ den Beschäftigtendatenschutz zu regeln. Ergänzend sollte die Kommission ermächtigt werden, hierzu delegierte Rechtsakte zu erlassen. Der Vorschlag der Kommission enthielt zudem bereits eine Reihe weiterer grundlegender Bestimmungen, die nicht ausschließlich aber auch den Beschäftigtendatenschutz betrafen.

Inhaltlich konkreter und restriktiver war dann der Beschluss des **Europaparlaments** (EP) vom 12.03.2014, der im Art. 82 (jetzt 88) eine engere Zweckbindung und das Verbot von Profilbildungen vorsah. Außerdem wurden unfreiwillige Einwilligungen und die Überwachung in Telekommunikationsnetzen thematisiert. Für Konzerne war eine gewisse Privilegierung vorgesehen.

Der **Rat der EU** schlug im Juni 2015 eine eigene Formulierung zu Art. 82 (jetzt 88) vor: „Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext … vorsehen“. Wie das Verhältnis der grundlegenden europäischen Normen in einer Verordnung und spezieller nationaler Gesetzgebung aussehen soll, verschweigen die Vorschläge der europäischen Gesetzgeber. Ebenso blieb unklar, wie die Erleichterungen für multinationale Unternehmen aussehen sollen.

[2] Arbeitnehmerdatenschutz wird massiv abgebaut, DANA 2/2009, 80.

[3] Z. B. BVerfG, B. v. 23.10.2006, 1 BvR 2027/02, DVBl 2007, 111 ff.

3 Art. 88 (82 im Entwurf) der EU-DSGVO

Der Rat, das Parlament und die Kommission der Europäischen Union (EU) einigten sich schließlich im sog. **Trilog** am 15.12.2015 auf einen gemeinsamen Text der Europäischen Datenschutz-Grundverordnung (EU-DSGVO). Im Mai oder Juni 2016 werden der Rat und das Parlament die EU-DSGVO beschließen. Ein Inkrafttreten der Regelungen ist für das Jahr 2018 vorgesehen.

Während viele Regelungen der EU-DSGVO unmittelbar anwendbar und durchsetzbar sein werden und keiner weiteren Umsetzung durch nationale Gesetze bedürfen, enthalten andere Bestimmungen lediglich **Regelungsoptionen für die Normgeber** auf nationaler oder europäischer Ebene und bedürfen einer Umsetzung oder einer Konkretisierung. Neben den Gesetzgebern kommen als Normgeber auch in begrenztem Maße die Exekutive sowie die Parteien von Kollektivvereinbarungen in Betracht.

Dies trifft für die „Datenverarbeitung im Beschäftigungskontext“ zu, die in Art. 88 EU-DSGVO geregelt wird. Damit wird die Regelungskompetenz zumindest teilweise an die **Mitgliedstaaten** zurückgespielt. Es ist daher zu klären, welchen Regelungsspielraum die EU-DSGVO den Mitgliedstaaten lässt, was dies für den deutschen Gesetzgeber und weitere mögliche nationale Normadressaten bedeutet und welche Regelungmöglichkeiten und Regelungsnotwendigkeiten hierdurch konkret entstehen.

Die Regelung des Art. 88 zur „Datenverarbeitung im Beschäftigungskontext“ hat folgenden Wortlaut:

1. Die Mitgliedstaaten können durch Gesetz oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von gesetzlich oder tarifvertraglich festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.

2. Diese Vorschriften umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Datenübermittlung innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen und die Überwachungssysteme am Arbeitsplatz.

3. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften, die er nach Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

In den Erwägungsgründen wird zu der vorgenannten Regelung Folgendes ausgeführt:

(155, im Entwurf 124) Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen (einschließlich 'Betriebsvereinbarungen') können spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden, und zwar insbesondere Vorschriften über die Bedingungen, unter

denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von gesetzlich oder tarifvertraglich festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses.

Die Regelung beschreibt in Art. 88 Abs. 1, zu welchen Zwecken Beschäftigtendaten verarbeitet werden dürfen und wann die Öffnungsklausel gelten soll. Für die in Nummer 1 genannten Zwecke dürfen auf nationaler Ebene Regelungen getroffen werden. Dies entspricht auch Art. 153 i. V. m. Art. 114 Abs. 2 AEUV, der die Kompetenz für die Regelung von Arbeitsrecht bzw. den Arbeitnehmerrechten und -interessen den Mitgliedstaaten überlässt. Die Aufzählung in Art. 88 EU-DSGVO ist beispielhaft, nicht abschließend. Der Anknüpfungspunkt der Datenverarbeitung (DV) muss in jedem Fall das **Beschäftigungsverhältnis** sein. Zwecke der Verarbeitung, die mit dem Beschäftigungsverhältnis nicht in Zusammenhang stehen, werden nicht erfasst.

Mit der Anwendbarkeit der EU-DSGVO gilt für den Beschäftigtenbereich das „Verbot mit Erlaubnisvorbehalt“. Artikel 6 Abs. 1 lit. b . EU-DSGVO, der die für die Vertragserfüllung erforderliche Datenverarbeitung erlaubt, ist im Beschäftigungskontext nicht direkt anwendbar. Vielmehr sind hierfür die in Art. 88 genannten spezifischeren Rechtsnormen einschlägig. Bei den in Art. 88 Abs. 1 für potenzielle nationale Regelungen genannten Zwecken handelt es sich um legitime Zwecke der Datenverarbeitung durch den Arbeitgeber. Hierbei soll der Schutz der Beschäftigten gemäß Absatz 2 durch **geeignete besondere Maßnahmen** erfolgen, die in den nationalen Regelungen festgeschrieben werden müssen. Die nationalen Normgeber sind bei der Gestaltung von Maßnahmen jedoch nicht frei, sondern müssen sich an den Grundprinzipien des Art. 5 EU-DSGVO und am Regelungskonzept der Verordnung unter Berücksichtigung der spezifischen Gegebenheiten des Beschäftigungsverhältnisses orientieren. Sie können nur von diesen Vorgaben abweichen, wenn es plausible Gründe gibt. Ob dieser Rahmen beachtet wird, kann letztlich vom EuGH überprüft werden.[4]

Art. 88 Abs. 1 erwähnt ausdrücklich **Kollektivvereinbarungen** als mögliche Zulässigkeitsgrundlage für den Umgang mit Beschäftigtendaten. Im Erwägungsgrund wird präzisiert, dass es sich dabei **auch** um Betriebsvereinbarungen handeln kann. Daraus ist zu schließen, dass wie bisher ebenso Tarifverträge als konkretisierende Rechtsnormen in Frage kommen. Würde der nationale Gesetzgeber weitere Möglichkeiten für Kollektivvereinbarungen schaffenzu treffen, so kämen auch diese als künftige Zulässigkeitsgrundlage in Betracht. Kollektivvereinbarungen müssen sich im Rahmen der EU-DSGVO bewegen wie dem evtl. vom nationalen Gesetzgeber vorgegebenen weiteren Rahmen. Dieser muss seinerseits mit der EU-DSGVO in Einklang stehen.

Sollen im Beschäftigungsverhältnis **Einwilligungen** zur Legitimation einer

[4] Schüßler/Zöll DuD 2013, 640 f.

Verarbeitung herangezogen werden, so muss der Arbeitgeber Art. 7 Abs. 4 EU-DSGVO beachten, da zwischen dem Arbeitgeber und dem Beschäftigten ein Abhängigkeitsverhältnis besteht. Zwar dürfte daraus wohl nicht geschlossen werden, dass Einwilligungen als Zulässigkeitsgrundlage völlig ausscheiden[5], aber wenn eine Verarbeitung für die Abwicklung des Beschäftigungsverhältnisses nicht erforderlich ist und für den Betroffenen Nachteile damit verbunden wären, kann keine Freiwilligkeit angenommen werden (vgl. auch Erwägungsgrund 43, im Entwurf 34). Betrachtet der nationale Gesetzgeber diese Voraussetzungen in bestimmten Konstellationen im Arbeitsverhältnis als gegeben, so wird er in diesen Bereichen auch einen völligen Ausschluss von Einwilligungen regeln können.[6]

Besondere Regelungskompetenzen hat der nationale Normgeber im Beschäftigungskontext insbesondere dort, wo in der EU-DSGVO für spezifische Formen der Datenverarbeitung regulative Konkretisierungen erlaubt werden. Dies ist z. B. im Hinblick auf hochproblematische automatisierte Entscheidungen und das **Profiling** (Art. 22, im Entwurf 20) von praktischer Relevanz. Hier sind dann besondere angemessene Garantien nötig (Erwägungsgrund Nr. 71, im Entwurf 58).

Hinsichtlich der Verarbeitung **besonderer Kategorien von Daten**, also etwa von genetischen, biometrischen oder Gesundheits-Daten (vgl. Art. 4 Abs. 13-15) oder Daten zu religiösen oder politischen Überzeugungen oder zur Gewerkschaftszugehörigkeit, enthält Art. 9 Abs. 2 lit b beschäftigungsrelevante Öffnungsregelungen bei Erforderlichkeit nach dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes, wobei auch insofern ausdrücklich auf die Regulierungsmöglichkeit in Kollektivvereinbarungen hingewiesen wird. Im Hinblick auf Gesundheitsdaten wird zudem in lit. h die Erforderlichkeit für die Gesundheitsvorsorge und die Arbeitsmedizin sowie für Dienste im Gesundheits- und Sozialbereich verwiesen.

4 Deutsche Gesetzgebungsgeschichte

Die EU-DSGVO verweist also in Bezug auf den Beschäftigtendatenschutz zurück auf die nationale Regelungsebene. Es mag daher hilfreich sein, sich die bisherigen Aktivitäten des deutschen Gesetzgebers in dieser Angelegenheit vor Augen zu führen.

Schon vor dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983[7], in dem aus dem deutschen Grundgesetz ein Grundrecht auf informationelle Selbstbestimmung abgeleitet wurde, wurde von unterschiedlichen Seiten ein Arbeitnehmerdatenschutzgesetz gefordert. Das Volkszählungsurteil verstärkte dieses Anliegen, indem für jede Form der personenbezogenen Datenverarbeitung eine möglichst spezifische gesetzliche Grundlage gefordert wurde. Seitdem sah jede **Koalitionsvereinbarung** der unterschiedlichen Regierungsparteien im Bundestag die Erarbeitung und Beschlussfassung eines Gesetzes vor, mit dem die Verarbeitung der Daten der Beschäftigten durch die Arbeitgeber reguliert werden sollte. Doch alle Versuche, dieses Anliegen umzusetzen, blieben erfolglos, da die jeweiligen Koalitionspartner sich nicht einigen konnten. Eine wesentliche Ursache für diese

[5] So wohl Franzen DuD 2012, 323 f.; wie hier Götz DuD 2013, 638.

[6] Anders wohl Schüßler/Zöll DuD 2013, 641.

[7] BVerfG, NJW 1984, 419 ff.

Unfähigkeit war die offensive Lobbypolitik der Arbeitgeberverbände, die ein solches Gesetz stets zu verhindern wussten. Dass von Seiten der Gewerkschaften und der SPD die Forderung nach einem Beschäftigtendatenschutzgesetz nicht mit erster oberster Priorität verfolgt wurde, spielte sicher auch eine Rolle.

Die **Arbeitsgerichte**, insbesondere das Bundesarbeitsgericht (BAG), wirkten mit einer relativ überwachungskritischen Rechtsprechung durch Entscheidungen im Einzelfall einer übermäßigen digitalen Kontrolle der Beschäftigten durch ihre Arbeitgeber entgegen. Die Überwachung von Beschäftigten wurde lange Zeit nur wenig öffentlich diskutiert. Beides führte dazu, dass kein übermäßiger politischer Handlungsdruck entstand.

Es mag Ironie der Geschichte sein, dass die schwarz-roten Regierungsparteien in der 16. Legislaturperiode sich in ihrem Koalitionsvertrag nicht mehr darauf verständigt hatten, den Beschäftigtendatenschutz spezifisch zu regeln. Doch just in dieser Zeit wurden gewaltige Überwachungsaktionen gegenüber Beschäftigten durch Großunternehmen bekannt, etwa durch Lidl, die Telekom und die Deutschen Bahn AG. Dies veranlasste die Regierungsfraktionen, mit heißer Nadel einen **§ 32 BDSG** zu stricken, womit erstmals 2009 eine allgemeine explizite gesetzliche Regelung zum Beschäftigtendatenschutz erlassen wurde. Dies erfolgte als kurzfristige Ergänzung zu einer BDSG-Änderung, bei der es um eine längerfristig vorbereitete Regulierung zum Adresshandel und zu Auskunfteien ging. Das Problem des § 32 BDSG war und ist, dass er als reine Reaktion auf die skandalösen Vorgänge in einigen Unternehmen nicht ansatzweise die Breite der damals schon bestehenden rechtlichen Problematik der Beschäftigtenüberwachung erfasste und viele übliche Verwendungen von Beschäftigtendaten im Unternehmen (z. B. bei der Protokollierung von IKT-Systemen, bei innerbetrieblichen Services wie Kantinensystemen oder bei Sicherheitssystemen wie Whistleblowing-Hotlines) ignorierte. Es blieb unklar, wie man deren rechtskonformen Betrieb zukünftig erreichen kann, da viele Anwendungen nicht im strengen Sinne der Durchführung des Beschäftigtenverhältnisses dienen.

Praktische Auslegungsfragen zu dieser Regelung, insbesondere zum Verhältnis der Spezialregelung des § 32 zu den allgemeinen Regeln des BDSG, blieben streitig und sind bis heute von der Rechtsprechung unentschieden. Folgerichtig verabredeten FDP und CDU/CSU für die folgende **17. Legislaturperiode** erneut die Schaffung eines umfassenden Beschäftigtendatenschutzrechts. Dies führte zu einer Vielzahl von Vorschlägen – von einem äußerst umstrittenen Regierungsvorschlag[8] über Entwürfe von SPD[9] und Bündnis 90/Die Grünen[10] bis hin zu einer Initiative des DGB[11]. Eine Einigung und eine Beschlussfassung kamen aus den vorgenannten Gründen wieder nicht zustande.

Die aktuelle Koalition von CDU/CSU und SPD verständigte sich für die **18. Legislaturperiode** im Herbst 2013 zunächst auf einen unverbindlichen Formelkompromiss, indem die Absicht, „eine nationale Regelung zum Beschäftigtendatenschutz“ zu schaffen, unter die Bedingung, dass „mit einem

[8] BT-Drs. 17/4230 v. 15.12.2010.

[9] BT-Drs. 17/69.

[10] BT-Drs. 17/4853.

[11] Abgedruckt in AuR 2010, 315.

Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht gerechnet werden“ könne, festgehalten wurde. Zum Schutz von Whistleblowern heißt es: „Beim Hinweisgeberschutz prüfen wir, ob die internationalen Vorgaben hinreichend umgesetzt sind“.[12]

Da der § 32 BDSG äußerst vage, unklar und umstritten ist, kann man in dieser Regelung **nach Inkrafttreten der EU-DSGVO** kaum noch eine spezifische Norm erkennen, die Art. 88 der Verordnung materiell-rechtlich konkretisiert; vielmehr muss man diese Regelung wohl grundsätzlich für obsolet ansehen.[13] In einer Frage kann und muss § 32 BDSG jedoch als spezialgesetzliche Konkretisierung verstanden werden: Der Anwendungsbereich des Arbeitnehmerdatenschutzes wird durch § 32 Abs. 2 BDSG auf personenbezogene Daten erstreckt, „ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung einer solchen Daten erhoben werden.“ Gemäß § 32 Abs. 2 BDSG erstreckt sich der Schutz von Beschäftigten daher auch auf Daten in unstrukturierten Akten.

Nachdem der Text der EU-DSGVO mit der Öffnungsklausel für den nationalen Gesetzgeber und deren Inkrafttreten im Jahr 2018 feststehen, haben sich weder die **Bundesregierung** noch die Regierungsfraktionen dazu geäußert hat, ob, mit welchem Zeitplan und mit welchen Inhalten der Beschäftigtendatenschutz in Deutschland geregelt werden soll.

5 Technische und strukturelle Aspekte der Beschäftigtendatenverarbeitung

Wer sich über die Regulierung des Beschäftigtendatenschutzes Gedanken macht, muss die **Realitäten** in den Unternehmen und Betrieben berücksichtigen. Sowohl das, was heute technisch möglich und üblich ist, als auch die Best Practises moderner Unternehmensorganisation müssen sich in Regulierungsbemühungen widerspiegeln. Dies bedeutet nicht, dass alles, was möglich und üblich ist, auch wünschenswert und zulässig sein muss. Doch müssen die Normen klare Antworten geben und dürfen nicht allgegenwärtige Entwicklungen ignorieren.

In vielen Staaten wird von den am Markt verfügbaren technischen Möglichkeiten intensiver Gebrauch gemacht. Dies gilt vor allem für die **USA**, in denen Beschäftigtenkontrolle wesentlich intensiver als in Staaten der EU betrieben wird. Viele Anbieter von Informations- und Kommunikationstechnik (IKT) haben dort ihren Sitz und entwickeln in erster Linie für ihren heimischen Markt. Obwohl ihre IKT-Produkte auch in Deutschland und in Europa genutzt werden, orientieren sich die Anbieter bei der Ausgestaltung ihrer Angebote, auch soweit sie zur Beschäftigtenkontrolle geeignet sind, zumeist nicht an in Europa bestehenden rechtlichen Restriktionen, sondern an dem, was technisch möglich und von Arbeitgeberseite gewünscht und nachgefragt wird.

[12] Koalitionsvertrag, S. 70, zit. nach DANA 1/2014, 18.

[13] Schüßler/Zöll DuD 2013, 643; zweifelnd Gola/Pötters/Thüsing, Art. 82 DSGVO: Öffnungsklausel für nationale Regelungen zum Beschäftigtendatenschutz, 2016, S. 7 f.; unklar auch Roßnagel, Stellungnahme zum öffentlichen Fachgespräch im Ausschuss Digitale Agenda des Deutschen Bundestags v. 19.02.2016, Ausschussdrucksache 18(24)94, S. 9.

IKT-Systeme bieten daher heute die technische Möglichkeit, Beschäftigte zu jedem Zeitpunkt und bei jedem Arbeitsschritt **nahezu vollständig zu überwachen**. Die Erfassung von Daten erfolgt, um nur einige zu nennen, über die automatisierten Produktionslinien, ERP-Systeme, voll integrierte Personalmanagementsysteme, Telekommunikations- und Bürokommunikations-Systeme, integrierte biometrische Erkennung und Erfassung, Telematik-Lösungen zur Flottenkontrolle, Videoüberwachung und mit digitaler Sensorik. Eine Datenanreicherung kann sowohl über allgemein zugängliche Quellen (insbesondere über soziale Netzwerke) als auch über spezifische Dritte – Behörden wie private Stellen – erfolgen. Ein beschäftigungsspezifischer Sonderfall ist die technische Möglichkeit, die Kundendaten eigener Beschäftigter, unabhängig von der rechtlichen Zulässigkeit, in die arbeitsrechtlich relevante Personaldatenverarbeitung einzubeziehen.

Ein Charakteristikum heutiger **IKT-Systeme** besteht in ihrer Omnipräsenz und Varianz. Fragestellungen jeder Größenordnung (vom Etikettendruck bis zum ERP-System) werden mit IKT behandelt; es gibt Vernetzung jeder Intensität (vom Stand-alone-Rechner über die Anbindung in einem Firmennetz bis zur weltweiten Erreichbarkeit im Internet), Verwendung unterschiedlichster Technologien (proprietäre Ansätze vs. standardisierte Lösungen). Entscheidungen zur physischen Datenhaltung (eigene Server oder Software/Platform/Infrastructure-as-a-Service bei Dienstleistern in Deutschland, Europa oder irgendwo in der Welt) und zur Funktionalität in Bezug auf die Verarbeitung und Nutzung personenbezogenen Daten einschließlich der Auswertung (Echtzeitnutzung, nachlaufende Auswertung, langfristige Archivierung) bilden einen bunten Strauß an Kombinationsmöglichkeiten.

Die Masse der beim Arbeitgeber gesammelten Daten erlaubt häufig zusätzliche aussagekräftige Bewertungen durch Nutzung von Data-Mining-Technologien. Die Verarbeitung der erfassten Daten erfolgt auf der Basis von komplexen Analyseverfahren unter Einsatz von Verfahren, die unter den Stichworten „Data Warehouse“ oder „**Big Data**“ zusammengefasst werden. Dabei lassen sich unterschiedlichste Datenbestände zur Beantwortung unternehmensrelevanter Fragen zu fast beliebigen Auswertungen zusammenführen.

Der Einsatz von IKT kann mit Bezug auf Beschäftigtendaten – je nach konkreter Umsetzung und konkretem Zweck – aus Datenschutzsicht **legitim oder auch illegitim** sein. Mit dem Einsatz von globalen Systemen über weltweite Netze sowie dem Einsatz von ausländischer Hard- und Software kann ein gesteigertes Risiko von Wirtschaftsspionage und -sabotage einhergehen ebenso wie das Risiko der Ausforschung und Einflussnahme durch ausländische Geheimdienste.

Die mit dieser IKT verfolgten **Zielsetzungen** lassen sich nur schwer normativ eingrenzen und sind mit den in § 32 BDSG geforderten Zwecken der „Einstellung“ und „Erfüllung des Arbeits- bzw. Beschäftigungsvertrags“ nur sehr allgemein beschrieben. Spezifische Zwecke können sein[14]: Organisation der Produktion, der Logistik, der Finanzströme, des Personaleinsatzes, Vermeidung von Risiken für Arbeitgeber, Beschäftigte, Kunden oder Lieferanten in Bezug auf analoge und digitale Sicherheit, Gesundheit der Beschäftigten und der Kunden, Vermeidung von finanziellem Schaden, Verfolgung von Straftaten sowie von Verstößen gegen Arbeitgebervorgaben, Qualitätssicherung und Erfüllung von branchenspezifischen Vorgaben (z. B.

[14] Vgl. auch die Aufzählung in Art. 88 Abs. 1 EU-DSGVO.

Lebensmittelsicherheit), Rechenschaftslegung, soziale Auswahl, Wirtschaftlichkeitskontrolle, Ablaufoptimierung, Kunden- und Lieferservice u.s.w.

Ein Normgeber im Bereich des Beschäftigtendatenschutzes muss sich vergegenwärtigen, dass die technische Entwicklung nicht an ihrem Ende angelangt ist. Vielmehr hält der **Trend zur Digitalisierung** weiter an. In der Produktion (Industrie 4.0) wie auch bei vielen Dienstleistungen (Robotik) werden immer mehr Sensoren verwendet, deren primäre Zielsetzung zumeist die Erfassung von Sachdaten ist, durch die aber regelmäßig (nebenbei) personenbeziehbare Daten von Beschäftigten anfallen. Ein spezifisches Problem besteht bei Anwendungen, bei denen keine klare Trennung zwischen privater und dienstlicher Datenverarbeitung stattfindet. Diese Verwischung wird teilweise von Beschäftigten im Interesse persönlichen Komforts (Bring your own Device – BYOD) explizit gefordert. Teilweise, etwa bei Bereitschafts- oder Servicedienstleistungen, die von heimischen Arbeitsplätzen aus erbracht werden, ist eine technische Trennung von Privatem und Dienstlichem im Rahmen von Beschäftigungsverhältnissen nur schwer möglich – meist kostet sie das Unternehmen Geld, das gerne gespart wird. Eine besondere Qualität besteht bei der Integration von Biotechnik in informationstechnische Verfahren, wie sie im Bereich des Arbeitsschutzes und der Gesundheitsprävention nötig sein kann. Zur Erweiterung der menschlichen Wahrnehmung bei Betriebsabläufen können Techniken der Augmented Reality (z. B. Brillen mit wahrnehmungserweiternder Video- und Tonerfassung und -auswertung sowie mit Bild- und Tonausgabe) zum Einsatz kommen. Hinsichtlich der Mensch-Maschine-Schnittstellen sind Weiterentwicklungen auch im Beschäftigtenbereich denkbar (Stichwort „Cyborgs“).

6 Auswirkungen auf das Beschäftigungsverhältnis und die Beschäftigten

Je komplexer die verwendeten Verfahren sind, desto höher ist der **Verlust an Transparenz und digitaler Souveränität**. Dies gilt in jedem Fall für die Beschäftigten und die Beschäftigtenvertretungen, in vielen Fällen aber auch für die IKT-Verantwortlichen im Betrieb und letztlich für den Arbeitgeber selbst. Unternehmen, die etwa bei Cloud- oder Software-Angeboten regelmäßig „Rundum-Sorglos-Pakete“ einkaufen, kennen in aller Regel weder deren volle Funktionalität noch die Konfigurationsmöglichkeiten. Der Transparenzverlust kann sogar den Anbieter eines IKT-Produktes treffen, etwa wenn das Produkt sich über selbstlernende Mechanismen weiterentwickelt und diese Systemveränderungen nicht hinreichend dokumentiert und nachvollzogen werden (können).

Bei KMUs und kleineren deutschen Niederlassungen ausländischer Großunternehmen besteht der Trend, die Kapazitäten der **eigenen IKT-Abteilung** so weit abzubauen, dass eine fast vollständige Abhängigkeit von IKT-Dienstleistern oder vom Mutterkonzern entsteht. Dies führt in der Regel dazu, dass im eigenen Unternehmen kaum noch Kenntnisse über die Art und den Umfang der Verarbeitung personenbezogener Daten vorhanden sind. In einem solchen Umfeld nach den Inhalten der Systemprotokollierung einer Anwendung zu fragen, ist meist hoffnungslos.

Die Risiken für die Beschäftigten beschränken sich aufgrund der geschilderten Situation nicht auf die klassische Beeinträchtigung der Privatsphäre, also der Intim- und Familiensphäre sowie des sozialen Umgangs. Vielmehr kann die Beschäftigtenüberwachung wegen der ubiquitären Unternehmenssysteme sämtliche Lebenslagen und **sämtliche persönlichen Bereiche** und damit sämtliche

Grundrechte der Beschäftigten erfassen, z. B. die Rechte auf Gesundheit, Mobilität, Konsum, Freizeitverhalten, Meinungsäußerung, politische, gewerkschaftliche und religiöse Betätigung. Netzspezifisch besonders gravierend ist das öffentliche digitale Anprangern und Diskreditieren mit oft schweren negativen seelischen, körperlichen, familiären, sozialen und beruflichen Folgen.

Merkmalsbezogene Selektionen durch den Arbeitgeber können bei der Einstellung, der Beurteilung der Arbeitsleistung, beim Arbeitseinsatz (zeitlich, räumlich, in Bezug auf spezifische Tätigkeiten), bei der Bezahlung und bei der Entlassung eine Rolle spielen. Dabei kommen teilweise sog. Scoring- und Ratingverfahren zum Einsatz, bei denen die individuelle persönliche Bewertung von Vorgesetzten durch eine Computerbewertung ersetzt oder zumindest unterstützt wird. Mit Hilfe von Tracking-Werkzeugen werden individuelle Aktivitäten, Fähigkeiten und Vorlieben ermittelt und bewertet, was zur Förderung wie auch zur Disziplinierung und zur Manipulation der Betroffenen verwendet werden kann. Selbst umfassende Persönlichkeitsprofile können erstellt werden.

Der Einsatz von IKT durch den Arbeitgeber muss nicht auf eine individuelle Wirkung gegenüber den Beschäftigten abzielen. IKT kann auch zur Überwachung und Kontrolle von **Arbeitskollektiven** eingesetzt werden. Dem dienen z. B. unternehmensinterne wie auch öffentliche Systeme der Bewertung und des Benchmarkings. Dadurch können die oben beschriebenen Effekte für Einzelpersonen gegenüber einer gesamten Gruppe ausgelöst werden mit aus Arbeitnehmersicht problematischen oder schädlichen Prozessen und Wirkungen (z. B. Mobbing, sozialer Druck, Konkurrenzkampf, Entsolidarisierung). Benchmarking zielt häufig darauf ab, dass sich der Einzelne am rechnerischen Durchschnitt einer Gruppe orientiert. Die ausgelösten Leistungssteigerungen heben wiederum den Durchschnittswert der Bezugsgruppe und lösen ein Kreislauf aus, der immer höhere Leistung abfordert und immer stärkeren Druck aufbaut.

Das bestehende **strukturelle Machtgefälle** zwischen Arbeitgeber und Arbeitnehmer wird durch den Einsatz von IKT regelmäßig massiv verstärkt. Die Auswahl der IKT erfolgt durch den Arbeitgeber. Die Arbeitnehmer können hierauf nur begrenzt über Mitbestimmungsregelungen modifizierend Einfluss nehmen. Wegen dieser Bestimmungsmacht des Arbeitgebers, die sich in der Nutzung der IKT fortsetzt, vertieft sich die Abhängigkeit der Arbeitnehmer.

Faktisch wird diese strukturelle Abhängigkeit überlagert durch eine möglicherweise sehr weitgehende Abhängigkeit des Arbeitgebers von **IKT-Anbietern**. Technikbedingt besteht eine Abhängigkeit der Geschäftsführung des Unternehmens von der eigenen IKT-Abteilung oder, in vielen Fällen, von der IKT-Abteilung einer Konzernmutter oder -schwester. Diese Abhängigkeit lässt sich durch Personal- und Investitionsentscheidungen sowie durch Weisungen und Kontrollen reduzieren bzw. kompensieren. Dies gilt aber nicht mehr, soweit – was aus Kostengründen immer weiter um sich greift – (zumeist standardisierte) Hard- und Software externer Anbieter zum Einsatz kommt oder die IKT-Abteilung gar nicht „im eigenen Hause“ sitzt. Faktisch hat dann der Arbeitgeber/Unternehmer manchmal nur die Möglichkeit, ein Produkt zu nutzen oder dies bleiben zu lassen. Ist er von anderen Konzernunternehmen abhängig, bleibt ihm meist noch nicht einmal diese Möglichkeit. Um nicht vor vollendete Tatsachen gestellt zu werden, ist die Beschäftigtenvertretung schon heute zumindest berechtigt, mittels der Mitbestimmung bei Systemen, die nach § 87 Abs. 1

Nr. 6 BetrVG der Mitbestimmung unterliegen, auf die Auswahl der IKT-Anbieter und die Bedingungen des Produkteinsatzes einzuwirken (s. u. 7).

7 Nationaler rechtlicher Rahmen

Der derzeit bestehende nationale Regelungsrahmen wird insbesondere durch das **Bundesdatenschutzgesetz** (BDSG) gesetzt, das auf öffentliche Stellen des Bundes sowie auf nicht-öffentliche Stellen, also auf die gesamte Privatwirtschaft, anwendbar ist. Dies gilt neben den materiell-rechtlichen Regelungen und den Betroffenenrechten (dazu weiter unten) für den technisch-organisatorischen Datenschutz (§ 9 BDSG) sowie für die organisatorischen Anforderungen (§§ 4d ff. BDSG), einschließlich der Normierung des betrieblichen Datenschutzbeauftragten (§§ 4g f. BDSG). In den letztgenannten Bereichen bestehen in Bezug auf das Beschäftigungsverhältnis nur begrenzt besondere Regelungsbedarfe, weshalb die allgemeinen Regeln im BDSG und künftig in der EU-DSGVO gelten können und sollten. Der teilweise von Gesetzgeber begangene Weg einer spezifischen Vollregelung (z. B. im Bereich der Sozialgesetzbücher – SGB) hat sich nicht bewährt. Die Regelungen des BDSG werden – voraussichtlich mit Wirkung ab 2018 – durch die EU-DSGVO abgelöst, wobei jedoch vom allgemeinen Regelungskonzept der EG-DSRl bzw. des BDSG nicht wesentlich abgewichen wird. Die nachstehenden Überlegungen gelten also auch, nachdem die EU-DSGVO das BDSG abgelöst haben wird.

Neben dem allgemeinen Datenschutzrecht haben technik- und zweckspezifische gesetzliche Datenschutzregelungen beschäftigungsrechtliche Relevanz. Dies gilt insbesondere für das **Telekommunikations- und das Telemediengesetz** (TKG, TMG), die anwendbar sind, wenn dienstlich von Beschäftigten genutzte Angebote des Arbeitgebers auch für private Zwecke verwendet werden. Da die Regelungsinhalte des TKG und des TMG jedoch nicht auf die Anwendung in Beschäftigungsverhältnissen angelegt sind, werden sie den dort bestehenden Interessenlagen oft nicht gerecht.[15]

Für die Beschäftigten bestehen nach deutschem bzw. europäischem Datenschutzrecht die **Betroffenenrechte** (Auskunft, Berichtigung, Sperrung, Löschung, Widerspruch, Anrufung einer Beschwerdestelle, Schadenersatz, Rechtsschutz) im gleichen Umfang, nach den gleichen Maßstäben und nach denselben Verfahren wie in anderen Rollen, etwa als Verbraucher oder im Verhältnis Staat-Bürger (§§ 19 ff., 33 ff. BDSG). Als Gegenrechte können die Arbeitgeber neben ihrem Direktionsrecht möglicherweise Betriebs- und Geschäftsgeheimnisse geltend machen.

Bestehen Gesetze für Beschäftigte zu **spezifischen Zwecken**, wie etwa der sozialen Absicherung (SGB) oder der Arbeitssicherheit (ASiG), so ergeben sich hieraus keine grundsätzlichen Modernisierungsprobleme, weshalb auf diese Rechtsbereiche hier nicht weiter eingegangen wird. Gemäß Art. 9 Abs. 2 lit. b EU-DSGVO besteht insofern auch nur ein begrenzter Anpassungsbedarf.

Neben dem Datenschutzrecht gilt für beschäftigungsspezifische Fragen das allgemeine und das besondere **individuelle und kollektive Arbeitsrecht**. Das

[15] Deshalb wurde zur Verbesserung der Rechtssicherheit im Januar 2016 eine „Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ veröffentlicht, https://www.datenschutz-mv.de/datenschutz/publikationen/informat/internet/oh-internet-arbeitsplatz.pdf.

Betriebsverfassungsgesetz (BetrVG) und personalvertretungsrechtliche Regelungen zielten ursprünglich nicht auf die Sicherung des Datenschutzes der Beschäftigten sondern u. a. auf die generelle Sicherung des allgemeinen Persönlichkeitsrechtes. Inzwischen haben diese Regelungen eine zentrale Relevanz für die Gewährleistung des Persönlichkeitsrechts der Beschäftigten beim IKT-Einsatz erlangt. Betriebsvereinbarungen sind insofern zum zentralen Instrument für die konkrete Garantie von Beschäftigtenrechten im Betrieb geworden. Über sie wird die Abwägungsentscheidung, die nach § 32 bzw. § 28 BDSG vorgenommen werden muss, getroffen. D. h. die prozeduralen Regelungen des Mitbestimmungsrechts sind zentrale Gewährleistungsinstrumente für die materiellen Beschäftigtenrechte beim IKT-Einsatz. Missachtet der Arbeitgeber beim IKT-Einsatz die Anforderungen des Mitbestimmungsrechts, so führt dies regelmäßig dazu, dass die Erhebung und Verarbeitung von Beschäftigtendaten auch aus Datenschutzsicht materiell-rechtlich unzulässig wird.

Das BDSG legitimiert Datenverarbeitung der verantwortlichen Stelle insbesondere auf vertraglicher Grundlage, evtl. nach **Abwägung** berechtigter Verarbeiterinteressen gegen schutzwürdige Betroffeneninteressen sowie durch explizite Einwilligung (§ 28 BDSG). Dies gilt auch für das Arbeitsverhältnis. Mit § 32 besteht im BDSG seit 2009 eine einzige arbeitsrechtsspezifische Sonderregelung, die auf den Beschäftigungsvertrag Bezug nimmt.

Von Arbeitnehmerseite wird immer wieder in Frage gestellt, ob vom Arbeitgeber abverlangte **Einwilligungen** zur Datenverarbeitung die nach § 4a BDSG die erforderliche Freiwilligkeit aufweisen. Das BAG hat kürzlich geurteilt, dass auch in dieser Abhängigkeitsbeziehung Einwilligungen datenschutzrechtlich grundsätzlich wirksam sein können.[16] Allerdings ist zu beachten, dass Einwilligungen, selbst wenn sie freiwillig erteilt werden, bestehende Mitbestimmungsrechte nicht ersetzen können. Unabhängig von der Zustimmung Beschäftigter muss das zuständige Gremium der Beschäftigtenvertretung bestehendes Mitbestimmungsrecht ausüben.

Generell gilt der **Verhältnismäßigkeitsgrundsatz**, wonach eine personenbezogene Datenverarbeitung für die Zwecke des Arbeitsvertrags bzw. des Arbeitgebers geeignet, erforderlich und angemessen sein muss. Angesichts der Vielfalt der Anwendungsbereiche und der Zwecke der eingesetzten IKT (s. o. 5) können auf abstrakt-gesetzlicher Ebene nur begrenzt materiell-rechtliche Festlegungen hinsichtlich der Abwägung zwischen Arbeitgeber- und Beschäftigteninteressen vorgenommen werden. Insbesondere ist kaum zu verhindern, dass der Arbeitgeber allein durch Wahl seines **Geschäftsmodells** die damit verbundenen erforderlichen Datenverarbeitungen festlegt. Die unternehmerische Tätigkeit entzieht sich dem Einfluss des Beschäftigten und ist auch der Mitbestimmung durch Betriebsräte nicht zugänglich. Dies hat zur Folge, dass der Arbeitgeber letztlich eine große Gestaltungsmöglichkeit bei der Festlegung hat, welche Datenerhebungen und -verarbeitungen „erforderlich“ sind.

Für eine Vielzahl von Zwecken bedarf es fachlich gesehen keiner personenbeziehbaren Daten, sondern es genügen anonymisierte, oft sogar aggregierte Daten. Dies gilt z. B. für viele Zwecke der Planung, der Qualitätssicherung oder der Wirtschaftlichkeitskontrolle. Ist nicht zu vermeiden, dass mit (reidentifizierbaren) Datensätzen gearbeitet wird, so kann zur Umsetzung des Gebots

[16] BAG, U. v. 11.12.2014, 8 AZR 1010/12.

der **Datensparsamkeit** mit pseudonymen und evtl. mit merkmalsaggregierten Daten gearbeitet werden. In solchen Fällen müssen die Voraussetzungen für zulässige Reidentifizierungen verbindlich festgeschrieben werden. Wird das Ziel einer Verdachtskonkretisierung (z. B. bei Fraud oder Loss Prevention) verfolgt, so ist regelmäßig nur ein gestuftes Vorgehen verhältnismäßig, bei dem Verdächte auf der Grundlage von Gruppendaten konkretisiert werden müssen, bevor eine direkte personalisierte Beobachtung und Auswertung erfolgt. Das innerbetriebliche Verfahren muss zudem Grenzen vorsehen, ab wann spätestens Ermittlungen an staatliche Ermittlungsbehörden abgegeben werden.

Als **absolute Tabuzone** gilt der Kernbereich persönlicher Lebensgestaltung. Weiterhin besteht ein Verbot der Totalüberwachung am Arbeitsplatz; d. h. es muss überwachungsfreie Zeiten und Zonen geben. Damit korrespondiert ein Verbot vollständiger Persönlichkeitsbilder, wobei jedoch eine klare Grenzziehung schwer möglich ist, weil eine exakte, unumstrittene Definition der Begriffe „Persönlichkeitsprofil“ und „Persönlichkeitsbild“ nicht existiert. Bei der innerbetrieblichen Erörterung des Umgangs mit Videoüberwachungsanlagen stellt sich regelmäßig die Frage, wieviel „unbeobachtete Zeit“ einem Beschäftigten (prozentual?) zugestanden werden muss und wie überwachungsfreie Zonen in der Praxis zu gestalten sind.

Generell wie spezifisch im Arbeitsverhältnis gilt der Grundsatz, dass personenbezogene Daten nur mit **Kenntnis des Betroffenen** erhoben, verarbeitet und genutzt werden dürfen. Soll von diesem Grundsatz abgewichen werden, so ist dies begründungspflichtig und unterliegt auch im Hinblick auf die Geheimhaltung einer Verhältnismäßigkeitsprüfung.

Eine besondere **Pflicht zur Begründung** und eine Pflicht zu einer strengeren Verhältnismäßigkeitsprüfung bestehen generell im Arbeitsverhältnis bei der Verarbeitung von

- besonderen Arten personenbezogener Daten (politische u. a. Anschauungen, Gesundheit, Sexualität, § 3 Abs. 9 BDSG, künftig Art. 9 Abs. 1 EU-DSGVO),
- besonderen Berufsgeheimnissen (§ 203 Abs. 1, 3 StGB), insbes. der ärztlichen Schweigepflicht.
- Im Speziellen bestehen derartige Begründungspflichten beispielsweise bei
- der Einholung von Einwilligungen,
- der Verarbeitung nicht-arbeitsplatzbezogener Daten (z. B. Internet, Auskunfteien)
- dem Umgang mit betriebsärztlichen Daten.

Die prozeduralen und materiell-rechtlichen Anforderungen an die Datenverarbeitung beim **Whistleblowing** sind derzeit weder allgemein noch arbeitsplatzbezogen gesetzlich geregelt. Dies führt insbesondere in Beschäftigungsverhältnissen immer wieder zu Konflikten, die gemäß der bestehenden Rechtslage nicht befriedigend und nicht im Interesse des einen Ethik- oder Rechtsverstoß aufdeckenden Beschäftigten gelöst werden können.

Generell kann gesagt werden, dass reine **materiell-rechtliche gesetzliche Regelungen**, also Normen mit einem Ge- oder Verbotsinhalt, im Beschäftigtenbereich oft wenig geeignet sind, bestimmte praxisrelevante, im Beschäftigungsbereich auftretende automatisierte Verarbeitungen und Sonderfälle abzudecken. Auf der

anderen Seite belassen sie mangels Konkretheit dem Arbeitgeber oft einen übermäßigen Beurteilungsspielraum. Von der unter 5 dieses Gutachtens geforderten Orientierung rechtlicher Regelungen an dem, was heute in Unternehmen realisiert wird, sind wir weit entfernt.

8 Normative Grundsatzerwägungen

Die dargestellten Umstände und der bestehende rechtliche Rahmen führen bei Unternehmens-Juristinnen und -Juristen immer wieder zu der Forderung, das geltende **Verbot mit Erlaubnisvorbehalt** hinsichtlich der personenbezogenen Datenverarbeitung im Bereich der Wirtschaft zu beseitigen. Nur so könnten die gewaltigen ökonomischen und sonstigen Potenziale des Einsatzes von Big-Data-Technologie realisiert werden. Auch wenn dies gelegentlich geleugnet wird, geht es den Vertretern dieser Ansicht um nichts anderes als die Etablierung eines in den USA und in vielen sonstigen Teilen der Welt herrschenden Silicon-Valley-Kapitalismus des „Everything goes“. Tatsächlich sorgen die fehlenden rechtlichen Restriktionen in den USA dafür, dass die dortige Unternehmen Erfolge bei der Maximierung von Profit und Kapital feiern können, die für europäische Unternehmen nicht möglich sind.[17] Diese Effekte lassen sich aber nur erreichen, indem sowohl die Kunden- als auch die Arbeitnehmerschaft einer beispiellosen informationellen Ausbeutung ausgesetzt werden. Soziale und freiheitliche Aspekte spielen regelmäßig keine oder nur eine untergeordnete Rolle.

Aus einer grundrechtlichen Sicht kann und darf dieser Weg nicht begangen werden. Eingriffe in das Grundrecht auf informationelle Selbstbestimmung haben ein hohes **Potenzial der Freiheitsbeschränkung**. Dies gilt generell in technisierten Informationsgesellschaften, insbesondere aber, wenn erkenntnis- und profitträchtige Instrumente der Big-Data-Technologie eingesetzt werden. Die Rechtsprechung des BVerfG und des EuGH sowie die Bestätigung durch die EU-DSGVO (Art. 6 Abs. 1) dürften eine hinreichende Sicherheit vor den Träumen der angesprochenen Wirtschaftsjuristen darstellen.

Dies ändert nichts am Problem, dass sich moderne IKT allein mit spezialgesetzlichen Ge- und Verboten nicht mehr lenken lässt. Der nach dem Volkszählungsurteil des BVerfG zunächst lange verfolgte Kurs der spezialgesetzlichen Konkretisierung zulässiger personenbezogener Datenverarbeitung ist an seine Grenzen gestoßen. In vielen öffentlichen, aber erst recht in nicht-öffentlichen Bereichen lassen sich Datenfelder, Datenarten, Verarbeitungsformen und verarbeitende Stellen nicht mehr ausdrücklich in Parlamentsgesetzen benennen. Selbst die eindeutige Beschreibung von Zweckbestimmungen ist oft, nicht nur bei zweckfreien Internetveröffentlichungen, unmöglich. Schon bald nach dem Volkszählungsurteil von 1983 wurde das Risiko der **Verrechtlichungsfalle** erkannt, also des Erlasses von zu spezifisch formulierten Gesetzen, die wegen ihres Regelungsinhaltes einerseits technische Entwicklungen nicht berücksichtigen und so ihren Regelungszweck verfehlten, andererseits im Falle ihrer Einhaltung den Einsatz sinnvoller technischer Entwicklungen torpedierten und technische Entwicklungen nicht berücksichtigten.

[17] Siehe hierzu die Dokumente des Netzwerks Datenschutzexpertise unter http://www.netzwerk-datenschutzexpertise.de/big-data.

Die Falle dieses Normierungsmodells wurde übrigens bereits vor vielen Jahren in Kreisen der **Beschäftigtenvertretungen** erkannt und diskutiert, als Betriebsvereinbarungen über die bis dahin üblichen Positivkataloge angesicht von ERP-Systemen wie SAP schlichtweg nicht mehr handhabbar waren. Seitdem implementieren und erforschen fortschrittliche Beschäftigtenvertretungen verschiedenste Modelle in Betriebsvereinbarungen, um IKT-Systeme wirksam zu vereinbaren, ohne in ordnerfüllenden Anlagen zu Datenfeldbeschreibungen zu ersticken. Der Gesetzgeber hinkt an dieser Stelle eindeutig betrieblichen Interessensvertretungen hinterher.

Die **Vorschläge der 17. Legislaturperiode** für eine Novelle des Beschäftigtendatenschutzrechtes tappten mehr oder weniger in die besagte Verrechtlichungsfalle. Dies gilt insbesondere für den Regierungsvorschlag, der versuchte, möglichst sämtliche denkbaren Eventualitäten zu regeln. Letztendlich landeten diese Normierungsversuche im immer gleichen Erfordernis einer Interessenabwägung. Dabei mussten die Abwägungsregeln derart offen bleiben, dass bei einer extensiven Anwendung die Arbeitgeber in unverantwortlicher Weise ein einzigartiges Überwachungsinstrumentarium hätten durchsetzen können.

Dem Bestimmtheitserfordernis und der Wesentlichkeitstheorie des BVerfG kann bei Grundrechtseingriffen auch dadurch genügt werden, dass anstelle einer präzisen gesetzlichen Benennung von Datenarten, Verarbeitungsformen, Stellen und Zwecken offenere Formulierungen verwendet werden und **rechtliche Kompensationen** – evtl. erst nach Beginn einer einmal begonnenen Datenverarbeitung – vorgesehen werden. Diese können in technisch-organisatorischen Sicherungen, in prozeduralen Vorkehrungen sowie in (auch materiell-rechtlichen) untergesetzlichen Normen liegen. Selbstverständlich dürfen mit diesen Regeln die bestehenden Grundrechtsgarantien nicht abgebaut werden. Doch besteht so die Chance von adäquaten Interessen- und Grundrechtsabwägungen unter Wahrung der nötigen Flexibilität, die eine starre gesetzliche Regelung nicht bieten kann. Außerdem lässt sich so die Schwierigkeit umgehen, vor Einsatz einer IKT-Anwendung bereits abschließend die Zulässigkeit sämtlicher Verarbeitungsschritte klären und abwägen zu müssen – und das, obwohl die Einführung großer System sich oft über Monate hinzieht, während derer die Umstände der Verarbeitung erste erprobt und entwickelt werden. Auch ist selbst nach der Produktivsetzung in aller Regel kein Endzustand erreicht, sondern die Systeme werden laufend den aktuellen Bedürfnissen angepasst. Ohne eine prozedural verankerte begleitende Datenschutzprüfung werden die meisten Systeme bereits kurze Zeit nach Abgabe der ersten Zulässigkeitsprüfung nicht mehr in dem damals untersuchten Zustand betrieben.

Über die notwendige **Grundrechtssicherung durch Verfahren, Organisation und Technik** kann und muss erreicht werden, dass vom Gesetzgeber der wesentliche Rahmen für die informationellen Maßnahmen bestimmt wird. Dessen Konkretisierung, Präzisierung und Umsetzung im Einzelfall wird dann Stellen überlassen, bei denen höhere Sachnähe, Fachlichkeit, Aktualität und Problemlösungskompetenz, evtl. ausgelöst durch höhere Betroffenheit, bestehen. Die Festlegung der Anforderungen an die Konkretisierung und Umsetzung muss weiterhin demokratisch legitimiert sein, etwa durch die Genehmigung oder Anerkennung unabhängiger Datenschutzkontrollinstanzen. Für den Betroffenen wie auch für die Datenschutzkontrollinstanzen, also die Aufsichtsbehörden, muss in jedem Fall die

Möglichkeit bestehen bleiben, vor Gericht eine Rechtskontrolle der untergesetzlichen Regelungen vorzunehmen.[18]

Es sind vielfältige **kompensierende Vorkehrungen** möglich: die Durchführung von (evtl. regelmäßigen) Datenschutzaudits durch eine unabhängige Stelle, die Verwendung von zertifizierter oder anderweitig geprüfter Soft- und Hardware, die Einschaltung der Aufsichtsbehörde, Transparenzpflichten (beginnend mit der individuellen Information bis hin zur allgemeinen Veröffentlichung), (unabhängige) Evaluationen, die Einräumung von Widerspruchsrechten für die Beschäftigten und Beschäftigtenvertretungen, Haftungs- und sonstige Sanktionsregelungen, (Beweis-) Verwertungs- und Nutzungsverbote. Untergesetzliche. eher materiell-rechtliche Festlegungen können sein: Pseudonymisierungs- und Anonymisierungspflichten, räumliche Begrenzungen der DV, Festlegungen von Rollen- und Zugriffsregimes, präzise Zweckfestlegungen, explizite Verarbeitungsverbote als Stopplinien, Speicher- bzw. Löschfristen.

Abgesehen von einer zumindest teilweisen Auflösung des oben dargestellten Regulierungsdilemmas hat ein ergänzender **prozeduraler Schutzansatz** folgende Vorteile: Sowohl die Arbeitgeber- als als auch die Arbeitnehmerseite können einer offeneren materiellen Regelung kombiniert mit einer Verfahrensregelung eher zustimmen als einer für sie nachteiligen materiellen Regelung. Die inzwischen in das 4. Jahrzehnt gehende Regulierungsblockade kann derart möglicherweise aufgelöst werden. Die selbstverständlich zu veröffentlichenden untergesetzlichen Regelungen können zu einem Wettbewerb um die beste Regulierung führen (Best Practise). Gute und schlechte Erfahrungen können bei Fortschreibungen berücksichtigt werden. Voraussetzung ist, dass Strukturen und Verfahren gefunden und gesetzlich implementiert werden, die interessen- und problemadäquat, transparent und öffentlich, technikoffen und erfolgversprechend sind. Innerhalb einer angemessenen Zeit müssen die Beteiligten veranlasst werden, die IT-Gestaltungsvorgaben so festzulegen, dass sie den verschiedenen Interessensgruppen weitestgehend gerecht werden. Hierbei müssen Druckmittel zur Verfügung stehen, die alle Seiten dazu veranlassen, ernsthaft eine Lösung zu suchen und zu finden.

Dieser Vorgehensweise förderlich ist, dass im Bereich des Beschäftigtendatenschutzes zwei wesentliche Protagonisten vorhanden sind: **Arbeitgeber und Arbeitnehmer**. Dies ist ein Vorteil gegenüber anderen Bereichen eines personenbezogenen IKT-Einsatzes, in denen komplexe Interessengeflechte mit divergierenden Positionen bestehen, so wie dies im Gesundheitsbereich der Fall ist. Zwar gibt es weitere Interessierte in dem Konflikt. Dies sind die IKT-Industrie und der Staat. Doch deren Interessen können bei der Konfliktbewältigung nachgeordnet bleiben. Deren Interessen können durch Rahmenbedingungen des Marktes (z. B. Zertifizierungsverfahren) oder durch staatliche Regulierung (so wie dies derzeit in den SGBs oder im ASiG erfolgt) gewahrt werden.

Förderlich ist, dass in Deutschland über viele Jahrzehnte hinweg gute Erfahrungen mit der Konfliktlösung zwischen Arbeitgebern und Arbeitnehmern in Fragen der **Tarif- und Arbeitsplatzgestaltung** gesammelt werden konnten, auf die in diesem neuen Feld zurückgegriffen werden kann. Dies gilt nicht nur für die Art, sondern auch für die Instrumente der Konfliktlösung mit Tarifvereinbarungen, Betriebsvereinbarungen und Schlichtungsverfahren.

[18] So ausdrücklich EuGH, U. v. 06.10.2015, C-362/14, Rn. 64, 65 – Safe Harbor.

Förderlich ist auch, dass – bisher ohne besondere öffentliche Beachtung – die Instrumente der Verhandlung und des Abschlusses von Vereinbarungen über den **IKT-Einsatz auf betrieblicher Ebene** relativ erfolgreich zum Einsatz kommen. Diese Instrumente stoßen angesichts der technischen Entwicklung zwar immer wieder an Grenzen, insbesondere was die Qualifikation der Verhandlungsparteien und die Transparenz der Verfahren betrifft. Dies ändert aber nichts an dem Umstand, dass Betriebsvereinbarungen sich nicht nur etabliert haben, sondern dass sie das Mittel der Konfliktbewältigung und der Akzeptanzerhöhung beim IKT-Einsatz im Betrieb darstellen und im Interesse beider Seiten liegen. Es bedarf also keiner grundlegend neuen Instrumente, sondern einer Weiterentwicklung und Verbesserung eines vorhandenen Instrumentariums und der Herstellung von Waffengleichheit für die Beschäftigtenseite bzw. für Betriebsräte.

Das Instrument der Tarifvereinbarungen als Rahmen für **Regelungen zwischen der gesetzlichen und der betrieblichen Ebene** kann aber nicht Eins-zu-eins übernommen werden, da IKT-Festlegungen für sämtliche in einem Betrieb oder einem Bereich tätigen Beschäftigten wirksam werden und die Festlegungen grundrechtskonkretisierend, d. h. demokratisch legitimiert und nur eingeschränkt verhandelbar sind. Dem muss durch eine adäquate Regelungsstruktur Rechnung getragen werden.

Anders als bei klassischen Tarifkonflikten kann bzw. sollte hier auf das Instrument der Zuspitzung durch **Streik** verzichtet werden. Geht es beim Streik wegen des Arbeitsentgelts um den Grundwiderspruch zwischen Arbeit und Kapital, haben wir es beim IKT-Einsatz eher mit einem Nebenwiderspruch zu tun, bei dem Interessen nicht antagonistisch gegenüber stehen müssen, es vielmehr um eine Interessensoptimierung geht. Regelmäßig haben beide Seiten ein gemeinsames Interesse an einem qualifizierteren IKT-Einsatz. Klärungs- und einigungsbedürftig ist dennoch in jedem Fall die konkrete Gestaltung.

9 Vorschläge für ein modernes Beschäftigten-/Arbeitnehmerdatenschutzrecht

Als **Standort** für ein nationales Beschäftigtendatenschutzrecht wurde von der Bundesregierung bisher das BDSG gewählt. Dies basierte auf der Überlegung, dass eine Konkretisierung der allgemeinen BDSG-Regeln für das Arbeitsverhältnis erfolgt. Diese Annahme ist unzutreffend. Wir haben es hier mit einer Schnittmenge zu tun, die in gleichem Maße Datenschutzrecht und Arbeitsrecht ist. Die dort jeweils bestehenden allgemeinen Regelungen müssen beide vollständig anwendbar bleiben. Das BDSG wäre zudem mit einem eigenen Kapitel, so wie es der Regierungsentwurf 2010 mit den §§ 32 bis 32l vorsah, überfrachtet, was nicht zu einer erhöhten Klarheit beitrüge. Um den konkretisierenden Charakter sowohl in Bezug auf das allgemeine Datenschutzrecht als auch auf das Arbeitsrecht herauszustreichen, empfiehlt sich der Erlass eines eigenständigen Beschäftigtendatenschutzgesetzes. Eine Regelung des Beschäftigtendatenschutzes in einem das BDSG ablösenden Ausführungsgesetz zur EU-DSGVO, das ab 2018 in Kraft treten sollte, verbietet sich ebenso, weil ein solches Ausführungsgesetz nur eine ergänzende Funktion zur EU-Verordnung haben wird. Gemäß den Vorgaben des Art. 88 EU-DSGVO zum Beschäftigtendatenschutz ist eine sehr weitgehende Regelung nötig, bei der nur in bestimmten prozessualen Fragen auf die allgemeinen Regelungen der EU-DSGVO wie einem noch zu erlassenden nationalen Ausführungsgesetz zurückgegriffen werden kann und muss.

Soweit dies möglich und sinnvoll ist, sollten in diesem Gesetz zu konkreten **Fragestellungen, Anwendungen und Zwecken** gegenüber dem allgemeinen Datenschutzrecht (bisher BDSG, künftig EU-DSGVO) spezielle Festlegungen vorgenommen werden. Dabei sind sämtliche Regelungsansätze aus den Vorschlägen in der 17. Legislaturperiode auf den Prüfstand zu stellen, die z. B. zu folgenden Aspekten Aussagen enthalten: Bewerbung, Einstellung, Gesundheitsuntersuchung, Gefahrenabwehr, Strafverfolgung, Videoüberwachung, Ortung/Tracking, Biometrieverfahren, Nutzung von Telekommunikations- und Telemediendiensten (auch soziale Netzwerke) für dienstliche und für private Zwecke, Heimarbeit, Konzerndatenverarbeitung. Auf spezifische Regelungen, die keine sinnvollen und wirksamen Konkretisierungen allgemeiner Vorschriften vornehmen, ist konsequent zu verzichten.

Neu eingeführt werden sollte die Konkretisierung gesetzlicher Regelungen auf **überbetrieblicher Ebene**. Die hierbei zu treffenden Kollektivvereinbarungen können durch den deutschen Gesetzgeber nur für die Arbeitsverhältnisse in Deutschland vorgesehen werden. Im Interesse möglichst weitgehender europäischer Einheitlichkeit sollte zumindest mittelfristig auch auf europäischer Ebene ein solcher Regelungsansatz verfolgt werden. Gegenstand solcher Vereinbarungen sollte alles sein, was zu einer beschäftigungsspezifischen Präzisierung der allgemeinen gesetzlichen Regelungen führt. So kann es naheliegend sein, branchenspezifische Konkretisierungen vorzunehmen. Denkbar sind aber auch branchenübergreifende Regelungen zu bestimmten Fragestellungen, wie etwa zum Einsatz von Videotechnik oder zur digitalen Zeiterfassung.

Regulatorische Vorbilder für die überbetrieblichen Kollektivvereinbarungen können neben den Regelungen des BetrVG die **§ 38a BDSB** sowie Art. 38 EU-DSGVO sein, welche die Anerkennung von Verhaltensregeln durch eine Aufsichtsbehörde vorsehen. Anstelle von Verbänden verarbeitender Stellen sollten die Kollektivvereinbarungen in paritätisch von Arbeitgebern und Arbeitnehmern besetzten Gremien erarbeitet werden, die neu zu schaffen wären. Auf der Beschäftigtenseite kommt dabei den Gewerkschaften eine wichtige Funktion zu.

Druckmittel zur Veranlassung von Verhandlungen und Vereinbarungen können gesetzlich geregelte, aufschiebende Vetos sein. Geregelt werden kann auch, dass anlässlich eines konkreten Konfliktes die Pflicht auferlegt wird, eine externe, zu veröffentlichende Expertise einzuholen. Möglich ist die Regelung der Pflicht, eine Aufsichtsbehörde oder einen sonstigen unabhängigen Moderator mit besonderer fachlicher Qualifikation als Schlichter hinzuziehen. Vorbildfunktion könnte das Modell der Einigungsstelle gemäß § 76 BetrVG haben. Initiator für das Verhandeln von Vereinbarungen könnte der unten erwähnte Datenschutzbeirat sein (s. u. 10). Indirekt als Auslöser für Verhandlungen und Vereinbarungen können Medienberichte und Gerichtsurteile wirken.

Die gegenüber dem nationalen Gesetz oder der EU-DSGVO zu konkretisierenden **Regelungsgegenstände** können alles im Beschäftigtendatenschutzrecht erfassen: das materielle Recht ebenso wie die Verpflichtung zu prozeduralen oder technisch-organisatorischen Vorkehrungen. Es sollte darauf geachtet werden, dass diese Regelungen so konkret wie möglich und so offen wie nötig sind. Ziel sollte eine größtmögliche Rechtssicherheit sein, ohne zugleich die sinnvollen Entwicklungsmöglichkeiten der IKT zu beschneiden.

Parallel dazu sollte die Regelung zur **Mitbestimmung auf betrieblicher Ebene** präzisiert werden. Derzeit sieht z. B. § 87 Abs. 1 Nr. 6 BetrVG bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten und die Leistung der Arbeitnehmer zu überwachen," eine Mitbestimmungspflicht nicht nur bei einer gezielten Arbeitnehmerüberwachung vor, sondern schon, wenn eine technische Einrichtung Verhaltens- und Leistungskontrollen ermöglicht.[19] Weitere Mitbestimmungstatbestände mit Bezug zur IKT finden sich in § 87 Abs. 1 Nr. 7 (Gesundheitsschutz) und § 94 BetrVG (Personalfragebögen).

Soweit auf nationaler oder europäischer Ebene eine datenschutzrechtliche **Zertifizierung** von IKT-Produkten und -verfahren vorgesehen ist, so die Art. 42, 43 EU-DSGVO, sollte ihre Aufnahme in Kollektivvereinbarungen gefördert werden, verbunden mit einer Privilegierung von zertifizierten Produkten im Rahmen der Einigungsverfahren auf überbetrieblicher wie auf Betriebsebene (vgl. jetzt schon § 9a BDSG).

Einer Schnittstellenregelung bedarf es auch in Bezug auf **Verhaltensregeln**, die durch die Datenschutzaufsicht genehmigt werden können (§ 38a BDSG, Art. 27 EG-DSRl, künftig Art. 40, 41 EU-DSGVO). Diese kann z. B. darin bestehen, dass die Arbeitnehmerseite in den Genehmigungsprozess der Verhaltensregeln einbezogen wird.

Unabhängig von den oben genannten Klagemöglichkeiten im Rahmen überbetrieblicher und betrieblicher Konflikte sollte auf betrieblicher Ebene für die Beschäftigtenvertretung ein arbeitsrechtliches **Klagerecht gegen die Einführung datenschutzrechtlich unzulässiger IKT-Verfahren** vorgesehen werden. Dies wäre eine sinnvolle normen- und verfahrenskontrollierende Ergänzung zu Art. 76 EU-DSGVO, der u. a. vorsieht, dass in individualrechtlichen Datenschutzkonflikten Betriebsräte oder Gewerkschaften in Vertretung der Betroffenen datenschutzrechtliche Gerichtsverfahren durchführen können. Offen ist, ob es zusätzlich zu der gerichtlichen Entscheidung über Streitigkeiten im Rahmen von überbetrieblichen Vereinbarungen für Gewerkschaften einer Art Verbandsklagerecht bedarf. Mit einem solchen Klagerecht könnte auf Seiten der Arbeitgeber die Bereitschaft gesteigert werden, den Abschluss von Vereinbarungen zu suchen.

Die Regelung des § 8 Abs. 3 BetrVG, wonach der Betriebsrat „bei der Durchführung seiner Aufgaben nach näherer Vereinbarung mit dem Arbeitgeber **Sachverständige** hinzuziehen (kann), soweit dies zur ordnungsgemäßen Erfüllung seiner Aufgaben erforderlich ist", sollte im Hinblick auf die datenschutztechnische und -rechtliche Bewertung präzisiert werden.

Die Rolle der **Datenschutzaufsichtsbehörden** (heute § 38 BDSG, künftig Art. 51 ff. EU-DSGVO) sollte bereichsspezifischer ausgestaltet werden. Es ist vorstellbar, dass diesen als neutralen Stellen eine Mediatorenfunktion zwischen Arbeitgebern und Arbeitnehmern zugewiesen wird. Das bestehende Recht des Betriebsrats, die Aufsichtsbehörde einzuschalten, ohne sich Illoyalität vorwerfen lassen zu müssen, sollte explizit normiert werden. Die Aufsichtsbehörden benötigen für derartige Fragen das Personal und die sonstigen Ressourcen, um innerhalb kürzester Zeit sprech- und antwortfähig sein.

[19] BAG B. v. 09.09.1975, 1 ABR 20/74, NJW 1975, 261.

Hinsichtlich der Bestellung und Abberufung von **betrieblichen Datenschutzbeauftragten** sollte der Beschäftigtenvertretung ein Mitbestimmungsrecht eingeräumt werden.

Materiell-rechtlich sollte sich das Beschäftigtendatenschutzrecht auf Aspekte beschränken, in denen ein wesentlicher zusätzlicher Regelungsgehalt zu den allgemeinen Vorschriften erforderlich und möglich ist. Dies gilt u. a. für folgende Themen:

- zusätzliche Freiwilligkeitsanforderungen bei Einwilligungen,
- Benennung der Fälle, in denen eine Einwilligung als Rechtsgrundlage für die Datenerhebung, -verarbeitung und -nutzung ausgeschlossen wird,
- Ausnahmeregelung von einer grundsätzlichen Verpflichtung zur Trennung zwischen privater und dienstlicher DV,
- die Regelung der privaten Nutzung von dienstlichen Telekommunikationseinrichtungen,
- Nutzungsverbote von Kundendaten von Mitarbeitenden für Personalzwecke
- Verbot von Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten durch den Arbeitgeber, die aus betriebsärztlichen Untersuchungen stammen.

Hinsichtlich der Abklärung von **Verstößen von Beschäftigten** gegen arbeitsrechtliche Pflichten sollte ein gestuftes Verfahren vorgesehen werden, bei dem bei Fehlen eines individuellen Verdachtes zur Verdachtskonkretisierung zunächst mit Pseudonymen und Gruppenaggregaten gearbeitet werden muss.

Erwogen werden sollte, inwieweit eine Regelung zur **Benutzung von Beschäftigten-Pseudonymen** in der Außenkommunikation von Beschäftigten möglich und sinnvoll ist.

Zum Recht über die **Personalakte** sollte klargestellt werden, welchen Inhalt eine Personalakte haben darf, welche Aufbewahrungsfristen gelten, wer Zugriff darauf hat, unter welchen Voraussetzungen Aktenbestandteile (über wahre, nachteilige Umstände) zu löschen sind, und welche Anforderungen an die digitale Aktenführung zu stellen sind.

Zum **Whistleblowing** bedarf es nach dem Urteil des Europäischen Gerichtshofes für Menschenrechte vom 21.07.2011[20] einer spezifischen Regelung. Dabei kann auf eine Vielzahl von schon vorhandenen Vorschlägen zurückgegriffen werden.[21]

Aus Sicht der Arbeitnehmer kann eine Regelung, welche im Beschäftigtenbereich eine **Konzernprivilegierung** vorsieht, die an die EU-DSGVO anknüpfen kann (Art. 4 Nr. 19) vorteilhaft und sinnvoll sein, wenn die Öffnung von Beschäftigtendaten gegenüber mehreren verantwortlichen Stellen im Konzern durch Sicherungen kompensiert wird und klare Verantwortlichkeiten festgelegt werden.

[20] EGMR U. v. 21.07.2011 – Heinisch/Deutschland, NJW 2011, 3501.

[21] Z. B. Gesetzentwürfe der SPD-Fraktion v. 07.02.2012, BT-Drs. 17/8567 der Fraktion Bündnis 90/Die Grünen v. 04.11.2014, BT-Drs. 17/9782.

10 Sonstige politisch bestimmbare Rahmenbedingungen

Eine adäquate Gesetzgebung ist die Grundlage für eine Verbesserung des Datenschutzes in einer sich immer mehr digitalisierenden Arbeitswelt. Das Heil des Persönlichkeitsschutzes für Beschäftigte kann nicht ausschließlich in der Gesetzgebung liegen. Vielmehr müssen in den Betrieben, Branchenverbänden, Gewerkschaften, Beschäftigtenvertretungen, Aufsichtsbehörden und bei den Anbietern von IKT-Lösungen Konzepte für einen datenschutzkonformen IKT-Einsatz am Arbeitsplatz erforscht, diskutiert, entwickelt und implementiert werden. Hierfür kann als Instrument der politischen Planung die Einrichtung eines **Datenschutzbeirats im Bundesarbeitsministerium** sinnvoll sein. Dieser kann Vorschläge für überbetriebliche Vereinbarungen machen oder diese gar verbindlich initiieren.

Bisher erfolgen öffentlich geförderte **Forschungs- und Entwicklungsanstrengungen** im Bereich des Datenschutzes zumeist jenseits des betrieblichen Anwendungsfeldes. Dies muss sich angesichts der neuen Herausforderungen durch Anwendungen in den Bereichen Industrie 4.0 und Big Data ändern. Bisher laufen Forschungs- und Entwicklungsarbeiten auf Initiative von IKT-Anbietern und Arbeitgebern insbesondere darauf hinaus, die Beschäftigtenüberwachung zu perfektionieren. Dem sind Anstrengungen für ein Mehr an Persönlichkeitsschutz entgegenzusetzen, die staatlich gefördert werden.

11 Schlussbemerkungen

IKT hat große **positive Auswirkungen** auf die Arbeitswelt. Sie führt zu Produktivitätssteigerungen und kann, sinnvoll eingesetzt, dazu beitragen, den Arbeitnehmerinnen und Arbeitnehmern ihre Tätigkeit zu erleichtern, sie zu qualifizieren und ihren Arbeitsplatz zu sichern. Der Einsatz von IKT kann zu einer erhöhten Zufriedenheit bei den Beschäftigten führen, etwa, wenn Kreativität gefördert wird, die Arbeitsleistungen besser sichtbar werden oder spielerische und Team-Elemente bei der Arbeit einfließen. Arbeitnehmervertretungen sollten deshalb die Einführung derartiger Systeme grundsätzlich fördern und fordern.

Es sollte jedoch allen Seiten, auch den Arbeitnehmervertretungen und den Beschäftigten, vermittelt werden, dass die Attraktivität von IKT-Systemen eine persönlichkeitsgefährdende Kehrseite hat. Arbeitgeber betonen gerne die mit IKT verbundenen Verbesserungen für ihre Beschäftigten, verschweigen jedoch die damit verbundenen zusätzlichen Überwachungs- und Kontrollmöglichkeiten. Diese Möglichkeiten sind jedoch oft der eigentliche Grund für die Einführung bestimmter Systeme. Ein solcher Einsatz führt zu einer schleichenden Entmündigung der Betroffenen. Diese ist nicht nur persönlich eine Gefahr für die Betroffenen, sondern auch für jede demokratische Gesellschaft, deren Grundlage mündige, **meinungsfreudige und kreative Menschen** sind. Der Persönlichkeitsschutz von Beschäftigten sollte daher letztlich das ureigene Interesse der Unternehmensleitungen sein. In einem Klima der Überwachung und der Kontrolle werden Kreativität, Motivation und Produktivität beeinträchtigt, die aber andererseits Voraussetzung für wirtschaftlichen Erfolg sind.

Deshalb sollte und kann das Anliegen eines modernen Beschäftigtendatenschutzes nicht länger durch sehr allgemein gehaltene Regelungen erfüllt und die Auslegung den Arbeitsgerichten überlassen werden. Es muss – insbesondere nachdem Europa den Rahmen gesteckt hat – auch ein Anliegen des nationalen Gesetzgebers sowie der

Vertretungen von Beschäftigten und Arbeitgebern sein. Der Deutsche Gewerkschaftsbund (DGB) hat, nachdem über den Text der EU-DSGVO Einvernehmen erzielt worden war, signalisiert, dass er die Ausarbeitung eines nationalen Beschäftigtendatenschutzgesetzes fordert und dass er sich an dessen Ausarbeitung konstruktiv beteiligen will.[22] Die Diskussion über ein **modernes Beschäftigtendatenschutzgesetz** muss heute und mit hoher Priorität geführt und zu einem Erfolg gebracht werden.

[22] Hayen, DGB fordert nationales Datenschutzgesetz, www.bund-verlag.de 13.01.2016.

Abkürzungen

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Art.	Artikel
AuR	Arbeit und Recht (Zeitschrift)
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
CDU/CSU	Christlich Demokratische Union/Christlich Soziale Union
DANA	DatenschutzNachrichten (Zeitschrift)
DGB	Deutscher Gewerkschaftsbund
d. h.	das heißt
DV	Datenverarbeitung
DVBl	Deutsches Verwaltungsblatt (Zeitschrift)
EG-DSRl	Europäische Datenschutz-Richtlinie
EGMR	Europäischer Gerichtshof für Menschenrechte
ERP	Enterprise Ressource Planning
EU	Europäische Union
EU-DSGVO	Europäische Datenschutz-Grundverordnung
EuGH	Europäischer Gerichtshof
EuGRCh	Europäische Grundrechte-Charta
FDP	Freie Demokratische Partei
IKT	Informations- und Kommunikationstechnik
IT	Informationstechnik
KMU	kleine und mittlere Unternehmen
NJW	Neue Juristische Wochenschrift (Zeitschrift)
SGBs	Sozialgesetzbücher
s. o.	siehe oben
SPD	Sozialdemokratische Partei Deutschlands
StGB	Strafgesetzbuch
s. u.	siehe unten

TMG	Telemediengesetz
TKG	Telekommunikationsgesetz
USA	Vereinigte Staaten von Amerika (United States of America)
z. B.	zum Beispiel