WISO DISKURS

09/2017

Peter Wedde

BESCHÄFTIGTENDATENSCHUTZ IN DER DIGITALISIERTEN WELT

FRIEDRICH EBERT STIFTUNG

Die Friedrich-Ebert-Stiftung

Die Friedrich-Ebert-Stiftung (FES) wurde 1925 gegründet und ist die traditionsreichste politische Stiftung Deutschlands. Dem Vermächtnis ihres Namensgebers ist sie bis heute verpflichtet und setzt sich für die Grundwerte der Sozialen Demokratie ein: Freiheit, Gerechtigkeit und Solidarität. Ideell ist sie der Sozialdemokratie und den freien Gewerkschaften verbunden.

Die FES fördert die Soziale Demokratie vor allem durch:

- politische Bildungsarbeit zur Stärkung der Zivilgesellschaft;
- Politikberatung;
- internationale Zusammenarbeit mit Auslandsbüros in über 100 Ländern;
- Begabtenförderung;
- das kollektive Gedächtnis der Sozialen Demokratie mit u. a. Archiv und Bibliothek.

Die Abteilung Wirtschafts- und Sozialpolitik der Friedrich-Ebert-Stiftung

Die Abteilung Wirtschafts- und Sozialpolitik verknüpft Analyse und Diskussion an der Schnittstelle von Wissenschaft, Politik, Praxis und Öffentlichkeit, um Antworten auf aktuelle und grundsätzliche Fragen der Wirtschafts- und Sozialpolitik zu geben. Wir bieten wirtschafts- und sozialpolitische Analysen und entwickeln Konzepte, die in einem von uns organisierten Dialog zwischen Wissenschaft, Politik, Praxis und Öffentlichkeit vermittelt werden.

WISO Diskurs

WISO Diskurse sind ausführlichere Expertisen und Studien, die Themen und politische Fragestellungen wissenschaftlich durchleuchten, fundierte politische Handlungsempfehlungen enthalten und einen Beitrag zur wissenschaftlich basierten Politikberatung leisten.

Über den Autor dieser Ausgabe

Prof. Dr. Peter Wedde ist Professor für Arbeitsrecht und Recht der Informationsgesellschaft an der Frankfurt University of Applied Sciences, wissenschaftlicher Leiter der Beratungsgesellschaft d+a consulting GbR und wissenschaftlicher Berater des Anwaltsbüros Steiner Mittländer Fischer in Frankfurt.

Für diese Publikation ist in der FES verantwortlich

Stefanie Moser ist in der Abteilung Wirtschafts- und Sozialpolitik verantwortlich für den Bereich Gewerkschaften.

09/**2017**

WISO DISKURS

Peter Wedde

BESCHÄFTIGTENDATENSCHUTZ IN DER DIGITALISIERTEN WELT

VORWORT

Die Europäische Datenschutz-Grundverordnung findet ab dem 25. Mai 2018 in allen Mitgliedsländern der EU Anwendung. Sie schafft erstmals europaweit einen einheitlichen Rechtsrahmen für den Datenschutz. Die darin enthaltenen Vorschriften gelten auch für den Umgang mit Daten am Arbeitsplatz.

Bereits heute erheben und verarbeiten Unternehmen in ihren täglichen Betriebsroutinen eine nie dagewesene Menge an Informationen digital. In Zukunft werden sowohl das Volumen der im Betriebsprozess erhobenen Daten neue Dimensionen erreichen als auch die Möglichkeiten, diese Informationen gezielt zu analysieren.

Die Daten, die Unternehmen verwerten, beschränken sich nicht auf rein technische Betriebsdaten, sondern bestehen zu einem großen Teil aus personenbezogenen Daten, also Informationen, die sich auf einzelne Beschäftigte beziehen bzw. diesen zugeordnet werden können. Mithilfe dieser Informationen lassen sich technische und organisatorische Arbeitsprozesse optimieren und Betriebsabläufe effizienter gestalten. Gleichzeitig können die gewonnenen Daten aber auch genutzt werden, um die Leistung und das Verhalten von Arbeitnehmer_innen zu kontrollieren und/oder zu steuern. Bei der Frage des Umgangs mit Daten und Informationen kollidieren die Interessen des Unternehmens deshalb fast zwangsläufig mit den Interessen der Beschäftigten.

Wie wirken sich technische und organisatorische Innovationen in den Betrieben auf den Datenschutz am Arbeitsplatz aus? Welche Daten dürfen von Unternehmen nach derzeitiger Rechtslage gespeichert und ausgewertet werden, und welche Neuerungen bringt hier die DSGVO? Bedarf es weitergehender Gesetze und Regelungen, um die Persönlichkeitsrechte von Arbeitnehmer_innen zu schützen?

Prof. Dr. Peter Wedde liefert in der vorliegenden Studie Antworten auf diese Fragen und zeigt, wie der Datenschutz am Arbeitsplatz weiterentwickelt werden sollte, um die Rechte der Beschäftigten zu stärken. Die Debatte, wie beim Thema Datenverarbeitung und -schutz ein fairer Ausgleich zwischen den Interessen von Beschäftigten und Unternehmen geschaffen werden kann, findet mit der DSGVO kein Ende. Sie hat gerade erst begonnen. Wir hoffen, dass unsere Studie Ideen und Impulse für diese Diskussion liefert, und wünschen eine anregende Lektüre.

STEFANIE MOSER
Abteilung Wirtschafts- und Sozialpolitik
der Friedrich-Ebert-Stiftung

ZUSAMMENFASSUNG

In der digitalen Arbeitswelt stehen universelle vernetzte Arbeitsmöglichkeiten zur Verfügung. Technische Voraussetzung für die Erledigung von Arbeit ist lediglich ein leistungsfähiger Internetanschluss, über den ein elektronischer Kontakt zum Betrieb hergestellt werden kann. Die notwendige Software gibt es online per Cloud-Computing. Die neuen flexiblen Formen der Aufgabenerledigung werden durch Beschäftigungsverhältnisse außerhalb „klassischer" Arbeitsverträge ergänzt. Projektbezogene Arbeitsaufgaben können etwa über digitale Plattformen an Crowdworker_innen vergeben werden. Der Abschluss eines Arbeitsvertrags ist hier keine zwingende Voraussetzung mehr.

Die neuen technischen Möglichkeiten beinhalten eine deutliche Zunahme der personenbezogenen Informationen über Beschäftigte. Mangels eines spezifischen Beschäftigtendatenschutzgesetzes bestimmt sich die Zulässigkeit der Erhebung und Verarbeitung von Beschäftigtendaten weiterhin nach den allgemeinen Regelungen des derzeit noch geltenden Bundesdatenschutzgesetzes (BDSG) bzw. ab dem 25.5.2018 nach den Vorschriften der europäischen Datenschutz-Grundverordnung (DSGVO) und des „BDSG-neu". Alle genannten gesetzlichen Regelungen enthalten zum Beschäftigtendatenschutz jeweils nur eine allgemeine Vorschrift. Sowohl im aktuellen als auch im künftigen Datenschutzrecht bleiben damit wichtige Themen ungeregelt wie etwa das Fragerecht im Bewerbungsverfahren, die Zulässigkeit heimlicher Kontrollen oder der Lokalisierung von Beschäftigten, der Ausschluss von umfassenden Bewegungsprofilen oder von Dauerüberwachungen bzw. Regelungen zur Verwendung biometrischer Daten von Beschäftigten.

Die individual- und kollektivrechtlichen Möglichkeiten von Beschäftigten und ihren Interessenvertretungen zum Schutz vor unzulässigen Datenverarbeitungen durch Arbeitgeber_innen geraten auf der Basis des geltenden Arbeitsrechts an ihre Grenzen. Es zeichnet sich ein zunehmendes Ungleichgewicht zu ihren Lasten ab.

Auf der individualrechtlichen Ebene resultiert dieses Ungleichgewicht insbesondere daraus, dass sich die Durchsetzung datenschutzrechtlicher Positionen gegen einen Arbeitgeber/eine Arbeitgeberin für die Beschäftigten in der Praxis mit dem Risiko arbeitsrechtlicher Sanktionen verbindet. Diesem Risiko würde ein spezifischer Kündigungsschutz entgegenwirken, der sich an dem Schutzstandard orientiert, den es anderenorts zum Schutz von „Whistleblowern" gibt. Auch ein Ausbau des in Art. 80 DSGVO verankerten „datenschutzrechtlichen Verbandsklagerechts" würde die Position der Beschäftigten stärken. Darüber hinaus kommt der Schaffung eines längst überfälligen allgemeinen Beschäftigtendatenschutzgesetzes weiterhin eine hohe Priorität zu.

Auf der kollektivrechtlichen Ebene ist ebenfalls eine Anpassung der Mitwirkungs- und Mitbestimmungsrechte an die besonderen Anforderungen der digitalen Arbeitswelt notwendig. Erfolgen Datenverarbeitungsprozesse irgendwo auf der Welt, muss es betrieblichen Interessenvertretungen unter Durchbrechung des kollektivrechtlichen Territorialitätsprinzips beispielsweise möglich sein, die Interessen der von ihnen vertretenen Belegschaften entlang der gesamten „digitalen Produktionskette" zu wahren. Neben der Absicherung bestehender Mitbestimmungsrechte zum Schutz vor unzulässigen Verhaltens- und Leistungskontrollen ist darüber hinaus die Schaffung eines neuen „Mitbestimmungsrechts zum Datenschutz" zwingend. Erst auf der Basis eines solchen Mitbestimmungsrechts könnten Betriebs- und Personalräte die durch die DSGVO und das „BDSG-neu" eröffneten neuen kollektivrechtlichen Spielräume nutzen, um datenschutzrechtliche Themen zu regeln, wie etwa die Verankerung einer durchgängigen Zweckbindung bei der Datenverarbeitung, die Festlegung der Bedingungen für individuelle Einwilligungen von Beschäftigten oder die Ausgestaltung umfassender Löschkonzepte. Hinzu könnte die Entwicklung von Verfahren der Datenschutz-Folgenabschätzung kommen, die Risiken für Persönlichkeitsrechte schon bei der Ausgestaltung von IT-Systemen und IT-Anwendungen erkennen und vermeiden.

Im Ergebnis würden diese gesetzgeberischen Maßnahmen dazu führen, dass in der digitalen Arbeitswelt Chancen und Risiken fair verteilt sind und dass die neuen Möglichkeiten allen Betriebsparteien gleichermaßen zugutekommen.

1

EINLEITUNG

Daten sollen das Öl der Informationsgesellschaft des 21. Jahrhunderts sein. Diese Aussage muss eigentlich schon deshalb stimmen, weil eine Internetsuche 988.000 Treffer zu dieser Aussage ergibt. Oder vielleicht sind Daten sogar das Gold der Informationsgesellschaft (= 1.740.000 Treffer). Es ist aber schon fast egal, ob es sich bei Daten um Öl oder um Gold handelt. In jedem Fall verbinden sich mit Informationen, die sich auf Personen beziehen lassen, vielfältige Gewinnmöglichkeiten. Das ökonomische Potenzial dieses wertvollen Rohstoffs wird durch den kometenhaften Aufstieg von Konzernen wie Google, Facebook & Co illustriert, die die Wertschöpfung des digitalen Wertstoffs erfolgreich zum alleinigen Geschäftsmodell gemacht haben. Es manifestiert sich aber auch in der vielfältigen neuen Gestaltung der Arbeitswelt, in der das Tempo des Wechsels von analogen zu digitalen Arbeitsformen derzeit rasant zunimmt. Gekennzeichnet wird der Wechsel in diesem Bereich etwa durch die Zunahme der Mobilität von Beschäftigten, durch die Ausbreitung neuer digitaler Automatisierungstechniken sowie durch das Aufkommen neuer Beschäftigungsformen wie etwa das sogenannte Crowdworking.

Die Gewinnung und Verwendung des wertvollen „Rohstoffs Information" erfolgt allerdings weltweit unter höchst unterschiedlichen Rahmenbedingungen. Teilweise erinnern die Zustände in manchen Bereichen an die wilden Goldgräberzeiten früherer Jahrhunderte, in denen oft allein das Recht des Stärkeren galt. Diese Feststellung gilt im Angesicht der ungehemmten Datensammelwut einiger wirtschaftlich sehr erfolgreicher Superkonzerne besonders bezüglich der unterschiedlichen normativen Rahmenbedingungen, die es in verschiedenen Staaten für den Umgang mit personenbezogenen und personenbeziehbaren Daten gibt. In Deutschland genießen beispielsweise Informationen, die auf bestimmte Personen bezogen werden können, einen herausragenden Schutz. Das Recht auf informationelle Selbstbestimmung garantiert als wichtiges Grundrecht der digitalen Zeit den Schutz der Persönlichkeit. Vergleichbare Schutzstandards gibt es auch in den meisten anderen Staaten der Europäischen Union (EU). Die Europäische Datenschutz-Grundverordnung, die ab dem 25. Mai 2018 zwingend in allen EU-Staaten gelten wird, führt innerhalb der EU zu einer Vereinheitlichung des normativen Schutzrahmens.

Aus globaler Sicht wird die EU damit künftig so etwas wie eine „Datenschutz-Oase", in der Persönlichkeitsrechte von Bürger_innen in einzigartiger Form geschützt und gepflegt werden. Hingegen verzichten zahlreiche Staaten in- oder außerhalb Europas weitgehend oder ganz auf vergleichbare Datenschutzstandards. Aus ökonomischer Sicht hat dieser Verzicht u. a. den Vorteil, dass digitale Dienstleistungen ohne die Erfüllung von Datenschutzanforderungen günstiger erbracht werden können. Der Schutz der Persönlichkeitsrechte ist so ein Kostenfaktor, der mit dem Ziel der Verbesserung der Wettbewerbsfähigkeit minimiert werden muss.

Aber auch innerhalb Deutschlands bzw. in der EU ist die Sicherstellung der Persönlichkeitsrechte durch einen wirksamen Datenschutz nicht unproblematisch. Besonders gefährdet sind Persönlichkeitsrechte im Arbeitsleben, weil die Verarbeitungen erforderlicher Daten hier Vertragsbestandteil ist. Allerdings ist die Grenze zwischen aus Sicht von Arbeitgeber_innen erforderlichen und damit datenschutzrechtlich zulässigen Verarbeitungen auf der einen und unzulässigen Ausforschungen auf der anderen Seite in der Praxis oft nicht sehr trennscharf. Hinzu kommt, dass Beschäftigten die Wahrnehmung gesetzlich garantierter Datenschutzrechte aufgrund ihrer sozialen Abhängigkeit vom Arbeitgeber/von der Arbeitgeberin oft schwerfällt. Damit wächst die Gefahr, dass die Möglichkeiten der informationellen Selbstbestimmung eingeengt werden.

Vor dem Hintergrund dieser Gefahr und angesichts des hohen Tempos der stattfindenden Entwicklungen und Veränderungen zeigt die folgende Darstellung auf, welche Auswirkungen der Digitalisierung auf den allgemeinen datenschutzrechtlichen Rahmen hat. Ausgehend von einer Beschreibung aktueller technischer Entwicklungstrends (Kapitel 2), die das Arbeitsleben derzeit herausragend beeinflussen, erfolgt eine Beschreibung der datenschutzrechtlichen Rahmenbedingungen des Beschäftigtendatenschutzes (Kapitel 3). Diese Beschreibung bezieht sich einerseits auf den heute noch geltenden Rechtsrahmen, beinhaltet darüber hinaus aber

auch Hinweise zu den Veränderungen, die sich aus dem künftig europaweit geltenden Datenschutzrecht ableiten.

Ein weiterer Abschnitt dieser Darstellung befasst sich mit der betrieblichen Praxis (Kapitel 4) und mit den bestehenden Handlungsmöglichkeiten der kollektiven Interessenvertretungen (Kapitel 5). Exemplarisch werden hier die nach dem Betriebsverfassungsgesetz (BetrVG) bestehenden Möglichkeiten von Betriebsräten sowie erkennbare Regelungsdefizite skizziert.

Kapitel 6 enthält Hinweise zu notwendigen Anpassungen, die der Gesetzgeber vornehmen muss, um den Schutz der Beschäftigten und die Handlungsfähigkeit ihrer betrieblichen Interessenvertretungen auch angesichts der aus der Digitalisierung folgenden Veränderungen sicherzustellen. Das Fazit (Kapitel 7) fasst die wichtigsten Trends und Erkenntnisse mit Blick auf den Beschäftigtendatenschutz zusammen.

2

TECHNISCHE ENTWICKLUNGSTRENDS UND ORGANISATORISCHES UMFELD

2.1 INTERNET ALS ZENTRALES KOMMUNIKATIONSMEDIUM

Die Digitalisierung der Arbeitswelt ist als Thema längst nicht mehr so neu, wie es aufgrund der intensiven Diskussion dieses Themas gerade scheint. Über die Auswirkungen, die Informationstechnik (IT) auf die Arbeitswelt hat und die sich hiermit verbindenden Konsequenzen für Beschäftigte, wird schon seit mehr als 20 Jahren diskutiert. Neuartig ist aber das derzeit rasante Tempo der Entwicklung. Dieses führt dazu, dass die unterschiedlichen Einsatzvarianten für IT-Anwendungen kaum noch überschaubar sind. Hinzu kommen neue betriebliche Gestaltungsspielräume, die aus der zunehmend umfassenden Vernetzung von Hard- und Software folgen. Zudem werden Geräte aus dem IT-Bereich immer kleiner, kostengünstiger und leistungsfähiger. IT-Anwendungen und Endgeräte können zudem auf das Internet als universelle Vernetzungs- und Kommunikationsinfrastruktur zurückgreifen.

Ein derzeitiger Endpunkt der Entwicklung ist das immer wieder prognostizierte „Internet der Dinge" (Wedde 1995). Dieser Begriff steht im privaten Bereich für eine vollständige Integration und Vernetzung von Alltagsgegenständen im häuslichen Bereich wie etwa die Anbindung von Fernsehgeräten, Waschmaschinen, Geschirrspülern oder Haussicherungssystemen (BMAS 2017; Bitkom 2015; Briegleb 2015). Auch sehr persönliche Geräte wie Fitnessarmbänder oder Herzschrittmacher werden gerade ebenso Teil des neuen Netzes wie etwa umfassend vernetzte Autos. Im kommerziellen Bereich wird im Zusammenhang mit dem Internet der Dinge immer wieder darauf verwiesen, dass hier Maschinen mit Maschinen in nie gekannter Form kommunizieren können. Und auch eigentlich „dumme" Gegenstände wie etwa Paletten innerhalb von Warenwirtschaftssystemen werden „intelligent" mittels RFID.[1] Im Ergebnis macht das Internet der Dinge im betrieblichen Rahmen Neugestaltungen von Arbeit möglich, die derzeit unter Stichworten wie „Industrie 4.0" oder „Arbeit 4.0" (vgl. BMAS 2017) diskutiert und teilweise auch schon umgesetzt werden.

Das Fortschreiten der technischen Entwicklung wird nicht nur im Bereich des Internets der Dinge mit hoher Wahrscheinlichkeit dazu führen, dass die Trennung zwischen Geräten und Anwendungen aus dem beruflichen Sektor auf der einen und aus dem privaten bzw. häuslichen Bereich auf der anderen Seite aufgehoben wird. Dies ist beispielsweise der Fall, wenn private Endgeräte auch für berufliche Anwendungen verwendet und eingesetzt werden. Kommt es zu einer solchen Verschmelzung, werden über die unterschiedlichen Lebensbereiche hinweg Analysen und Auswertungen des individuellen Handelns und Verhaltens möglich. Über die hierfür notwendigen Analyse-Tools verfügen insbesondere die großen Anbieter von Internet-Kommunikationsplattformen und Suchmaschinen wie etwa Google, Facebook oder Microsoft bereits. Diese Anbieter sind in der Lage, die anfallenden Klar- und Metadaten jeglicher Kommunikationsformen zu erheben und auszuwerten. Dabei geht es gar nicht mehr gezielt um personenbezogene Daten einzelner Bürger_innen, sondern immer mehr um die Gewinnung von Strukturwissen und allgemeinen Erkenntnissen. Dieses Strukturwissen kann insbesondere dazu genutzt werden, das Verhalten einzelner Menschen zu prognostizieren oder deren persönliche Situation einzuschätzen. Entsprechende Möglichkeiten werden inzwischen unter dem Stichwort „Mining the Social Graph" diskutiert (Höller/Wedde 2016).

Trends wie das Internet der Dinge oder die Industrie 4.0 haben eine gemeinsame technische Grundlage: das weltweit verfügbare Internet als zentrales Medium für den Austausch aller Arten von Informationen und Anwendungen. Die Leistungsanforderungen an das Internet nehmen ständig zu. Im privaten Bereich folgt diese Zunahme beispielsweise aus der immer intensiver werdenden Nutzung von Audio- oder Video-Streaming-Diensten. Im beruflichen bzw. kommerziellen Bereich resultieren die erhöhten Anforderungen aus der Zunahme des Cloud-Computing das auf zentralisierte Datenspeicherung und permanente Abrufbarkeit von Informationen setzt. Hohe Anforderungen an die Leistungsfähigkeit des Internets leiten sich zudem aus der zunehmenden Verbreitung von neuartigen onlinebasierenden Soft-

1 „RFID" steht für die „Radio Frequency Identification"-Technologie, bei der sendefähige Aufkleber auf Gegenständen direkt mit digitalen Kontroll- und Steuerungsgeräten verbunden sind (Höller/Wedde 2016: 299, Rn. 8).

wareangeboten ab. Anwendungen wie die im folgenden Abschnitt beschriebenen führen dazu, dass der Ruf nach mehr Bandbreite und nach höheren Übertragungsgeschwindigkeiten eines der zentralen Begleitgeräusche der Digitalisierung ist.

Der Zugriff auf das Internet ist in Deutschland aufgrund der Verbesserung der Leistungsfähigkeit von Mobilfunknetzen und dem Ausbau der WLAN-Strukturen im öffentlichen wie im privaten Bereich inzwischen praktisch (fast) überall möglich. In speziellen Bereichen wird das WLAN durch neue Techniken wie etwa die sogenannte „Near Field Communication" (= „Nahfeldkommunikation") oder das inzwischen in vielfältigen Ausgestaltungen eingesetzte Bluetooth ergänzt und erweitert (Höller/Wedde 2016). Allerdings wird immer noch von Orten und Gegenden berichtet, die ohne einen Zugang zum schnellen Internet sind.

2.2 VERÄNDERUNG DER SOFTWARESTRUKTUREN: SAAS UND CLOUDWARE

Das leistungsfähige Internet machen sich inzwischen viele Softwareanbieter zunutze, indem sie ihre Produkte nicht mehr auf konventionellem Weg anbieten und verkaufen. Benötigte Softwarepakete können über das Internet als Datei gekauft und anschließend mithilfe eines Freischalt-Codes auf den eigenen Geräten installiert werden. Benötigte Handbücher oder Back-up-Dateien sind ebenfalls nur noch auf diesem Weg erhältlich.

Doch auch diese Vertriebsform ist inzwischen eigentlich schon wieder überholt. An ihre Stelle tritt sowohl für kommerzielle Anwender und Unternehmen als auch für Privatnutzer vielfach das Konzept von „Software as a Service" (SaaS). Hierbei wird die vollständige Software nicht mehr auf den Endgeräten der Nutzer_innen installiert, sondern ist nur noch „online" über das Internet verfügbar. Auf den Geräten finden sich nur noch Programme für den Zugriff auf die Software. Für den Fall, dass kein Zugang zum Internet vorhanden ist, gibt es teilweise (abgespeckte) „Notprogramme".

SaaS hat für die Anwender den Vorteil, dass sie immer über die neueste Software verfügen. Nachteilig ist allerdings, dass die Abhängigkeit von bestimmten Anwendern zunimmt. Zudem haben sie nur noch geringe Möglichkeiten, individuelle Anpassungen vorzunehmen. Das sogenannte Customizing, das heißt die Anpassung von Standardsoftware an betriebliche Bedürfnisse, gehört damit in weiten Bereichen der Vergangenheit an. Die Möglichkeiten der Anwender_innen beschränken sich auf das, was Softwareanbieter ihnen elektronisch zur Verfügung stellen.

Dieser neue Softwaretrend hat nachhaltige Auswirkungen auf die arbeitsrechtliche Situation. Betriebsräte erleben schon heute, dass Arbeitgeber_innen ihnen entgegenhalten, dass sie mitbestimmungsrechtlich indizierte Änderungen an IT-Systemen oder mitbestimmungsrechtliche Vereinbarungen nicht umsetzen können, weil SaaS dies nicht zulässt. Der neue technische Trend könnte damit in diesem Bereich das Ende der Mitbestimmung signalisieren.

2.3 „APPISIERUNG"

Der Zugriff auf SaaS-Anwendungen sowie auf die in der Cloud gespeicherten Daten ist inzwischen nicht nur über „konventionelle" Endgeräte wie etwa PCs und Notebooks möglich. Er kann regelmäßig auch über mobile Smartphones oder Tablets erfolgen. Voraussetzung für diese Zugriffe ist lediglich eine entsprechende App. Der Begriff „App" steht für „Applications". Hierbei handelt es sich um kleine Zusatzprogramme, die die spezifischen Fähigkeiten von Endgeräten wie Smartphones oder Tablets nutzen und die den Anwender_innen dort Zugriffsmöglichkeiten auf die verschiedenen Soft-wareanwendungen bieten und Verarbeitungsmöglichkeiten zur Verfügung stellen. Auf den Bildschirmen der mobilen Geräte werden Apps zumeist als „Kacheln" dargestellt. Diese Darstellungsform wird inzwischen auch von Betriebssystemen wie etwa „Windows 10" aus dem Hause Microsoft aufgegriffen. Dies zeigt, wie weit die Gewöhnung an die neue Welt der Apps inzwischen fortgeschritten ist.

Sind die notwendigen Apps auf einem Endgerät installiert, müssen Nutzer_innen nur noch persönliche Zugangsdaten eingeben, um auf betriebliche oder private Daten oder Anwendungen zugreifen zu können. Aus Sicht von Nutzer_innen und Anwender_innen ist dies ein komfortabler Weg. Er verbindet sich aber mit dem Risiko, dass oft nicht mehr genau bekannt ist, wo welche Daten gespeichert werden und was hinter den Apps steckt.

Die umfassende „Appisierung" von Datenverarbeitungsprozessen im beruflichen wie im privaten Bereich beinhaltet eine Reihe von Problemen. So ist für Durchschnittsanwender_innen bei vielen Apps nicht erkennbar, welche Datenverarbeitungsprozesse durch diese Software im Hintergrund angestoßen werden. Teilweise greifen die Apps auf Daten der Benutzer_innen zu, die mit dem eigentlichen Verarbeitungszweck gar nichts zu tun haben. Interessant sind für die Anbieter der Apps insbesondere Daten über den Standort der Benutzer_innen, aber auch Adress- und Kalenderinformation. Hinzu kommt, dass die Nutzung beruflicher und privater Apps auf denselben Geräten schnell zu einer Vermischung von Daten aus diesen unterschiedlichen Lebensbereichen führen kann und dass dem Anbieter oder dem Arbeitgeber/der Arbeitgeberin im Extremfall sehr persönliche Informationen zugänglich werden können.

2.4 FLEXIBILISIERUNG UND MOBILISIERUNG DER ARBEIT

Vernetzte mobile Endgeräte machen es in der digitalisierten Arbeitswelt möglich, dass die Erbringung von Arbeitsleistungen nicht mehr an bestimmte Orte gebunden ist. Diese Feststellung gilt nicht nur für Verwaltungs- und Dienstleistungsbereiche. Auch die Steuerung und Kontrolle von Produktionsanlagen oder Maßnahmen der Qualitätssicherung lässt sich beispielsweise grundsätzlich ortsunabhängig erbringen. Voraussetzung ist in allen Fällen lediglich, dass Beschäftigte eine stabile und leistungsfähige Verbindung zum Internet haben, über die sich Aufgaben erledigen, Prozesse steuern oder Kontrollen durchführen lassen.

Ist die elektronische Kommunikation über eine leistungsfähige Internetverbindung möglich, spielt die geografische

Lage des Betriebes bzw. des aktuellen Aufenthaltsortes von Beschäftigten keine entscheidende Rolle mehr. Damit verlieren konventionelle Betriebsstätten für viele Arbeitsformen zunehmend an Bedeutung. Darüber hinaus verbessern sich die Voraussetzungen für die Leistungen von Arbeitsformen, die schon bisher außerhalb des Betriebs angesiedelt waren wie etwa im Bereich von Vertrieb oder Service.

Optimale Voraussetzungen bestehen inzwischen auch für Formen häuslicher Arbeit. Im Homeoffice können praktisch alle Arbeiten erbracht werden, die in Betrieben, am Schreibtisch oder an Bildschirmen der Produktion möglich sind. Häusliche Arbeit ist damit aus technischer Sicht unproblematisch, zumal in vielen Haushalten inzwischen ein leistungsfähiger Internetanschluss zur Verfügung steht.

2.5 BRING YOUR OWN DEVICE

Unterstützt wird der Trend hin zu mobiler Arbeit und zur Tätigkeit im Homeoffice durch die zunehmende Verbreitung leistungsfähiger mobiler Endgeräte im beruflichen wie im privaten Bereich (Schwemmle/Wedde 2012). Vor diesem Hintergrund scheint es nur logisch, private Geräte auch für dienstliche Zwecke zu verwenden. Befördert wurde dieser Trend auch dadurch, dass einzelne Beschäftigte privat über leistungsfähigere Geräte verfügten als die, die Arbeitgeber_innen ihnen zur Verfügung stellten. Als Bezeichnung für diese Nutzung privater Geräte im dienstlichen Zusammenhang hat sich der Begriff „Bring Your Own Device (BYOD)" eingebürgert (Brandt 2016: 34f.; Höller/Wedde 2016: 365, Rn. 302).

Problematisch ist, dass es bei BYOD zu einer Vermischung von dienstlichen und privaten Datenflüssen kommen kann, wenn nicht ausreichende technische und organisatorische Vorsorge getroffen wird. Diese Vorsorge verbindet sich aus technischer Sicht regelmäßig damit, dass Arbeitgeber_innen Zugriff auf die privaten Geräte der Beschäftigten nehmen, um hier einen besonders gesicherten Client zu installieren oder Anpassungen der Software durchzuführen. Erfolgen diese technischen und organisatorischen Sicherungsmaßnahmen nicht, besteht die Gefahr, dass betriebliche Daten unbefugt in fremde Hände geraten können.

Entsprechende Schutzmaßnahmen können inzwischen etwa auf der Grundlage von „Mobile Device Management (MDM)"-Systemen realisiert werden. Bei MDM handelt es sich um Software, die in zentralen Systemen sowie auf allen Endgeräten installiert wird. Über diese spezielle Software kann beispielsweise gesteuert werden, ob Endgeräte auf bestimmte Systeme oder Dateien zugreifen können, welche Upload- und Download-Möglichkeiten bestehen oder zu welchen Zeiten Verbindungen überhaupt möglich sind (Höller/Thannheiser 2015; Steinwender 2013).

Mittels MDM-Software ließe sich zudem auch sicherstellen, dass nach einer zehnstündigen Arbeitszeit, die aufgrund verschiedener Aktivitäten in betrieblichen Systemen erkennbar ist, für die nächsten elf Stunden kein weiterer Zugriff und somit keine digitale Erreichbarkeit möglich ist. Ggf. könnte eine solche MDM-Sperre auch so ausgestaltet werden, dass Zugriffe und Verbindungen zwar möglich bleiben, dass die Übertragungsgeschwindigkeiten aber deutlich reduziert wird, was eine Weiterarbeit in Notfällen möglich machen würde.

2.6 BIG DATA UND DATA-MINING

Der Begriff „Big Data" steht in der Diskussion für eine Gruppe von Software, die es ermöglicht, unstrukturierte Daten aus verschiedensten Dateien und Systemen für übergreifende und zentrale Auswertungen aufzubereiten und auszuwerten (Höller/Wedde 2016; Tiemeyer 2015). Klassische Textdateien werden ebenso einbezogen wie beispielsweise Bild- oder Videodateien, aber auch Informationen aus spracherkennenden IT-Systemen. Die anfallenden großen Datenmengen, die ausgewertet werden müssen, sind für Big-Data-Software allenfalls bezogen auf die Verarbeitungsgeschwindigkeit eine Herausforderung, nicht aber hinsichtlich der grundsätzlichen Möglichkeiten einer strukturierten Aufbereitung an sich.

Die Erkenntnisse, die sich mittels Big-Data-Auswertungen gewinnen lassen, sind umso effektiver, je mehr Daten einbezogen werden können. Dies gilt auch für Beschäftigtendaten und erklärt das Interesse von Anwender_innen, auf Datenlöschungen so weit wie möglich zu verzichten und stattdessen in den vorhandenen Informationsbeständen Data-Mining zu betreiben. Dieser Begriff wiederum steht für eine Auswertungsmethode, die darauf zielt, neues bzw. bisher noch nicht identifiziertes betriebliches Wissen zu erkennen und nutzbar zu machen (Höller/Wedde 2016; Wedde 2016a; Wilke 2006). Aufschlussreich können darüber hinaus für Big-Data-Analysen auch Informationen aus dem privaten Bereich sein, die etwa aufgrund einer zulässigen privaten Nutzung auf dienstlichen Geräten vorhanden sind oder die im Rahmen von BYOD-Konzepten für Analysesoftware zugänglich werden.

Eine Möglichkeit, die Big-Data-Anwendungen auf der Grundlage von Data-Mining in sich bergen, sind relativ zuverlässige Voraussagen des wahrscheinlichen Verhaltens von Beschäftigten in der Zukunft. In diesem Rahmen setzen einschlägige Analyseprogramme das Verhalten einzelner Beschäftigter in Relation zum Durchschnittsverhalten. Auf der Grundlage einer breiten Datenbasis wird es beispielsweise möglich, Abweichungen im Arbeitsverhalten zu erkennen, die auf Situationen hinweisen, die aus Sicht von Arbeitgeber_innen problematisch sind wie etwa sich anbahnende Krankheiten von Beschäftigten, Abwanderungsgedanken oder das Aufkommen von Widerstand gegen Arbeitsbedingungen, die von einer Gruppe von Beschäftigten als belastend oder ungerecht empfunden werden. Besonders der letztgenannte Trend könnte auch bezüglich der Frage bewertet werden, ab wann mit der Gründung eines noch nicht vorhandenen Betriebsrats zu rechnen ist.

2.7 CLOUD- UND CROWDWORK

Die Datenverarbeitung in der Cloud, kurz oft auch als Cloud-Computing bezeichnet, ist einer der großen Trends in der digitalen Arbeitswelt. Der Begriff „Cloud" steht im Sinne der wörtlichen Übersetzung für eine Wolke. In dieser „digitalen Wolke" befinden sich Server und Rechnernetze, die über das Internet verbunden sind. Die Cloud-Struktur ermöglicht es Nutzer_innen, Rechnerleistungen in diese Cloud zu verlagern, ohne dass sie noch genau wissen, wo Verarbeitungen geografisch stattfinden. Eigentlich ist Cloud-Computing nicht wirklich neu, sondern steht nur für eine moderne Weiter-

entwicklung des schon seit mehr als 20 Jahren bekannten „Outsourcing(s)“ oder des „Offshoring(s)“ (Wedde/Klöver 1993).

Aus technischer Sicht spielt es für Cloud-Computing keine Rolle, ob notwendige Datenverarbeitung in unmittelbarer Nähe des Betriebs erfolgt oder irgendwo auf der Welt. Die bei größeren Entfernungen auftretenden minimalen Zeitverzögerungen spielen allenfalls für bestimmte Anwendungen eine Rolle, etwa für den „Hochgeschwindigkeitshandel“ im Börsenbereich. Handelt es sich um betriebliche Standardanwendungen oder -aufgaben, werden diese kleinen Zeitverzögerungen hingegen allenfalls von der Software bemerkt, nicht aber von den Beschäftigten.

Im Rahmen von Cloud-Computing können sowohl Rechnerleistungen nach Bedarf abgerufen als auch notwendiger Speicherplatz eingekauft und belegt werden. Hinzu kommen inzwischen mit SaaS immer öfter vollständige Anwendungen, sodass die gesamte Rechnerleistung aus einer Hand abgerufen werden kann (Höller/Wedde 2016).

Aus arbeitsrechtlicher Sicht steht der Begriff „Crowdwork“ für eine neue Form der Arbeit, bei der Beschäftigte für beliebige Anbieter bzw. Kund_innen Arbeits- und Dienstleistungen – vermittelt über das Internet – erbringen. Ein immer wieder zitiertes Beispiel für Crowdworking ist der „Mechanical Turk“ der Firma Amazon. Hier können sich arbeitswillige Crowdworker_innen um Aufträge bewerben und diese erledigen. Gezahlt wird auf Basis der erledigten Leistungen sowie der dabei erkennbaren Qualität der Arbeit (Strube 2015). Crowdwork gibt es aber auch im Rahmen von Arbeitsverhältnissen. In Deutschland wurde die Diskussion hierzu angestoßen durch die Absicht der Firma IBM, im Rahmen eines Programms „Liquid“ in Deutschland Tausende von Arbeitsplätzen abzubauen (Stach 2015). Anstelle der freigesetzten Beschäftigten sollten Aufgaben – vermittelt über eine Cloud – im Internet erbracht werden. Das Programm wurde allerdings nach Bekanntwerden in dieser Form in Deutschland nicht realisiert. Das Konzept, in dem Crowdwork erbracht wird, wird auch oft als Crowdsourcing bezeichnet (Leimeister et al. 2015: 11). Die Begriffe „Crowdsourcing“ und „Crowdwork“ oder „Crowdworking“ werden allerdings in vielen Fällen synonym verwendet.

Aus datenschutzrechtlicher Sicht ist bei den unterschiedlichen Formen von Cloud- oder Crowdwork oft nicht nachvollziehbar, auf welcher Grundlage die Erhebung, Verarbeitung und Nutzung der Beschäftigtendaten erfolgt. Dies beginnt schon bei der derzeit noch nach § 4a Abs. 1 Bundesdatenschutzgesetz (BDSG) bestehenden Notwendigkeit der schriftlichen Erteilung einer Einwilligung, die oft nicht gegeben ist. Erfolgt die Vermittlung von Aufträgen über Plattformen oder sind Beschäftigte als Subunternehmer_innen tätig, fehlt es oft an den notwendigen Verträgen zur Auftragsdatenverarbeitung oder zur Funktionsübertragung. Diese Defizite werden mit hoher Wahrscheinlichkeit auch ab Wirksamkeit der Datenschutz-Grundverordnung (DSGVO) und des „BDSG-neu“ fortbestehen. Das hat zwar für die Anbieter von Cloud- oder Crowdwork den wirtschaftlichen Vorteil, dass sie auf kostenträchtige Datenschutzmaßnahmen verzichten können. Dieser Vorteil wandelt sich für die auf Basis konventioneller Arbeitsverhältnisse Beschäftigten in den Nachteil, dass ihre Arbeit aus datenschutzrechtlicher Sicht nicht mehr konkurrenzfähig ist.

2.8 INTERNATIONALISIERUNG

Aus technischer und organisatorischer Sicht kennt die digitale Arbeit keine geografischen Grenzen mehr. Diese Feststellung gilt nicht nur für die vorstehend angesprochenen Formen von Cloud- und Crowdwork, sondern auch für konventionelle Beschäftigungsformen. Auf der rechtlichen Ebene stehen den Möglichkeiten der weltweiten Datenverarbeitung allerdings datenschutzrechtliche Vorgaben entgegen (vgl. Kapitel 3).

Technische Möglichkeiten, die auf geografische Situationen keine Rücksicht mehr nehmen müssen, führen schon aus Kostengründen dazu, dass viele Beschäftigte inzwischen im internationalen Kontext tätig sind und beispielsweise im Rahmen einer sogenannten Matrixorganisation Vorgesetzte aus anderen Ländern haben oder Beschäftigte in anderen Ländern führen. Bezogen auf die Verarbeitung selbst gilt das Gleiche. Auch hier lassen sich gerade im Zusammenhang mit Cloud-Computing-Konzepten Datenflüsse über Staatsgrenzen und über Kontinente hinweg feststellen. Der Internationalisierung von Arbeitsprozessen scheinen in der digitalen Welt keine Grenzen gesetzt zu sein.

2.9 ZWISCHENERGEBNIS

Unternehmen, kommerziellen Anwender_innen und privaten Nutzer_innen stehen in der digitalen Welt inzwischen universelle Verarbeitungsmöglichkeiten zur Verfügung, die zudem keine geografischen Festlegungen mehr erfordern. Außerdem ist die Arbeitserbringung aus Sicht von Unternehmen unter Einsatz von Cloud-Computing in vielen Fällen sehr flexibel und zumeist auch deutlich kostengünstiger als bisher. Hinzu kommt, dass statische Modelle der Hard- und Softwarearchitektur, die noch vor ein paar Jahren in vielen Bereichen Standard waren, inzwischen vielfach der Vergangenheit angehören. Sie werden beispielsweise durch Cloud-Computing und SaaS ersetzt. Und die individuelle Arbeit erfolgt mit diesen neuen Möglichkeiten an schon fast beliebigen Endgeräten und vielfach mobil.

Dieser durch ein hohes Maß an Flexibilität geprägten Situation stehen allgemein auf der rechtlichen und speziell auf der datenschutzrechtlichen Ebene statische Regelungsmodelle gegenüber. Notwendige Anpassungen dieser Regelungsmodelle erfolgen (wenn überhaupt) regelmäßig erst zeitversetzt nach der Einführung neuer technischer Möglichkeiten. Dies führt vielfach zu einer Aushöhlung des gesetzlichen Schutzrahmens. Damit bestimmt nicht mehr der Gesetzgeber die Leitlinien des normativen Schutzrahmens, der etwa zur Wahrung von Persönlichkeitsrechten zur Verfügung steht, sondern die Anwender_innen von technischen Prozessen und Möglichkeiten. Diese Situation führt schon fast zwangsläufig zu einer Verwässerung des Schutzstandards, der sich für Arbeitnehmer_innen bisher aus einschlägigen arbeitsrechtlichen Schutzregeln ableitet. Welche Probleme für den Beschäftigtendatenschutz aus den neuen technischen Rahmenbedingungen resultieren und wie sich das prognostizierte Auseinanderfallen der technischen Möglichkeiten und des rechtlichen Rahmens auswirken, zeigt das folgende Kapitel.

3

GESETZLICHE GRUNDLAGEN

3.1 RECHTLICHE ASPEKTE DER DIGITALISIERUNG AUS DER SICHT VON BESCHÄFTIGTEN

Die Digitalisierung der Arbeitswelt beeinflusst die individuelle Situation von Beschäftigen und insbesondere die von Arbeitnehmer_innen massiv. Auswirkungen gibt es insbesondere auf den Bereich des Beschäftigtendatenschutzes, der im Mittelpunkt dieses Abschnitts steht. Darüber hinaus wird aber auch der allgemeine arbeitsrechtliche Regelungs- und Schutzrahmen tangiert, der zugunsten von Arbeitnehmer_innen besteht. Dies wird beispielsweise für den Bereich des Arbeitszeitrechts am Aufeinandertreffen von Flexibilisierungsforderungen der Arbeitgeber_innen auf der einen und den bestehenden Arbeitszeitbegrenzungen in den §§ 3 ff. des Arbeitszeitgesetzes (ArbZG) auf der anderen Seite deutlich. Gleiches gilt für das Verbot der Arbeit an Sonn- und Feiertagen in § 9 ArbZG, das beispielsweise auch bei mobiler oder häuslicher Arbeit zu beachten ist, oder für die durch § 5 ArbZG vorgeschriebenen Mindestruhezeiten. Allgemeine arbeitsrechtliche Themen werden im Folgenden nur am Rande behandelt. Im Mittelpunkt der Darstellung wird der Beschäftigtendatenschutz stehen.

(a) Digitalisierung der Arbeit und Beschäftigtendatenschutz

Für den Beschäftigtendatenschutz leiten sich aus der Digitalisierung der Arbeit grundlegende neue Anforderungen ab. Diese resultieren sowohl aus neuen Formen der Software wie etwa (insbesondere SaaS) als auch aus Softwareanwendungen, die speziell auf die Analyse des Arbeitsverhaltens abzielen wie insbesondere spezielle Analyse-Tools (Höller 2016).

Die Folgen dieser Entwicklung sind vielfältig. Herausragend ist eine feststellbare Zunahme von Informationen, die über jeden einzelnen Arbeitnehmer/jede einzelne Arbeitnehmerin vorliegen. Hierbei geht es längst nicht mehr um allein unmittelbar personenbezogene Daten, an denen sich das Verhalten und die Leistung von einzelnen Beschäftigten ablesen lässt, wie etwa erbrachte Stückzahlen, Tempo der Arbeitserledigung oder die sekundengenaue Uhrzeit einzelner Arbeitsschritte. In den Mittelpunkt des Interesses rücken vielmehr allgemeine oder verallgemeinerbare Zusatzinformationen und „Metadaten". In betriebsinternen sozialen Netzwerken fällt neben den Informationen, die dort von einzelnen Beschäftigten bewusst freigegeben werden, eine Fülle von Erkenntnissen über Beschäftigte an wie etwa Hinweise zum allgemeinen Kommunikationsverhalten, zur Akzeptanz bei Kolleg_innen oder zu Arbeitsmethoden. Im Ergebnis nimmt damit das Wissen zu, das Arbeitgeber_innen über einzelne Arbeitnehmer_innen haben. Dieses lässt sich noch vertiefen, wenn Analysesoftware eingesetzt wird, die alle vorhandenen (Zusatz-) Informationen langfristig speichert, auf der Metaebene mit vergleichbaren Daten aus anderen Bereichen und Unternehmen abgleicht und hieraus individuelle Verhaltensprognosen ableitet. Analyse-Tools ermöglichen es auch, aus einem Verhalten in der Gegenwart auf wahrscheinliche Verhaltensweisen und Entscheidungen von Beschäftigten in der Zukunft zu schließen. So wirbt etwa die Personalverarbeitungssoftware „Workday" damit, dass Abwanderungsgedanken von Beschäftigten mittels entsprechender Analyse-Tools vorab erkannt werden können. Auf der Grundlage dieser Erkenntnisse werden Arbeitgeber_innen Reaktionsvorschläge zur Verfügung gestellt, um wichtige Beschäftigte weiter an das Unternehmen zu binden – oder aber, um das Arbeitsverhältnis entbehrlicher Beschäftigter problemlos abzuwickeln und zum richtigen Zeitpunkt für Nachfolger_innen zu sorgen. Damit sind die viel zitierten „gläsernen Belegschaften"[2] Wirklichkeit geworden.

Diese aus Sicht von Personalabteilungen komfortable Situation trifft auf einen datenschutzrechtlichen Schutzrahmen, der durch relativ restriktive und enge Vorgaben gekennzeichnet ist. Einschlägige Gesetze wie insbesondere das BDSG beinhalten grundlegende Vorgaben aus der Rechtsprechung, wie sie insbesondere das Bundesverfassungsgericht (BVerfG) in seiner Entscheidung zur Rechtswidrigkeit der geplanten Volkszählung im Jahr 1983 gemacht hat (BVerfG 1983). Das mit dieser Entscheidung begründete „Recht auf informationelle Selbstbestimmung" gibt einzelnen Bürger_innen ein absolutes Verfügungsrecht an ihren Daten, das nur ausnahmsweise mit Blick auf das Gemeinwohl eingeschränkt werden kann.

---

2 So der Titel des „Standardwerks" von Wolfgang Däubler aus dem Jahr 1987.

Diese verfassungsrechtliche Vorgabe prägt mit Blick auf die Drittwirkung von Grundrechten und die Umsetzung der Vorgaben des Bundesverfassungsgerichts die Verarbeitung von Beschäftigtendaten durch Arbeitgeber_innen.

Von grundlegender Bedeutung ist in diesem Zusammenhang die Ausgestaltung des BDSG als Verbotsgesetz mit Erlaubnisvorbehalt. Das heißt, dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nach der zentralen Regelung in § 4 Abs. 1 BDSG überhaupt nur dann erfolgen kann, wenn es hierfür eine eindeutige und klare gesetzliche Grundlage oder eine freiwillige Einwilligung der betroffenen Personen gibt.

(b) „Europäischer Beschäftigtendatenschutz"

Der rechtliche Rahmen für den Beschäftigtendatenschutz, der sich derzeit in Deutschland insbesondere aus dem BDSG ableitet, wird ab dem 25.5.2018 durch die Vorschriften der Europäischen DSGVO bestimmt. Diese Verordnung, die dann der europaweit einheitliche Maßstab für die Zulässigkeit der Verarbeitung sein wird, verändert allerdings die rechtliche Situation im Bereich des Beschäftigtendatenschutzes nicht. Das resultiert insbesondere daraus, dass die DSGVO strukturell identisch mit den einschlägigen Vorgaben des BDSG ist. Änderungen zeichnen sich allerdings zu Detailfragen ab wie etwa bezüglich der Pflicht zum „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" („Privacy by Design") in Artikel 25 DSGVO. IT-Anwender_innen, die personenbezogene Daten verarbeiten, müssen deshalb IT-Systeme beispielsweise so ausgestalten, dass wählbare Datenschutzeinstellungen standardmäßig aktiviert oder dass Löschungsfristen so kurz wie möglich eingestellt sind. Entsprechende Pflichten bestehen bezogen auf Beschäftigtendaten auch für Arbeitgeber_innen. Gleiches gilt für das in Artikel 17 DSGVO enthaltene „Recht auf Löschung" in seiner Ausgestaltung als „Recht auf Vergessenwerden", das in der Praxis beispielsweise die durchgängige Verankerung von Löschkonzepten im Bereich der Verarbeitung von Beschäftigtendaten unumgänglich macht. Unterstrichen wird die Wertigkeit, die dem Datenschutz zukünftig einzuräumen ist, auch dadurch, dass Artikel 83 DSGVO für Verstöße gegen die Vorgaben der DSGVO einen Bußgeldrahmen von bis zu 20 Millionen Euro oder im Fall eines Konzerns bis zu vier Prozent vom Konzernjahresumsatz des Vorjahres vorsieht.

Die neue DSGVO überlässt die Ausgestaltung des Beschäftigtendatenschutzes innerhalb des allgemeinen datenschutzrechtlichen Rahmens, den sie vorgibt, den Mitgliedstaaten. Nach Artikel 88 DSGVO können diese spezifischen Vorschriften zum Beschäftigtendatenschutz durch Rechtsvorschriften oder durch Kollektivvereinbarungen vorsehen. In diesem Rahmen können Betriebsräte in künftigen Betriebsvereinbarungen auch spezielle Datenschutzregelungen für Bewerbungsverfahren sowie für die Durchführung von Arbeitsverträgen verankern. Voraussetzung dieser Regelung ist nach Artikel 88 Abs. 2 DSGVO die Verankerung angemessener und besonderer Maßnahmen zur Wahrung der menschlichen Würde, dem rechtlichen Interesse und der Grundrechte betroffener Personen, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb eines Konzerns und bezüglich der Überwachungssysteme am Arbeitsplatz.

Ergänzend zu den Regelungen der DSGVO müssen für die Bewertung von Art und Umfang des Beschäftigtendatenschutzes die einschlägigen Vorschriften beachtet werden, die das Datenschutz-Anpassungs- und Umsetzungsgesetzes (DSAnpUG) enthält. Dieses Gesetz soll die Spielräume ausfüllen, die die DSGVO den EU-Einzelstaaten zur Verfügung stellt. Ein Hauptbestandteil dieses Artikelgesetzes ist eine Neufassung des BDSG („BDSG-neu"), soweit diese vor dem Hintergrund der DSGVO notwendig und möglich ist. Dieses „Anpassungsgesetz-BDSG" zielt im Kern darauf, den durch die DSGVO gegebenen Gestaltungsspielraum bezüglich der Übernahme von datenschutzrechtlichen Regelungen auszufüllen.

Ungeachtet der anstehenden Neuregelung des gesetzlichen Datenschutzes geht die folgende Darstellung der datenschutzrechtlichen Vorgaben zum Beschäftigtendatenschutz von der aktuellen Rechtssituation aus. Die Ausführungen werden allerdings durch die Benennung der künftig geltenden Vorschriften der DSGVO bzw. des „BDSG-neu" (jeweils in Klammern) ergänzt. Darüber hinaus werden grundlegende Veränderungen benannt, die sich aus dem neuen Recht ableiten.

Tabelle 1
Wichtige gesetzliche Vorschriften zum Beschäftigtendatenschutz

Datenschutzrechtliche Vorgaben zum Beschäftigtendatenschutz	„Aktuelles Recht" Vorschriften des BDSG	„Künftiges Recht" Vorschriften der DSGVO und des „BDSG-neu"
Besondere Arten personenbezogener Daten	§ 3 Abs. 9 BDSG	Artikel 9 Abs. 1 DSGVO
Datenvermeidung und Datensparsamkeit	§ 3a BDSG	Artikel 5 Abs. 1 Buchstabe c) DSGVO
Allgemeine Zulässigkeit der Verarbeitung	§ 4 Abs. 1 BDSG	Artikel 6 Abs. 1 DSGVO
Spezielle Erlaubnisnorm für die Verarbeitung von Beschäftigtendaten	§ 32 Abs. 1 Satz 1 BDSG	Artikel 88 Abs. 1 DSGVO in Verbindung mit § 26 „BDSG-neu"
Einwilligung als Rechtsgrundlage	§ 4a BDSG	Artikel 7 Abs. 1 Buchstabe a) DSGVO in Verbindung mit § 26 Abs.
Berechtigte Interessen des Arbeitgebers	§ 28 Abs. 1 Satz 1 Nr. 2 BDSG	Artikel 6 Abs. 1 Buchstabe f) DSGVO
Löschung von Daten	§ 35 Abs. 2 BDSG	Artikel 17 DSGVO
Sperrung von Daten	§ 35 Abs. 3 BDSG	§ 35 „BDSG-neu"
Auskunftsrechte	§ 34 Abs. 1 BDSG	Artikel 15 Abs. 1 DSGVO
Auftragsdatenverarbeitung	§ 11 BDSG	Artikel 28 DSGVO
Übermittlung von Daten in Drittländer	§ 4b Abs. 1 BDSG	Artikel 44 DSGVO

(c) Zulässigkeit der Verarbeitung nach § 4 Abs. 1 BDSG

Die im vorstehenden Abschnitt a) angesprochene Ausgestaltung des BDSG als Verbotsgesetz mit Erlaubnisnormen findet ihren gesetzlichen Niederschlag in § 4 Abs. 1 BDSG (künftig Artikel 6 Abs. 1 DSGVO). Nach dieser Vorschrift ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG selbst oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder wenn Betroffene eingewilligt haben. Ist die gesetzliche Zulässigkeit gegeben, müssen von Arbeitgeber_innen die weiteren allgemeinen Vorgaben des BDSG beachtet werden wie insbesondere der Grundsatz der Datenvermeidung und Datensparsamkeit in § 3a BDSG (künftig Artikel 5 Abs. 1 Buchstabe c) DSGVO). Hiernach muss sich jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten ebenso wie die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel ausrichten, so wenig personenbezogene Daten wie möglich zu verwenden. Ist eine Verwendung von Beschäftigtendaten unumgänglich, müssen diese anonymisiert oder pseudonymisiert werden, soweit dies möglich bzw. verhältnismäßig ist. In Artikel 5 Abs. 1 Buchstabe c) DSGVO ist der ausdrückliche Hinweis auf die Notwendigkeit einer Anonymisierung bzw. Pseudonymisierung zwar nicht mehr ausdrücklich enthalten. Die Notwendigkeit entsprechender Maßnahmen leitet sich indes aus dem hier für die gesamte DSGVO festgeschriebenen Grundsatz der Datenminimierung ab.

Beschäftigte müssen zudem über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung ihrer Daten von ihrem Arbeitgeber/von ihrer Arbeitgeberin als verantwortlicher Stelle informiert werden. Diese vorgesehenen Zwecke müssen nach § 28 Abs. 1 Satz 2 BDSG (künftig Artikel 5 Abs. 1 Buchstabe b) DSGVO) bereits bei der Erhebung konkret festgelegt werden. Damit besteht insgesamt ein enger Rahmen, innerhalb dessen eine Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten überhaupt zulässig ist.

Eine spezielle Erlaubnisnorm im Sinne von § 4 Abs. 1 BDSG für den Umgang mit Beschäftigtendaten ist § 32 Abs. 1 BDSG (künftig Artikel 88 Abs. 1 DSGVO i.V.m. § 26 „BDSG-neu") (vgl. den folgenden Abschnitt f).

d) Einwilligung nach § 4a Abs. 1 BDSG

Gibt es keinen gesetzlichen oder kollektivrechtlichen Erlaubnistatbestand für die Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten, kommt nach § 4 Abs. 1 BDSG (künftig Artikel 6 Abs. 1 Buchstabe a) DSGVO) alternativ eine Einwilligung der Beschäftigten gemäß § 4a BDSG (künftig Artikel 7 Abs. 1 DSGVO) in Betracht. Diese kann den Umgang mit Beschäftigtendaten durch Arbeitgeber_innen legitimieren. Sie muss allerdings nach dem Wortlaut des § 4a Abs. 1 BDSG auf einer freien Entscheidung der Beschäftigten beruhen (ähnlich im Ergebnis Artikel 7 Abs. 4 DSGVO). Ob die notwendige Freiwilligkeit im Rahmen eines Arbeitsverhältnisses überhaupt gegeben sein kann, ist fraglich (Däubler 2015). Unterstellt man die Wirksamkeit von Einwilligungen entgegen der nachvollziehbaren Bedenken, obliegt der Nachweis der Freiwilligkeit im Streitfall dem Arbeitgeber/der Arbeitgeberin (Wedde 2004; zum künftigen Recht nach Artikel 7 Abs. 4 DSGVO i.V.m. § 26 Abs. 2 „BDSG-neu": Däubler 2015).

Verlangt ein Arbeitgeber/eine Arbeitgeberin eine Einwilligung zur Legitimation für die Verwendung von Beschäftigtendaten, muss er/sie die betroffenen Beschäftigten nach § 4a Abs. 1 Satz 2 BDSG insbesondere auf die vorgesehenen Zwecke der Erhebung, Verarbeitung und Nutzung hinweisen, soweit dies nach den Umständen des Einzelfalls erforderlich ist. Weiterhin muss ein Hinweis auf die Folgen der Verweigerung einer Einwilligung erfolgen. Nach § 4a Abs. 1 BDSG bedarf die Einwilligung der Schriftform.

Eine entsprechende Schriftformklausel fehlt in Artikel 7 DSGVO. Allerdings wird Arbeitgeber_innen als datenschutzrechtlich Verantwortlichen durch Artikel 7 Abs. 1 DSGVO die Beweislast dafür auferlegt, dass Beschäftigte als betroffene Personen in die Verarbeitung ihrer personenbezogenen Daten eingewilligt haben. In Umsetzung dieser Vorgabe sieht § 26 Abs. 2 Satz 2 „BDSG-neu" wiederum die Schriftform vor. Damit bleibt auch nach dem 24. Mai 2018 ein Schriftformzwang bestehen. Dabei ist zu beachten, dass schriftliche Einwilligungen nach Artikel 7 Abs. 2 DSGVO in einer klaren und einfachen Sprache abgefasst sein müssen.

Herausragende Anforderungen an eine Einwilligung werden nach § 4a Abs. 3 BDSG (künftig Artikel 9 Abs. 2 Buchstabe a) DSGVO) dann gestellt, wenn auf dieser Grundlage besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG (künftig Artikel 9 Abs. 1 DSGVO) verarbeitet werden sollen. Hierbei handelt es sich um personenbezogene Angaben zur rassischen und ethnischen Herkunft von Beschäftigten sowie zu deren politischer Meinung, zu religiösen oder philosophischen Überzeugungen, zur Gewerkschaftszugehörigkeit, zur Gesundheit oder zum Sexualleben. Eine wirksame Einwilligung muss sich ausdrücklich auf diese Daten beziehen.

Soll eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Beschäftigungsverhältnis auf eine datenschutzrechtliche Einwilligung nach § 4a BDSG (oder künftig auf Artikel 7 DSGVO) gestützt werden, verbindet sich hiermit für Arbeitgeber_innen ein grundsätzliches Risiko: Die freiwillig erteilte Einwilligung kann von den Betroffenen jederzeit widerrufen werden (ausführlich: Däubler 2015). Erfolgt ein solcher Widerruf, stellt dieser hierauf basierende Verarbeitungsprozesse im beruflichen Bereich infrage. Insoweit wird das Verfahren der Legitimation über eine Einwilligung immer dort ausscheiden, wo es um grundlegende oder herausragend wichtige Verarbeitungsprozesse geht.

(e) Betriebsvereinbarungen als Erlaubnisnorm

Fehlt eine einschlägige gesetzliche Erlaubnisnorm im Sinne von § 4 Abs. 1 BDSG, kann an deren Stelle eine normative Regelung in einer Betriebs- oder Dienstvereinbarung treten (Sassenberg/Bamber 2006; Weichert 2016). Damit eröffnet das BDSG den Betriebsparteien bereits heute die Möglichkeit, bestimmte Prozesse der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten gesetzeskonform zu legitimieren.

Allerdings ist zu beachten, dass insbesondere Betriebsräte in der Gestaltung entsprechender Betriebsvereinbarungen keineswegs frei sind. Einerseits müssen sie die einschlägigen Schutzvorgaben des Datenschutzrechts als Mindeststandard berücksichtigen. Damit scheiden kollektivrechtliche Regelungen aus, die in den Wesensgehalt des bestehenden Daten-

schutzrechts eingreifen. Beeinträchtigungen der Persönlichkeitsrechte bzw. der datenschutzrechtlichen Situation sind somit nur im verhältnismäßigen Rahmen zulässig.

Andererseits gilt es, § 75 Abs. 2 des Betriebsverfassungsgesetzes (BetrVG) zu beachten. Nach dieser Vorschrift haben Arbeitgeber/Arbeitgeberin und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer_innen zu schützen und zu fördern. Diese gesetzliche Vorgabe weist deutlich darauf hin, dass kollektivrechtliche Vereinbarungen unter Beachtung des Persönlichkeitsrechts und damit auch der datenschutzrechtlichen Vorgabe zum Schutze des Rechts auf informationelle Selbstbestimmung erfolgen müssen. Unzulässig wäre damit beispielsweise eine Betriebsvereinbarung, die dem Arbeitgeber/der Arbeitgeberin das heimliche Mithören von Telefongesprächen in Callcentern erlauben würde (BAG 1995).

Die Möglichkeit der Ausgestaltung des Beschäftigtendatenschutzes durch Betriebsvereinbarungen wird in der DSGVO nunmehr ausdrücklich gestärkt. In Artikel 88 Abs. 1 DSGVO heißt es hierzu, dass die Mitgliedstaaten spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext durch Rechtsvorschriften oder durch Kollektivvereinbarungen vorsehen können. Entsprechende Vereinbarungen wie insbesondere Betriebsvereinbarungen nach § 77 Abs. 2 BetrVG müssen nach Artikel 88 Abs. 2 DSGVO angemessene und besondere Schutzregelungen enthalten. Hierzu gehören nach dem Wortlaut der Vorschrift etwa „umfassende angemessene Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz“. Auf die Beachtung dieser Vorgaben verweist im Übrigen auch die ergänzende Regelung zur Zulässigkeit von Kollektivvereinbarungen in § 26 Abs. 4 „BDSG-neu“.

Offen bleibt angesichts der Tatsache, dass es im BetrVG kein Mitbestimmungsrecht zum Datenschutz gibt, auf welcher Rechtsgrundlage Betriebsräte die in den angesprochenen Vorschriften der DSGVO und des „BDSG-neue“ genannten Kollektivvereinbarungen durchsetzen können. Ohne ein entsprechendes Mitbestimmungsrecht können Ausgestaltungen datenschutzrechtlicher Themen allenfalls im Zusammenhang mit der Einführung oder Änderung von technischen Einrichtungen i. S. v. § 87 Abs. 1 Nr. 6 BetrVG erfolgen (BMAS 2017). Bezogen auf allgemeine Regelungen zum Datenschutz wie etwa die Ausgestaltung und Verankerung von Verschlüsselungsverfahren, von Datenlöschungskonzepten, von Datenschutzaudits oder von Regelungen zur Datenminimierung haben Betriebsräte nach dem geltenden BetrVG kein Initiativrecht und damit auch keine wirksame Durchsetzungsmacht.

(f) Beschäftigtendatenschutz nach § 32 BDSG

§ 32 Abs. 1 BDSG ist für die Verarbeitung von Beschäftigtendaten im Arbeitsverhältnis die zentrale Erlaubnisnorm im Sinne von § 4 Abs. 1 BDSDG. Nach § 32 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten der Beschäftigten im Bewerbungsverfahren, während der Durchführung von Beschäftigungsverhältnissen sowie nach deren Ende im Rahmen des Erforderlichen zulässig. Bei der Prüfung der Erforderlichkeit ist mit Blick auf die Persönlichkeitsrechte der Beschäftigten ein strenger Maßstab anzulegen. Erlaubt ist nicht etwa all das, was Arbeitgeber_innen für sinnvoll und hilfreich halten. Ihre Verarbeitungsbefugnisse werden vielmehr durch das aus objektiver Sicht für die Durchführung des Arbeitsverhältnisses Notwendige begrenzt. Maßstab ist neben der Erforderlichkeit die Verhältnismäßigkeit angestrebter Erhebungen, Verarbeitungen und Nutzungen. Arbeitgeber_innen sind in diesem Rahmen beispielsweise befugt, die Adressen, Bankverbindungen, Informationen zur Berufsausbildung oder das Vorhandensein von Führerscheinen bei ihren Beschäftigten abzufragen. Unzulässig ist hingegen beispielsweise die Erhebung und Verarbeitung von Freizeitaktivitäten oder Hobbys der Beschäftigten, deren privaten Telefonnummern oder E-Mail-Adressen oder auch die Frage nach einem privaten Account in sozialen Medien und den dort enthaltenen Daten. Damit wäre es auch unzulässig, wenn Arbeitgeber_innen oder Vorgesetzte von Beschäftigten verlangen, sie als „Freund“ in einem sozialen Netzwerk zu akzeptieren.

Der Rahmen des nach § 32 Abs. 1 BDSG Zulässigen ist eng gefasst. Diese Aussage gilt neben bereits bestehenden Beschäftigungsverhältnissen auch bezogen auf die Bewerbungsphase, in der ebenfalls nur objektiv erforderliche Informationen erhoben werden dürfen (Däubler 2016).

An dieser aktuellen datenschutzrechtlichen Situation wird auch das „BDSG-neu“ nichts Grundlegendes ändern. Die in § 26 „BDSG-neu“ enthaltene Regelung zur „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses“ fasst lediglich die im BDSG an verschiedenen Stellen enthaltenen Definitionen und Vorschriften zusammen, die sich auf Beschäftigte beziehen. Darüber hinaus führt sie Regelungen der DSGVO wieder auf das Niveau des BDSG zurück wie etwa durch die Verankerung der Schriftform für Einwilligungen in § 26 Abs. 2 Satz 2 „BDSG-neu“. Eine Reihe von praxisrelevanten Themen wie etwa das Fragerecht im Bewerbungsverfahren, den Ausschluss heimlicher Kontrollen im Beschäftigungsverhältnis, die Begrenzung der Lokalisierung von Beschäftigten, ein Verbot der Erstellung von umfassenden Bewegungsprofilen, den Ausschluss von Dauerüberwachungen oder die Zulässigkeit der Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken lässt der Gesetzgeber in dieser neuen Vorschrift allerdings ausdrücklich offen (Deutscher Bundestag 2017: 97). Das bedeutet praktisch, dass wichtige Themen des Beschäftigtendatenschutzes weiterhin ohne die notwendige spezialgesetzliche Regelung sind.

(g) Berechtigte Interessen von Arbeitgeber_innen

Bezogen auf die nach § 4 Abs. 1 BDSG (künftig Artikel 6 Abs. 1 DSGVO) erforderlichen gesetzlichen Erlaubnistatbestände ist in der juristischen Diskussion strittig, ob der Arbeitgeber/die Arbeitgeberin über den von § 32 Abs. 1 BDSG (§ 26 „BDSG-neu“) vorgegebenen engen Rahmen hinaus weitere Daten auf der Grundlage von § 28 Abs. 1 Satz 1 Nr. 2 BDSG (künftig Artikel 6 Abs. 1 Buchstabe f) DSGVO) erheben kann.

Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten sowie ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist. Aus diesem Wortlaut wird die Auffassung abgeleitet, dass die Vorschrift parallel zu § 32 Abs. 1 BDSG zur Anwendung kommt (Taeger 2013). Dieser Auffassung wird entgegengehalten, dass § 32 als Spezialnorm die allgemeine Regelung in § 28 Abs. 1 Satz 1 Nr. 2 BDSG verdrängt und dass zudem die letztgenannte Vorschrift kein allgemeiner Auffangtatbestand ist (Seifert 2014; Simitis 2014a). Ist die letztgenannte Auffassung zutreffend, käme eine Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten außerhalb des durch § 32 Abs. 1 BDSG vorgegebenen Bereichs der Erforderlichkeit überhaupt nur dann in Betracht, wenn es um berechtigte Interessen einer verantwortlichen Stelle geht, die ohne Bezug zur Durchführung von Beschäftigungsverhältnissen sind bzw. die über das individuelle Arbeitsverhältnis hinausgehen. In Betracht käme etwa der geplante Verkauf eines Unternehmens. In diesen Fällen könnte eine Bewertung der „Belegschaftssituation" im Rahmen von sogenannten „Due-Dilligence-Prüfungen" die auf diese Prüfzwecke beschränkte Verarbeitung individueller Beschäftigtendaten beinhalten. In diesen Fällen wäre allerdings vor der Durchführung von Verarbeitungsprozessen zu prüfen, ob berechtigte Zwecke nicht auch auf der Basis pseudonymisierter oder anonymisierter Informationen erfüllt werden können (Wedde 2016b; Wedde 2014).

Anders stellt sich die Situation dar, wenn die Anwendbarkeit von § 28 Abs. 1 Satz 1 Nr. 2 BDSG neben der Spezialnorm des § 32 Abs. 1 BDSG auf Beschäftigtenverhältnisse gegeben wäre. Dann stünde die Möglichkeit einer Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten indes unter dem Vorbehalt, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung nicht offensichtlich überwiegen. Dies wäre wahrscheinlich der Fall, wenn aus Sicht der verantwortlichen Stelle erhebliche, sofort ins Auge springende Umstände ersichtlich wären, die eine Beeinträchtigung der schutzwürdigen Interessen nahelegen würden (Wolff/Brink 2015: 71). Aus dieser im Rahmen einer Verhältnismäßigkeitsprüfung zu beachtenden Begrenzung leitet sich ab, dass auf eine Legitimation der Datenverarbeitung durch § 28 Abs. 1 Satz 1 Nr. 1 BDSG immer dann verzichtet werden muss, wenn ein Unterlaufen der durch § 32 Abs. 1 Satz 1 vorgegebenen Erforderlichkeit unterstellt oder vermutet werden kann. Dies setzt der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten auf der Basis dieser Vorschrift als datenschutzrechtlicher Erlaubnisnorm sehr enge Grenzen.

Das angesprochene Überwiegen der schutzwürdigen Interessen der Betroffenen am Ausschluss der Verarbeitung ist insbesondere dann anzunehmen, wenn ein Arbeitgeber/eine Arbeitgeberin über das in § 32 Abs. 1 Satz 1 BDSG genannte Maß der Erforderlichkeit hinaus besondere Arten personenbezogener Daten wie etwa Informationen zum Gesundheitszustand von Beschäftigten sammeln will – etwa durch die Ausgabe von Fitnessarmbändern an die Belegschaft und eine hiermit geplante zentrale Verarbeitung von Bewegungsdaten in einem zentralen Rechnersystem. Gleiches gilt für den Einsatz leistungsfähiger biometrischer Zugangskontrollsysteme, die etwa auf der Grundlage von Iris-Scans arbeiten. Auch diese lassen sich allenfalls für Arbeitsplätze mit herausragendem Schutzbedarf rechtfertigen, bei denen der Zutritt Unbefugter mit an 100 Prozent grenzender Sicherheit ausgeschlossen werden muss, nicht aber für durchschnittliche Tätigkeiten in Büros oder Produktionsbereichen.

Die vorstehend beschriebene datenschutzrechtliche Situation findet sich nahezu identisch in Artikel 6 Abs. 1 Buchstabe f) DSGVO bzw. in § 26 Abs. 1 „BDSG-neu" wieder. Damit besteht die vorstehend beschriebene rechtliche Situation ebenso fort wie die sich hiermit verbindenden Auslegungsprobleme.

(h) Möglichkeiten und Grenzen des Beschäftigtendatenschutzes

Der Umfang des für den Bereich des Beschäftigtendatenschutzrechts datenschutzrechtlichen Zulässigen ist insgesamt eng gefasst. Mit Blick auf das allgemeine datenschutzrechtliche Gebot der Datenminimierung, dass sowohl in § 3a BDSG wie auch in Artikel 5 Abs. 1 DSGVO postuliert ist, muss sich die Verarbeitung und Nutzung von Informationen über Beschäftigte durch Arbeitgeber_innen auf Daten beschränken, die unter Wahrung schutzwürdiger Interessen der Betroffenen erhoben wurden und die für die Begründung, Durchführung und Beendigung erforderlich sind. Zudem muss bei der Erhebung jeweils der Zweck klar festgelegt worden sein. Unzulässig ist es hingegen, alle für Arbeitgeber_innen zugänglichen Informationen „auf Vorrat" zu sammeln.

Diese datenschutzrechtliche Situation setzt allen denkbaren Formen Big-Data-Auswertungen für Beschäftigtendaten klare Grenzen. Für die hierfür notwendige Verarbeitung von Daten auf Vorrat ohne konkret festgelegte Zweckfestlegung gibt es weder im aktuellen BDSG noch im künftigen europäischen Recht eine datenschutzrechtliche Legitimation.

Im Beschäftigungsverhältnis ist damit datenschutz- wie arbeitsrechtlich nicht etwa alles erlaubt, was technisch möglich ist, sondern nur das, was Persönlichkeitsrechte der Beschäftigten hinreichend wahrt und beachtet. Diese Position bestätigt die Rechtsprechung in einschlägigen Entscheidungen zur Zulässigkeit von Kontrollen von Beschäftigten bzw. zu deren Grenzen. So wird beispielsweise vom Bundesarbeitsgericht in ständiger Rechtsprechung die Position vertreten, dass beim Einsatz technischer Einrichtungen wie etwa durch Videokameras regelmäßig keine Totalüberwachung der Beschäftigten erfolgen darf (BAG 2003; BAG 2016a). Nach Auffassung des Bundesarbeitsgerichts muss sich die Zulässigkeit von Kontrollen der Arbeitgeber_innen mittels technischer Einrichtungen am sogenannten Ultima-Ratio-Prinzip orientieren: Hiernach müssen Arbeitgeber_innen, denen mehrere Kontroll- und Überwachungsmöglichkeiten zur Verfügung stehen, hiervon die auswählen, die am wenigsten in Persönlichkeitsrechte der Beschäftigten eingreift (BAG 2004). Vorratsdatenspeicherungen sind auch unter Beachtung dieser Vorgabe unzulässig.

3.2 DER RAHMEN FÜR DIE ARBEIT VON BETRIEBS- UND PERSONALRÄTEN IN DER DIGITALISIERTEN ARBEITSWELT

Personal- und Betriebsräten fällt bei Digitalisierung bezogen auf die Ausgestaltung von Schutzmechanismen für Beschäftigte sowie bei der Festlegung von Grenzen der IT-Nutzung eine herausragende Rolle zu. Dies folgt schon daraus, dass Beschäftigten selbst einerseits nur begrenzte Möglichkeiten zur Sicherung ihrer Persönlichkeitsrechte zur Verfügung stehen und dass andererseits die Wahrnehmung datenschutzrechtlicher Handlungsmöglichkeiten in einem abhängigen Beschäftigungsverhältnis nur begrenzt realisierbar ist.

Welche Spielräume zugunsten von Betriebs- und Personalräten bestehen, wird im Folgenden exemplarisch für den Bereich des BetrVG beschrieben. Eine Ausweitung der Beschreibung für den Bereich des Personalvertretungsrechts auf Bundes- und Landesebene unterbleibt an dieser Stelle aus Raumgründen.

(a) Grenzen der Mitbestimmung

Betriebsräten stehen bezogen auf die Digitalisierung bei der Ausführung des durch das BetrVG vorgegebenen Mitwirkungs- und Mitbestimmungsrahmens die allgemeinen Rechte und Möglichkeiten zur Verfügung, die das aus dem Jahr 1972 stammende Gesetz bereithält. Diese Datierung verweist auf ein grundlegendes Strukturproblem: Der kollektivrechtliche Regelungsrahmen des BetrVG zielte bei seiner Schaffung vor mehr als 40 Jahren auf eine Arbeitswelt, in der die digitalisierten Prozesse und Techniken von heute und die hieraus erwachsenden Arbeitsmöglichkeiten auch nicht nur ansatzweise erkennbar waren. So wurde beispielsweise das Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG, das sich auf die Einführung und Anwendung von technischen Einrichtungen zur Verhaltens- und Leistungskontrolle bezieht, zur Regelung von Problemen geschaffen, die im Zusammenhang mit sogenannten „Produktografen" oder „Multimomentkameras" gesehen wurden (Klebe 2016).

Die Kontrollmöglichkeiten, die Hard- und Software heute in der digitalen Arbeitswelt bieten, standen 1972 nicht auch nur ansatzweise im Fokus dieser Gesetzgebung. Dass § 87 Abs. 1 Nr. 6 BetrVG bis heute dennoch der zentrale Mitbestimmungstatbestand für die kollektivrechtliche Regelung von Verhaltens- und Leistungskontrollen geblieben ist, die sich etwa mit SaaS-Konzepten oder mit der betrieblichen Nutzung von sozialen Netzwerken wie Facebook verbinden, verdankt die Vorschrift ihrer Fortschreibung durch die Rechtsprechung. Diese hat den Regelungsgehalt und Regelungsrahmen von § 87 Abs. 1 Nr. 6 BetrVG immer wieder in Übereinstimmung mit der technischen Entwicklung gebracht (BAG 2016b).

Allerdings führt das Auseinanderfallen der im BetrVG ursprünglich geregelten Sachverhalte und der betrieblichen Wirklichkeit immer öfter zu Umsetzungsproblemen. Das lässt sich etwa am Geltungsbereich des Gesetzes demonstrieren: Dieses beschränkt sich im Rahmen des sogenannten Territorialitätsprinzips (Trümner 2016) auf den Bereich der Bundesrepublik Deutschland. Die Mitbestimmung nach dem BetrVG endet damit an den nationalen Grenzen Deutschlands, während das digitale Handeln von Unternehmen und Konzernen und die hierfür erforderlichen technischen Grundlagen längst globaler erfolgen und auf geografische Grenzlegung keine Rücksicht mehr nehmen.

Die durch das Territorialitätsprinzip gezogenen Grenzen stellen aus Sicht von Betriebsräten nicht nur bezogen auf multinationale Unternehmen und Konzerne ein Problem dar. Auch in mittelständischen Unternehmen ist es inzwischen vielfach üblich, grenzüberschreitend zu agieren, etwa bei der Nutzung von Cloud-Computing, von SaaS-Anwendungen oder beim Rückgriff auf Cloud- oder Crowdworking. Die rechtlichen Möglichkeiten von Betriebsräten enden aber weiterhin an den geografischen Grenzen der Bundesrepublik.

Grenzüberschreitende Digitalisierung führt damit aus kollektivrechtlicher Sicht in der Praxis zu deutlichen Einschränkungen der gesetzlichen Mitwirkungs- und Mitbestimmungsrechte und damit zu einer Reduzierung der Handlungsmöglichkeiten von Betriebsräten. Betriebsräte müssen sich in dieser Situation darauf beschränken, ihre im Anwendungsbereich des BetrVG verbleibenden Mitbestimmungsrechte für Regelungen zu verwenden, die mittelbar auch die Bedingungen des Umgangs mit Beschäftigtendaten außerhalb Deutschlands im Sinne der Beschäftigten positiv beeinflussen.

(b) Gestaltungsspielräume

Eine herausragende Bedeutung kommt in diesem Zusammenhang dem schon angesprochenen Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG zu. Hiernach hat der Betriebsrat mitzubestimmen bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer_innen zu überwachen. Im Rahmen dieses Mitbestimmungsrechts können Betriebsräte vom Arbeitgeber_innen auch die Einhaltung einschlägiger gesetzlicher Vorgaben verlangen, die bezogen auf den Datenschutz der Beschäftigten insbesondere im BDSG zu finden sind. Darüber hinaus können sie gemäß der Zielrichtung des Mitbestimmungsrechts an der Ausgestaltung von einschlägigen technischen Einrichtungen mit dem Ziel mitwirken, unzulässige Kontrollen von Beschäftigten ganz auszuschließen oder auf ein Minimum zu beschränken. Durch eine entsprechende Ausgestaltung von Betriebsvereinbarungen können Arbeitgeber_innen dabei auch verpflichtet werden, vereinbarte Standards auch bezogen auf die Verarbeitung außerhalb des Anwendungsbereichs des BetrVG sicherzustellen, etwa durch die Ausgestaltung von Verträgen zur Auftragsdatenverarbeitung gemäß § 11 BDSG (künftig Artikel 28 DSGVO).

Entgrenzungstendenzen, die etwa bei mobiler Arbeit drohen, können Betriebsräte unter Rückgriff auf das Mitbestimmungsrecht in § 87 Abs. 1 Nr. 2 und 3 BetrVG entgegenwirken, indem etwa Arbeitszeitfenster oder Mindestpausen festgeschrieben werden. Darüber hinaus können auf der Grundlage des Mitbestimmungsrechts in § 87 Abs. 1 Nr. 7 BetrVG auf die besonderen Arbeitsbedingungen von mobil tätigen Beschäftigten bezogene Regelungen zur Verhütung von Arbeitsunfällen oder zum Gesundheitsschutz durchgesetzt werden.

Bezogen auf die Datenerhebung bei Beschäftigten ist das Zustimmungsrecht in § 94 Abs. 1 bezüglich des Inhalts von

Personalfragebögen einschlägig. Auf dieser Grundlage können Betriebsräte an der Ausgestaltung von Verfahren der Datenerhebung bei Beschäftigten mitreden. Sie können darauf drängen, dass grundlegende datenschutzrechtliche Vorgaben wie etwa die in § 3a BDSG enthaltene Datenvermeidung oder Datensparsamkeit berücksichtigt werden.

Bezogen auf die Qualifizierung von Beschäftigten für die Anforderung der digitalisierten Arbeit kommt den Mitwirkungs- und Mitbestimmungsrechten für den Bereich der Berufsbildung in den §§ 96 bis 98 BetrVG eine besondere Bedeutung zu. Auch wenn in dieser Vorschrift durchsetzbare Mitbestimmungsrechte nur teilweise enthalten sind, eröffnen diese Regelungen Betriebsräten die Möglichkeit, auf eine adäquate Qualifikation der Beschäftigten hinzuwirken, die insbesondere auch den Bereich des Datenschutzes und der Datensicherheit erfasst.

4

BETRIEBLICHE PRAXIS

4.1 IGNORANZ ALS REGELFALL?

Die rechtlichen Vorgaben, die es für den Bereich des Beschäftigtendatenschutzes in der digitalisierten Welt gibt, aber auch die Grenzen für die Erhebung, Verarbeitung und Nutzung dieser Daten, sind inhaltlich eigentlich sehr klar und eindeutig. Dies gilt ebenso für die Regeln des BDSG wie für die einschlägigen neuen Vorschriften in der DSGVO bzw. im „BDSG-neu". Beide Regelungswerke sind beispielsweise gleichermaßen als Verbotsgesetze mit Erlaubnistatbeständen ausgestaltet.

Vor dem Hintergrund einer klaren und eindeutigen Gesetzessituation überrascht es, dass eine Reihe von Arbeitgeber_innen nicht weiß, was mit den aktuell geltenden datenschutzrechtlichen Normen anzufangen ist. Datenschutz wird in der betrieblichen Praxis teilweise als Behinderung der eigenen Gestaltungs- und Organisationsmöglichkeiten angesehen. Folglich werden datenschutzwidrige Ausgestaltungen von Prozessen, Verfahren oder Abläufen nicht behoben und vielfach einfach ignoriert. An dieser Situation wird auch das neue europäische Datenschutzrecht vermutlich nichts Grundlegendes ändern.

Wo Ignoranz aufgrund einer offenkundigen Diskrepanz zwischen betrieblicher Realität und gesetzlichen Rahmenbedingungen nicht mehr möglich ist, wird geltendes Datenschutzrecht als nicht mehr zeitgemäß oder als überzogen qualifiziert. So hat Bundeskanzlerin Merkel jüngst vor einem überzogenen Datenschutz gewarnt und für einen Abschied vom Prinzip der Datensparsamkeit plädiert (Neuerer 2017). Logische Konsequenz dieses Denkmusters ist die Forderung an den Gesetzgeber, die unter Missachtung einschlägiger Schutznormen selbst geschaffene neue Realität durch eine Anpassung des Datenschutzrechts wiederherzustellen. Als Alternative zum „Datenschutz" wird „Datenvielfalt" gefordert. Vor dem Hintergrund einer klaren datenschutzrechtlichen Situation ist das in etwa so, als ob Autofahrer_innen, die in einer 30er-Zone mehrfach geblitzt worden sind, die drastische Erhöhung der hier zulässigen Höchstgeschwindigkeit fordern würden.

Ob die festzustellende Ignoranz gegenüber zwingenden datenschutzrechtlichen Vorgaben ein zukunftsfähiges Modell ist, bleibt allerdings mit Blick auf die neuen Sanktionsmöglichkeiten, die die DSGVO enthält, abzuwarten. Nach Artikel 83 Abs. 5 DSGVO müssen Verantwortliche ab dem 25.5.2018 im Extremfall mit Geldbußen von bis 20 Millionen Euro bzw. von bis zu vier Prozent des weltweit im Vorjahr erzielten Jahresumsatzes rechnen, je nachdem, welcher Betrag höher ist. Dass die Geldbußen im konkreten Fall nicht niedrig ausfallen dürfen, folgt aus der Vorgabe in Artikel 83 Abs. 1 DSGVO, nach der die Verhängung der Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein soll.

4.2 BIG BROTHER AUF JEDEM SCHREIBTISCH?

Die Kommunikation per E-Mail wird gerade neu erfunden. Auf vielen Bildschirmen wird diese Form der Kommunikation durch interne soziale Netzwerke ersetzt (Greve 2016; Greve/Wedde 2014; Rozek 2015; Wedde 2015). Hierbei handelt es sich um „Facebook-artige" Kommunikationsoberflächen, die nicht nur den schnellen Informationsaustausch innerhalb definierter Arbeitsgruppen ermöglicht, sondern beispielsweise auch die gemeinsame Bearbeitung von Dokumenten, die jederzeitige Durchführung von Audio- und Videokonferenzen von stationären oder mobilen Endgeräten aus oder die Verteilung und Kontrolle von Arbeitserledigungen. Interne soziale Netzwerke ermöglichen schnelle Kommunikationsformen und kooperatives Arbeiten.

Interne soziale Netzwerke machen aber auch die individuelle Arbeit für Beschäftigte in einer neuen Art und Weise transparent. Diese Feststellung gilt insbesondere für konventionelle Messmethoden wie die Erfassung von Beginn und Ende einer Aufgabenerledigung durch einen „Timestamp", d. h. für die sekundengenaue Erfassung von Datum und Uhrzeit. Derartige elektronische Markierungen werden in internen sozialen Netzwerken standardmäßig vergeben. Damit bleibt über einen langen Zeitraum nachvollziehbar, wie lang es etwa gedauert hat, ehe ein Beschäftigter auf eine Anfrage reagiert hat, oder wie viel Zeit für die Erledigung einer Aufgabe gebraucht wird. Dies ist mit Blick auf den Beschäftigtendatenschutz problematisch, zumal die „Timestamps" vielfach nicht löschbar sind und langfristig zu unterschiedlichen Zwecken ausgewertet werden können.

Allerdings gehören diese konventionellen Messmethoden beinahe schon der Vergangenheit an. Inzwischen zeichnet sich gerade in internen sozialen Netzwerken eine neue Messmethode ab, die unter dem Stichwort „Mining the social graph" diskutiert wird (Höller 2016: 8). Hierbei handelt es sich um die Auswertung vorhandener Daten und Datenmengen mittels geeigneter Big-Data-Software. Angestrebt wird im arbeitsrechtlichen Bereich etwa, dass Muster im Handeln von Beschäftigten erkennbar werden (etwa eine Kündigungsabsicht, vgl. dazu den folgenden Abschnitt), die sich verallgemeinern lassen. Folgt dann das Handeln einzelner Beschäftigter dem identifizierten Muster, informiert die Software die Vorgesetzten oder die Personalabteilung.

Entsprechende Techniken beinhalten eine neue Dimension der Kontrolle von Beschäftigten. Besonders problematisch ist, dass zwar die Programmierer von Big-Data-Software wissen, welcher Algorithmus für diese Software verwendet wird und welche Muster analysiert werden, nicht aber die von den Auswertungen direkt betroffenen Beschäftigten. Dies führt zu einer Disparität, die unmittelbar auch auf Kosten von Persönlichkeitsrechten von Beschäftigten geht. Eine belastbare datenschutzrechtliche Grundlage für eine solche Form der Vorratsdatenerfassung und -auswertung gibt es im Regelfall nicht.

Problematisch ist mit Blick auf die angesprochenen Big-Data-Anwendungen auch, dass sie hervorragend zur Lösung von Anforderungen geeignet scheinen, die in der betrieblichen Praxis umstritten sind. Hierzu gehört beispielsweise die betriebliche Umsetzung der Anforderungen, die sich für Arbeitgeber_innen aus den EU-Antiterrorverordnungen und den zugehörigen Sanktionslisten ableiten (Däubler-Gmelin 2014; Wedde 2016c). Mittels Big-Data-Anwendungen könnten nicht nur Personaldatenbanken bezüglich ihrer Übereinstimmung mit den Sanktionslisten überprüft werden. Darüber hinaus wäre es auch möglich, ganz allgemein nach entsprechend verdächtigen Verhaltensweisen zu suchen. Ähnliches gilt bezüglich der Verwendung für Compliance-Zwecke.[3] Big Data würde es möglich machen, Verstöße gegen Compliance-Vorgaben flächendeckend zu erkennen und zu bewerten. Schließlich lassen sich Big-Data-Analysen auch optimal in betriebliche Sicherheitskonzepte integrieren, etwa um potenzielle interne Angreifer_innen anhand von allgemeinen Verhaltensmuster zu identifizieren.

4.3 VERDICHTUNG DER ARBEIT UND ZUNAHME VON KONTROLLEN

Die Digitalisierung der Arbeit zielt vorrangig auf die Effektivierung von Arbeitsprozessen. Eine Folge ist, dass Arbeit in Verwaltungen, Dienstleistungen oder Produktionen sowohl rationeller als auch kompensierter abläuft. Diese Verdichtung der Arbeit führt nicht nur zu einer Erhöhung der individuellen Leistungsanforderungen, sondern auch zu einer Zunahme individueller Leistungskontrollen. Im Ergebnis nimmt damit nicht nur das Volumen von Datenerhebungen und -verarbeitungen zu, sondern auch die Zahl der Eingriffe in datenschutzrechtliche Schutztatbestände.

(a) Die Praxis

Erkennbar ist dieser Effekt beispielsweise im Logistikbereich. Dort werden Kundenbestellungen in vielen Großlagern von sogenannten „Pickern" erledigt. Dieser Begriff steht für Beschäftigte, die unter permanenter Anleitung und Kontrolle von zentralen IT-Systemen arbeiten. Eigentlich handelt es sich bei „Pickern" um das „verdrahtete Frontend" der Logistikcomputer.

Praktisch läuft die Arbeit in diesen Logistikzentren so ab, dass den „Pickern" über eine Computerstimme per Kopfhörer oder durch eine Anzeige über ein am Körper getragenes Display mitgeteilt wird, in welchen Regalfächern die bestellten Gegenstände zu finden sind (Siebenhüter 2016). Dabei berechnet ein zentrales Computersystem den kürzesten bzw. optimalsten Weg zwischen den einzelnen Lagerorten und leitet hieraus präzise Routenanweisungen ab. Die Informationen über den aktuellen Aufenthaltsort von Beschäftigten im Lager erhält das System von „GPS-Komponenten", die in die am Körper getragenen Geräte integriert sind. Da zudem jede Entnahme aus einem Fach unmittelbar registriert wird, lässt sich sekundengenau nachvollziehen, was einzelne Beschäftigte gerade tun, wo sie sich befinden oder wie schnell sie sich im Lager bewegen.

Weicht das Handeln einzelner „Picker" von den programmierten Vorgaben ab, wird dies vom System unmittelbar registriert und ggf. für Vorgesetzte durch eine „Alarmmeldung" wahrnehmbar gemacht. Gleiches gilt für eine Abweichung der individuellen Arbeitsgeschwindigkeit von bestimmten Soll-Vorgaben. „Picker" befinden sich damit im Ergebnis in einer Art „Dauerakkord". Für kleine Freiheiten, die es früher bei entsprechenden Tätigkeiten gab, wie etwa ein kurzes Gespräch mit Kolleg_innen oder eine kleine Trink- oder Verschnaufpause bleibt in vollständig durchorganisierten Systemen keine Zeit mehr.

Ähnliche Entwicklungen gibt es auch im Bereich der klassischen Verwaltung. Auch hier wird die Arbeitserbringung bereits vielfach direkt von digitalen Systemen gesteuert und kontrolliert. So erfolgt die Fallbearbeitung bei Versicherungen inzwischen längst auf der Grundlage präziser zeitlicher wie inhaltlicher Vorgaben. Weichen benötigte Bearbeitungszeiten oder getroffene Entscheidungen von diesen Vorgaben ab, löst dies Hinweise an Vorgesetzte aus. Der individuelle Handlungsspielraum der Beschäftigten wird so auf ein Minimum reduziert.

Nicht viel anders ergeht es Beschäftigten in digitalisierten Produktionsbereichen. Sie müssen sich im Regelfall an jeder benutzten Maschine persönlich anmelden. Sind die Maschinen über eine zentrale Produktionssteuerung vernetzt, ist es möglich, jeden Arbeitsschritt, jeden Handgriff oder jede Rüstzeit zentral zu erheben, zu analysieren und auszuwerten. Das dabei entstehende Handlungsprofil der einzelnen Beschäftigten lässt sich anschließend elektronisch sowohl mit Standardvorgaben als auch mit den Werten anderer Beschäftigter vergleichen.

Bei allen diesen unterschiedlichen Formen der Steuerung und der damit verbundenen Kontrolle fällt eine kaum noch überschaubare Menge personenbezogener Daten über einzelne Beschäftigte an. Diese Daten können mittels der bereits angesprochenen Big-Data-Anwendungen ausgewertet werden.

---

3 Der Begriff „Compliance" steht für die Einhaltung aller einschlägigen Gesetze und sonstigen Vorschriften sowie für die Beachtung interner Richtlinien und Vorgaben (Mert 2016: 18; Wedde 2016d: 8).

(b) Datenschutzkonformität

Alle vorstehenden Beispiele sind aus datenschutzrechtlicher Sicht bedenklich. Dies folgt bereits daraus, dass hierbei allgemeine Grundsätze wie etwa die gemäß § 3a BDSG bestehende Notwendigkeit der Datenvermeidung bzw. Datensparsamkeit nicht gewahrt werden oder weil das in § 32 Abs. 1 Satz 1 BDSG enthaltene Gebot der Erforderlichkeit einer Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten für die Durchführung eines Beschäftigungsverhältnisses nicht gesetzeskonform umgesetzt wird. Aber auch der Grundsatz, dass alle nicht mehr für den eigentlichen Zweck erforderlichen personenbezogenen Daten nach § 35 Abs. 2 Nr. 1 BDSG zu löschen sind, wenn ihre Speicherung mangels datenschutzrechtlicher Erlaubnisgrundlage unzulässig ist, wird von entsprechenden Systemen bzw. von deren Betreibern vielfach ignoriert. So entsteht eine Situation, in der betriebliche Gestaltungen nicht mehr mit zwingenden datenschutzrechtlichen Vorgaben übereinstimmen. Diese Situation wird möglicherweise durch die verbesserten Datenschutzregelungen noch verstärkt, die die DSGVO enthält. Das neue europaweit einheitliche Datenschutzrecht misst etwa mit der Bekräftigung des Grundsatzes der Datenminimierung in Artikel 5 Abs. 1 Buchstabe c) DSGVO dem Gedanken der Datenvermeidung und der Datensparsamkeit eine noch größere Bedeutung zu, als es das BDSG derzeit tut. Hinzu kommt beispielsweise die durch Artikel 17 DSGVO ausgeweitete Verpflichtung zur Datenlöschung. Das dort enthaltene „Recht auf Vergessenwerden" können auch Beschäftigte für sich gegenüber ihrem Arbeitgeber/ihrer Arbeitgeberin in Anspruch nehmen.

4.4 KONTROLLEN VON BESCHÄFTIGTEN – DIE ZUKUNFT

Neue IT-Techniken wie insbesondere Big-Data- und Data-Mining-Anwendungen ermöglichen neue Kontrollformen. Dabei geht es gar nicht mehr primär darum, das Verhalten einzelner Beschäftigter sekundengenau zu überwachen und zu kontrollieren. Die neuen Formen der Überwachung zielen vielmehr darauf, Abweichungen des individuellen Arbeitsverhaltens vom „Normalverhalten" aller Beschäftigten zu erkennen und hierauf zu reagieren. Dabei fließen neben aktuellen Informationen über einzelne Beschäftigte auch solche aus der Vergangenheit in die Datenbasis ein.

Dafür ein Beispiel, das sich an tatsächliche Gegebenheiten anlehnt: In einem Unternehmen wird mittels entsprechender Big-Data-Software auf der Grundlage aller vorhandenen personenbezogenen Daten analysiert, wie sich das Verhalten von Beschäftigten, die ihren Arbeitsvertrag gekündigt haben, im Vorfeld dieser Kündigung verändert. Bezogen auf Produktionsmitarbeiter_innen ist dabei aufgefallen, dass sich sowohl das Tempo der Arbeitserledigung als auch die Qualität der Arbeit in der Phase vor der Kündigung verändert haben. Hinzu gekommen ist beispielsweise eine Zunahme von Toilettengängen und deren Dauer, die vom System aus der Tatsache der Abwesenheit vom Arbeitsplatz sowie aus den Daten des Türöffners zur gesicherten Abteilung abgeleitet wurden. Teilweise wurde auch eine Zunahme der Krankheitstage identifiziert. Bezogen auf Verwaltungsmitarbeiter_innen wurde analysiert, dass sie in der Phase vor der Kündigung ihre Gleitzeitpolster gezielt abbauten, weniger E-Mails weiterleiteten, ihre dienstlichen E-Mails deutlich kürzer wurden und sich die auf einzelne E-Mails bezogenen Lesezeiten deutlich verringerten. Alle diese Informationen werden in einem Big-Data-System als „Maßstab" verwendet. Stimmt dieser mit dem tatsächlichen Verhalten eines Beschäftigten überein, erzeugt das System automatisch einen entsprechenden Hinweis. Arbeitgeber_innen können daraufhin für sie wichtige Arbeitnehmer_innen, bei denen Abwanderungsgedanken prognostiziert werden, durch gezielte Förderungsmaßnahmen von einer Kündigung abbringen. Bei als nicht so wichtig eingeschätzten Arbeitnehmer_innen kann der Arbeitgeber/die Arbeitgeberin den Schritt hin zu einer Eigenkündigung durch fantasievolle Veränderungen der individuellen Arbeitsbedingungen fördern.

Dieses Beispiel ist teilweise (noch) fiktiv. Die für seine praktische Umsetzung erforderliche Software steht aber längst zur Verfügung und wird in Teilen bereits genutzt. So werden beispielsweise mittels Standardsoftware aus dem Bereich der Personalverwaltung (etwa in „Workday"), aber auch von Anwendungen aus dem Bereich „Social Graph" (etwa im „Office Graph" des Microsoft-Software-Pakets „Office 365") entsprechende Daten über Beschäftigte gesammelt und mit geeigneten Algorithmen ausgewertet (vgl. bezogen auf „Workday" entsprechende Hinweise des deutschen Geschäftsführers der Firma in FAZ.NET 2016). Über die konkreten Ergebnisse und Erkenntnisse, die in der Software vorhanden sind und damit Arbeitgeber_innen grundsätzlich zur Verfügung stehen, werden im Regelfall weder die Beschäftigten noch ihre betrieblichen Interessenvertreter_innen informiert. Aber auch viele Arbeitgeber_innen wissen vermutlich nicht genau, welche Informationsdichte die verwendeten Algorithmen erzeugen bzw. welche Erkenntnisse die Anbieter der Software über „Rückkanäle" erlangen können.

Aus datenschutzrechtlicher Sicht ist dies schon deshalb problematisch, weil sich die im Beispiel beschriebene neue Form der Datenverarbeitung nicht mehr an einem konkreten Zweck orientiert. Stattdessen erfolgt eine zweckfreie vom ursprünglichen Zweck der Erhebung getrennte Auswertung und Aufbereitung von Informationen. Diese Situation steht im Widerspruch zur grundlegenden datenschutzrechtlichen Vorgabe einer engen Zweckbindung, die sowohl im BDSG (§ 28 Abs. 1 Satz 2 BDSG bzw. § 4 Abs. 3 BDSG) als auch in der DSGVO (Artikel 5 Abs. 1 Buchstabe b DSGVO bzw. Artikel 13 Abs. 1 Buchstabe c) DSGVO) enthalten ist.

Schon dieser offenkundige Mangel der Datenschutzkonformität weckt Zweifel daran, dass es für die Umsetzung der angesprochenen technischen Möglichkeiten eine belastbare datenschutzrechtliche Grundlage gibt. Hinzu kommt, dass es mit Blick auf die Persönlichkeitsrechte der Betroffenen ganz allgemein problematisch ist, dass Beschäftigte in der Regel nicht wissen, welche Informationen über sie in der eingesetzten Big-Data-Software enthalten sind und welche Algorithmen benutzt werden, um ihr individuelles Verhalten zu bewerten. Zudem fällt es ihnen in der Regel schwer, die Zusammenhänge zu sehen und die Schlussfolgerungen in einer Form herzustellen, wie dies technische Systeme auf der Grundlage zahlreicher Parallelfälle und ausgeklügelter Analysesoftware können.

Allerdings ist es durchaus fraglich, ob die Bewertung der angesprochenen Big-Data-Systeme künftig überhaupt noch ein datenschutzrechtliches Thema sein wird. Der Grund für diese Frage besteht darin, dass diese Systeme die vorhandenen persönlichen Daten vielfach in aggregierte Informationen oder Metadaten umwandeln, die über keinen unmittelbaren Personenbezug mehr verfügen. Vor diesem Hintergrund ist denkbar, dass Arbeitgeber_innen sich künftig auf den Standpunkt stellen, dass diese Form der „anonymen Mustererkennung" außerhalb des Anwendungs- und Schutzbereichs des Datenschutzrechts steht. Der nächste logische Argumentationsschritt wäre dann, dass mangels Personenbezug kein unmittelbarer Anwendungsfall des Bundesdatenschutzgesetzes bzw. der DSGVO und des „BDSG-neu" mehr gegeben ist und dass auch das Mitbestimmungsrecht § 87 Abs. 1 Nr. 6 BetrVG mangels personenbeziehbarer Kontrollen nicht zur Anwendung kommt. Und das, obwohl sich die allgemeinen Erkenntnisse zulasten einzelner Beschäftigter als Maßstab für das individuelle Verhalten heranziehen lassen.

5

PROBLEMFELDER

Die Digitalisierung der Arbeitswelt ist mit einer deutlichen Zunahme der Erhebung und Verarbeitung personenbezogener Daten in betrieblichen Systemen verbunden. Diese Feststellung gilt ebenso für personenbeziehbare Maschinendaten in Produktionsbereichen wie für entsprechende Informationen über Beschäftigte im Verwaltungs-, Service- oder Dienstleistungsbereich. Letztlich droht aus Sicht der Beschäftigten der Wegfall der datenschutzrechtlich geforderten Transparenz bezüglich der Verwendung und Verarbeitung ihrer personenbezogenen Daten durch Arbeitgeber_innen. Ein solcher Effekt ist aber mit dem Recht auf informationelle Selbstbestimmung nicht zu vereinbaren, das insbesondere das Recht des Einzelnen beinhaltet, über die Preisgabe der eigenen personenbezogenen Daten zu entscheiden.[4] Dies schließt die Vergabe von Verarbeitungsbefugnissen nur für bestimmte Zwecke ein.

Aus datenschutzrechtlicher Sicht ist in diesem Zusammenhang insbesondere die Ausweitung zweckfreier Vorratsdatenspeicherung im Rahmen von Data-Mining und Big Data sowie die Zunahme von Datenübermittlungen ohne wirksame Zweckbindung aus dem Betrieb oder Unternehmen heraus an anderer Stelle problematisch, weil sich hier insbesondere die Löschungspflichten, die aus § 35 Abs. 2 BDSG folgen, nicht mehr umsetzen lassen. Gleiches gilt für das durch Artikel 17 DSGVO garantierte „Recht auf Vergessenwerden". Es besteht an dieser Stelle ein diametraler Gegensatz zwischen den technischen Möglichkeiten auf der einen und den datenschutzrechtlichen Vorgaben auf der anderen Seite.

Nimmt man die einschlägigen datenschutzrechtlichen Maßstäbe ernst, dann bedeutet dies beispielsweise, dass die Erstellung von personenbezogenen „sozialen Graphen", die etwa bei Microsoft Office 365 möglich ist, schon wegen der fehlenden bzw. nicht ausreichenden Löschungsmöglichkeiten unzulässig ist. Gleiches gilt für die Übermittlung von Metadaten aus Kundensystemen an die Hersteller von Software, solange nicht garantiert ist, dass keinerlei Rückbezug auf bestimmte Personen oder auf Personengruppen erfolgen kann.

5.1 GRENZEN DER VORRATSDATEN-SPEICHERUNG

Das Datenschutzrecht begrenzt die Verarbeitungsbefugnisse von Arbeitgeber_innen bezüglich der personenbezogenen Daten ihrer Beschäftigten grundlegend. Sowohl aus dem BDSG als auch aus der DSGVO leitet sich beispielsweise die Notwendigkeit ab, Verarbeitungszwecke konkret, transparent und verbindlich festzulegen oder nicht mehr erforderliche Daten schnell und sicher zu löschen. Schon diese Vorgaben stehen einer Vorratsdatenspeicherung außerhalb der konkreten Zwecke eines Beschäftigungsverhältnisses entgegen. Weitere datenschutzrechtliche Grenzen für zweckfreie Vorratsdatenspeicherungen leiten sich aus allgemeinen normativen Leitlinien ab wie etwa aus den allgemeinen Vorgaben zur Datenvermeidung und Datensparsamkeit in § 3a BDSG (künftig Artikel 5 Abs. 1 Buchstabe c) DSGVO) oder aus der in § 32 Abs. 1 BDSG (künftig § 26 Abs. 1 „BDSG-neu") sich ableitenden Beschränkung auf erforderliche Daten.

Nach § 32 Abs. 1 Satz 1 BDSG dürfen etwa für die Durchführung eines Beschäftigungsverhältnisses nur solche Erhebungen, Verarbeitungen und Nutzungen von personenbezogenen Daten erfolgen, die unmittelbar für die Durchführung von Beschäftigungsverhältnissen erforderlich sind und die dort einen konkreten Zweck erfüllen. Dabei handelt es sich im Regelfall insbesondere um aktuelle Daten zur Arbeitserbringung oder -verwaltung, nicht aber um Detailinformationen über ein länger zurückliegendes Handeln. Beschäftigtendaten aus der Vergangenheit sind bezogen auf Arbeitsverhältnisse nur in bestimmten Fällen erforderlich, wie etwa die nach § 3 Abs. 1 Entgeltfortzahlungsgesetz (EFZG) notwendigen Informationen, ob eine Arbeitsunfähigkeit innerhalb von zwölf Monaten auf dieselbe Krankheit zurückzuführen ist.

Nicht von den einschlägigen datenschutzrechtlichen Erlaubnisnormen erfasst sind hingegen aus objektiver Sicht nicht erforderliche Beschäftigtendaten wie etwa Inhalte von

4 Der 1. Leitsatz im „Volkszählungs-Urteil" lautet: „Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art 2 Abs 1 in Verbindung mit GG Art 1 Abs 1 umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" (BVerfG 1983).

Chats zu allgemeinen Themen, die Beschäftigte in einem internen sozialen Netzwerk vor längerer Zeit geführt haben. Gleiches gilt für Informationen zum „Sozialverhalten", die aus einem „Social Graph" gewonnen werden und die in Form von sogenannten„Score-Werten" vergleichende Bewertungen ermöglichen.

(a) Löschung

Bezogen auf Vorratsdatenspeicherungen kommt der Vorgabe zur Datenlöschung in § 35 Abs. 2 Nr. 3 BDSG (künftig Artikel 17 DSGVO) eine herausragende Bedeutung zu. Diese Löschungsvorgabe gilt insbesondere in den Fällen, in denen der ursprüngliche Verarbeitungszweck der Verarbeitung erfüllt worden ist. Hat etwa ein Beschäftigter eine komplizierte Berechnung durchgeführt und wurden deren Ergebnisse von den zuständigen Stellen im Betrieb geprüft und akzeptiert, gibt es keine Grundlage dafür, weiterhin detaillierte Informationen dazu zu speichern, welche Arbeitsschritte durchgeführt wurden oder wie lange er für Teilarbeiten gebraucht hat. Gleiches gilt für Informationen zur Dauer der Erstellung einer E-Mail, eines Textdokuments oder einer Präsentation. Dafür, diese Daten nach Wegfall des Verarbeitungszwecks weiter zu speichern und zu verarbeiten, gibt es somit ebenso wenig eine datenschutzrechtliche Grundlage wie beispielsweise für deren Auswertung mittels eines „Social Graph".

Diese Bewertung wird durch einschlägige Regelungen der DSGVO gestärkt. Der Grundsatz der Datenminimierung wird durch Artikel 5 Abs. 1 Buchstabe c) DSGVO der gesamten Regelung als prägender Maßstab vorangestellt. Hiernach ist es eine Voraussetzung für die Verarbeitung personenbezogener Daten, dass diese für die festgelegten Verarbeitungszwecke angemessen und erheblich sind und dass sie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind. Darüber hinaus ist der Grundsatz der Datenminimierung gemäß Artikel 6 DSGVO zu beachten. Die Verarbeitung personenbezogener Daten ist hiernach weiterhin nur rechtmäßig, wenn sie mindestens eine der in Artikel 6 Abs. 1 DSGVO genannten Bedingungen erfüllt. Bezogen auf Beschäftigungsverhältnisse eröffnet Artikel 88 Abs. 1 DSGVO den Mitgliedstaaten die Möglichkeit, besondere Regelungen für die Zulässigkeit der Verarbeitung von Beschäftigtendaten zu treffen.

Auch die Löschungsvorgaben, die die DSGVO enthält, sind strenger formuliert als die entsprechenden Vorgaben im BDSG. Das in Artikel 17 Abs. 1 DSGVO enthaltene Recht auf Löschung ist nach dem Wortlaut ausdrücklich als „Recht auf Vergessenwerden" ausgestaltet. Nach Artikel 17 Abs. 1 Buchstabe a) DSGVO sind Daten beispielsweise zu löschen, wenn sie für die ursprünglichen Erhebungszwecke nicht mehr notwendig sind. Nicht mehr in der DSGVO enthalten ist die derzeit in § 35 Abs. 3 Nr. 3 BDSG formulierte Alternative einer Sperrung, wenn eine Löschung nur mit einem unverhältnismäßig hohen Aufwand möglich wäre. Aufgrund dieser eindeutigen Rechtssituation ist es fraglich, ob die nunmehr vom Gesetzgeber im „BDSG-neu" vorgesehene erneute Aufnahme von Sperrungsmöglichkeiten einer rechtlichen Prüfung standhalten wird.

(b) Umsetzung

In welchem Umfang die vorstehend skizzierten Begrenzungen der Vorratsdatenverarbeitung sowie gesetzlich vorgeschriebene Datenlöschungen in der Praxis umgesetzt werden können, hängt entscheidend von der Bereitschaft der Arbeitgeber_innen ab, rechtskonforme Zustände herzustellen und zu garantieren. Sind entsprechende Vorgaben oder Begrenzungen in Betriebsvereinbarungen verankert, können Betriebsräte deren Einhaltung nach den Regeln des BetrVG durchsetzen. Betriebliche Datenschutzbeauftragte können auf die fehlende Rechtsgrundlage hinweisen und die Beendigung der entsprechenden Verarbeitungen und Nutzungen einfordern.

Lässt sich eine datenschutzkonforme Situation auf keinem dieser Wege herstellen, stehen Beschäftigte vor den Alternativen, die staatlichen Datenschutzaufsichtsbehörden einzuschalten, ihre Rechte vor dem zuständigen Arbeitsgericht durchzusetzen oder die Verstöße gegen datenschutzrechtliche Vorgaben hinzunehmen. Vor der Einschaltung Dritter scheuen allerdings viele Beschäftigte aus Angst vor beruflichen Nachteilen oft zurück.

Eine Veränderung dieser Situation könnte aus dem Tätigwerden einer Datenschutzorganisation gemäß Artikel 80 DSGVO resultieren. Nach dieser neuen Regelung sind Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig sind, künftig befugt, bei Verstößen gegen datenschutzrechtliche Vorgaben im Namen von Betroffenen Beschwerden beim Arbeitgeber/bei der Arbeitgeberin oder bei den zuständigen Aufsichtsbehörden einzulegen. Weiterhin ist die Anrufung zuständiger Gerichte im Namen der Betroffenen möglich. Derzeit ist zwar noch unklar, in welchem Umfang und mit welchen Ergebnissen sich diese Vertretungsregelung praktisch auswirken wird. Nach dem Wortlaut der Vorschrift kommt aber auch ein Tätigkeitwerden der entsprechenden Stellen ohne Nennung der Beschäftigten in Betracht, die sie angerufen haben. Das hätte für Beschäftigte den Vorteil, dass der Arbeitgeber/die Arbeitgeberin nicht erfährt, wer datenschutzrechtliche Missstände anprangert.

Die neuen Möglichkeiten, die sich künftig aus Artikel 80 DSGVO ableiten werden, stehen grundsätzlich auch Einrichtungen, Organisationen oder Vereinigungen offen, die unter Beteiligung von Gewerkschaften gegründet werden. Diese könnten etwa als gemeinnützige „Stiftung Beschäftigtendatenschutz" ausgestaltet werden und das satzungsmäßige Ziel verfolgen, Beschäftigten dabei zu helfen, ihr Persönlichkeitsrecht am Arbeitsplatz dort zu wahren, wo für sie die individuelle Sicherstellung datenschutzkonformer Zustände nicht möglich oder zu riskant ist. Gewerkschaften könnten mit einer Beteiligung an einer solchen „Stiftung Beschäftigungsdatenschutz" zudem öffentlich den Stellenwert unterstreichen, den dieses Thema für sie hat.

5.2 UNTERNEHMENSÜBERGREIFENDE VERARBEITUNGEN

(a) Grundsätze

Ein zentraler Aspekt der Digitalisierung ist die umfassende Vernetzung aller Arten von Daten. Diese Vernetzung findet längst nicht mehr nur innerhalb von Abteilungen oder Betriebe statt, sondern in den meisten Fällen auch unternehmens-

übergreifend: Elektronische Vernetzungen mit externen Dritten wie Kund_innen oder Lieferant_innen sind inzwischen schon fast der Regelfall. Innerhalb von Konzernen finden umfassende Datenflüsse ohne Rücksicht auf gesellschaftsrechtliche Grenzen statt.

Geografische Grenzen für Vernetzungen gibt es inzwischen praktisch nicht mehr. In der vernetzten digitalen Welt ist es aus technischer Sicht unerheblich, ob Arbeitsprozesse in Deutschland, in Europa oder irgendwo anders auf der Welt stattfinden. Eine vernetzte Erledigung und Kontrolle von Arbeitsaufgaben ist vielmehr überall möglich, wo eine stabile und leistungsfähige Internetverbindung zur Verfügung steht.

Aus datenschutzrechtlicher Sicht setzen die beschriebenen unternehmensübergreifenden Verarbeitungen voraus, dass die hierfür notwendigen gesetzlichen Erlaubnistatbestände erfüllt sind. Für die Übermittlung an externe Datenverarbeiter muss es etwa eine explizite datenschutzrechtliche Erlaubnisnorm geben. Dies gilt auch innerhalb von Konzernstrukturen, da weder das BDSG noch die DSGVO ein datenschutzrechtliches Konzernprivileg enthält, das eine unternehmensübergreifende Verarbeitung innerhalb von Konzernen legitimiert. Bezogen auf Beschäftigtendaten gehen die einschlägigen datenschutzrechtlichen Normen vielmehr davon aus, dass alle erforderlichen Erhebungen, Verarbeitungen und Nutzungen innerhalb der Grenzen eines Betriebs oder Unternehmens erfolgen.

Legitimiert werden können die angesprochenen unternehmensübergreifenden Verarbeitungen durch einen Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG (künftig Artikel 28 DSGVO). Auftragsdatenverarbeitung ist datenschutzrechtlich zulässig, wenn Auftragnehmer_innen Aufgaben ausschließlich nach Weisungen der Auftraggeber_innen durchführen dürfen, ohne darüber hinaus eigenständige inhaltliche Verarbeitungsbefugnisse zu haben. Soll eine Datenverarbeitung hingegen nach eigenen Vorstellungen und Entscheidungen anderer Stellen durchgeführt werden (etwa durch eine zentrale Personalabteilung in einem Konzernunternehmen), liegt keine Auftragsdatenverarbeitung vor, sondern eine sogenannte Funktionsübertragung. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten bedarf in diesen Fällen nach § 4 Abs. 1 BDSG einer gesetzlichen Erlaubnisvorschrift (für Beschäftigungsverhältnisse in § 32 Abs. 1 Satz 1 BDSG enthalten), einer Legitimation durch eine Betriebsvereinbarung oder einer wirksamen Einwilligung der Beschäftigten nach § 4a BDSG. Bezogen auf Beschäftigungsverhältnisse ist in diesem Zusammenhang zu beachten, dass unternehmensübergreifende Verarbeitungen und Nutzungen nicht als erforderlich im Sinne von § 32 Abs. 1 Satz 1 BDSG zu qualifizieren sind. Eine nahezu identische Rechtssituation leitet sich für die künftige datenschutzrechtliche Situation auf Grundlage der DSGVO und des „BDSG-neu“ ab.

Unternehmensübergreifende Datenverarbeitungen sind damit zwar aus datenschutzrechtlicher Sicht grundsätzlich möglich und zulässig. Voraussetzung ist aber, dass die notwendigen Verträge oder Vereinbarungen abgeschlossen werden bzw. dass erforderliche individuelle Einwilligungen vorliegen. Ohne Erfüllung mindestens einer dieser Voraussetzungen darf die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten, die für die Anbahnung, Durchführung oder Beendigung von Beschäftigungsverhältnissen erforderlich sind, ausschließlich innerhalb der Grenzen eines Unternehmens erfolgen.

(b) Grenzüberschreitende Datenverarbeitung

Die vorstehend skizzierten Regeln für eine unternehmensübergreifende Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten beziehen sich primär auf die Verarbeitung innerhalb Deutschlands. Verarbeitungsprozesse finden jedoch immer öfter international statt. Dies gilt selbst für kleine Betriebe und Unternehmen, sobald sie die Daten ihrer Beschäftigten in der Cloud eines Softwareanbieters irgendwo auf der Welt speichern. Damit stellt sich die Frage nach der datenschutzrechtlichen Zulässigkeit grenzüberschreitender Verarbeitungsvorgänge.

Unproblematisch ist hierbei die grenzüberschreitende Verarbeitung von Beschäftigtendaten innerhalb der EU. Seit der Verkündung der Europäischen Datenschutzrichtlinie im Jahr 1995 (EU-Parlament und -Rat 1995) ist der freie Verkehr zwischen EU-Staaten durch Artikel 1 Abs. 2 dieser Richtlinie privilegiert und durch entsprechende Vorschriften in den nationalen Datenschutzgesetzen abgesichert. § 4b Abs. 1 BDSG (künftig Artikel 44 DSGVO) legt hierzu beispielsweise fest, dass für die Übermittlungen von personenbezogenen Daten innerhalb der EU und des Europäischen Wirtschaftsraums (EWR) dieselben Regeln gelten wie für Übermittlungen innerhalb der Bundesrepublik Deutschland. Entsprechend werden beispielsweise alle in der EU oder in Staaten des EWR angesiedelten Auftragnehmer_innen im Verhältnis zur verantwortlichen Stelle in Deutschland nicht als Dritte gemäß § 3 Abs. 8 Satz 3 BDSG (künftig Artikel 4 Ziff. 9 DSGVO) angesehen, wenn mit ihnen ein Auftrag nach § 11 BDSG (künftig Artikel 28 DSGVO) abgeschlossen wird. Auf dieser rechtlichen Grundlage können auch Beschäftigtendaten verarbeitet werden.

Keine entsprechende Privilegierung gibt es für Staaten außerhalb der EU und des EWR. Datenübermittlungen in diesen Staaten sind allerdings dann möglich, wenn sie von der EU auf der Grundlage von § 4b BDSG (künftig Artikel 44 und 45 Abs. 1 DSGVO) als „datenschutzrechtlich sichere Drittländer“ anerkannt sind (Simitis 2014b). Eine Datenübermittlung, -verarbeitung und -nutzung in Drittländern kann darüber hinaus auch dann erfolgen, wenn zwischen der verantwortlichen Stelle und den Empfänger_innen der Daten ein sogenannter „EU-Standardvertrag“ (Europäische Kommission 2010) abgeschlossen ist. Durch diese Vertragskonzeption soll auf zivilrechtlicher Ebene der datenschutzrechtliche Schutzrahmen hergestellt und garantiert werden, der innerhalb der EU gilt. Allein der Abschluss eines „EU-Standardvertrags“ berechtigt in diesen Fällen Arbeitgeber_innen nicht zur Übermittlung von Beschäftigtendaten. Hinzukommen müssen dieselben datenschutzrechtlichen Voraussetzungen, die es auch für eine Übermittlung innerhalb Deutschlands oder der EU geben müsste. Praktisch setzt das insbesondere eine Prüfung der Erforderlichkeit gemäß § 32 Abs. 1 Satz 1 BDSG bzw. gemäß § 26 Abs. 1 „BDSG-neu“ voraus. Darüber hinaus ist zu beachten, dass auch durch den Abschluss eines „EU-Standardvertrags“ das Fehlen eines datenschutzrechtlichen Konzernprivilegs von Arbeitgeber_innen nicht einseitig kompensiert werden kann. Eine Übermittlung an andere Unternehmen erfolgt damit nach denselben Regeln, die auch in Deutsch-

land zur Anwendung kommen, und bedarf einer datenschutzrechtlichen Legitimation.

(c) Verarbeitung von Beschäftigtendaten in den USA

Eine besondere Situation besteht zwischen der EU und den USA. Unternehmen aus den USA war es lange Zeit möglich, auf der Grundlage der sogenannten „Safe Harbour"-Regeln im Rahmen einer Art „Selbstverpflichtung" gegenüber der EU zu erklären, dass sie den dort geltenden Datenschutzstandard einhalten und garantieren. Der Europäische Gerichtshof (EuGH) hat allerdings mit Urteil vom 6.12.2015 (EuGH 2015) festgestellt, dass der „Safe Harbour"-Mechanismus kein wirksames Mittel ist, um für eine Verarbeitung von personenbezogenen Daten in den USA oder durch US-amerikanische Unternehmen sicherzustellen, dass der in Europa geltende Datenschutz garantiert wird. Kritisch sieht der EuGH in seinem Urteil insbesondere die weitgehenden und rechtsstaatlich praktisch unkontrollierten Möglichkeiten für die Zugriffe US-amerikanischer Sicherheitsbehörden.

An die Stelle der „Safe Harbour"-Regeln ist inzwischen nach einer Entscheidung der Europäischen Kommission der „EU-USA Privacy Shield" getreten (BfDI o. J.). Der Inhalt dieser von der EU-Kommission mit den USA vereinbarten Regelung ist allerdings auf deutliche Kritik gestoßen. Der Vereinbarung wird insbesondere entgegengehalten, dass sie Vorgaben aus der Entscheidung des EuGH vom 6.12.2015 nicht ausreichend aufgenommen hat. Durch sie würde beispielsweise in den USA weder ein wirksamer Rechtschutz für Betroffene geschaffen noch erfolge durch sie eine Beschränkung der Nutzung durch US-Behörden auf bestimmte und strikt begrenzte Zwecke (Weichert/Schuler 2016). Insoweit ist fraglich, ob dieses neue Konzept einer absehbaren erneuten Überprüfung durch den EuGH standhalten wird.

6

HANDLUNGSBEDARF UND HANDLUNGSMÖGLICHKEITEN

Die praktische Umsetzung der (teilweise zwingenden) datenschutzrechtlichen Regeln, die auf den Schutz von Beschäftigten zielen, trifft in der betrieblichen Praxis immer wieder auf Umsetzungs- und Durchsetzungsprobleme. Herausragend sind diese Probleme bei der unternehmensübergreifenden Verarbeitung und Nutzung auch deshalb, weil es hier aus Sicht von Beschäftigten umfangreiche Kontrolldefizite gibt. Auf der kollektivrechtlichen Ebene ist zu vermerken, dass Betriebsräte kollektivrechtliche Regelungen zum Beschäftigtendatenschutz mangels eines einschlägigen Mitbestimmungstatbestands nur indirekt und damit lückenhaft durchsetzen können.

6.1 GEWÄHRLEISTUNG

Findet die Verarbeitung von Beschäftigtendaten außerhalb des Unternehmens des Arbeitgebers/der Arbeitgeberin statt, fällt es Beschäftigten schwer, zu erkennen und zu überprüfen, was mit ihren Daten passiert. Zwar ist der Arbeitgeber/die Arbeitgeberin ihnen gegenüber als verantwortliche Stelle gemäß § 34 Abs. 1 BDSG (künftig Artikel 15 Abs. 1 DSGVO) zur umfassenden Auskunft darüber verpflichtet, wo und auf welcher rechtlichen Grundlage ihre Beschäftigtendaten für welche Zwecke verarbeitet und genutzt werden. Gerade in größeren Konzern, die praktisch immer auch international aufgestellt sind, ist die vollständige Erteilung einer solchen Auskunft schwierig, weil oft der Arbeitgeber/die Arbeitgeberin selbst gar nicht präzise weiß, welche Daten innerhalb eines Konzerns wo und für welche Zwecke verarbeitet und genutzt werden. Dies gilt erst recht, wenn die Verarbeitung und Nutzung außerhalb der EU oder des EWR erfolgt.

Auch die Rechtskonformität lässt sich bei einer Verarbeitung außerhalb von EU oder EWR nur begrenzt oder gar nicht garantieren. Diese Aussage gilt besonders für Verarbeitungen in den USA, weil dort umfassende Zugriffsrechte der dortigen Sicherheitsbehörden bestehen, die mit europäischen Datenschutzvorgaben ebenso wenig kompatibel sind wie das Fehlen von entsprechenden Auskunfts- und Widerspruchsmöglichkeiten (EuGH 2015).

Um diese Situation zu verändern, müssten die Befugnisse von Arbeitgeber_innen zur Weitergabe von Beschäftigtendaten deutlicher als derzeit davon abhängig gemacht werden, dass die von ihnen beauftragten Stellen bzw. Unternehmen die Einhaltung der Regeln zum Beschäftigtendatenschutz umfassend und wirksam garantieren. Hierfür ist es nicht ausreichend, allein darauf zu bauen, dass Auftragnehmer_innen die ihnen obliegenden vertraglichen Datenschutzpflichten einhalten. Erforderlich ist es darüber hinaus, das Handeln der Auftragnehmer_innen einer regelmäßigen Überprüfung zu unterziehen, etwa durch wirksame und aussagekräftige Auditierungen oder durch Kontrollen vor Ort. Entsprechende Maßnahmen sollten nicht nur mit Blick darauf vorgesehen werden, dass Verstöße gegen datenschutzrechtliche Verpflichtungen künftig nach Artikel 83 DSGVO mit hohen Geldbußen geahndet werden können.

Die Notwendigkeit der Überprüfung von Auftragnehmer_innen ist unabhängig von gesellschaftsrechtlichen Beziehungen. Verantwortliche Stellen müssen „echte“ Dritte ebenso einer Bewertung unterziehen wie Unternehmen, die demselben Konzern angehören. Innerhalb eines Konzerns stehen Konzernunternehmen in Deutschland allerdings in der Praxis oft vor dem Problem, dass gerade ausländische Konzernspitzen oder andere Konzernunternehmen mit datenschutzrechtlichen Kontrollen nicht einverstanden sind. Es kann vermutet werden, dass dann Mitglieder von Geschäftsführungen in einzelnen Konzernunternehmen auf die Durchsetzung von datenschutzrechtlichen Kontrollen verzichten, weil sie sich Sorgen um ihre eigene Karriere im Konzern machen. Dass das Bekanntwerden von Datenschutzverstößen schnell auch das Ende der individuellen Karriere bedeuten kann, wird dabei oft nicht als Option gesehen.

Für die übergeordnete Kontrolle der Einhaltung einschlägiger datenschutzrechtlicher Vorschriften sind auch bei der Datenverarbeitung im Auftrag oder bei einer Funktionsübertragung die staatlichen Aufsichtsbehörden zuständig. In Deutschland sind dies in den meisten Bundesländern die Landesbeauftragten für den Datenschutz. Diese Zuständigkeit wird durch die DSGVO bzw. durch das „BDSG-neu“ nicht grundsätzlich verändert. Allerdings zeigt sich in der

Praxis, dass den meisten Aufsichtsbehörden eine wirksame und flächendeckende Kontrolle schon personell nicht möglich ist. Aus diesem Kontrolldefizit folgt wiederum, dass viele Verstöße nicht entdeckt und damit auch nicht sanktioniert werden, etwa wenn eine Auftragsdatenverarbeitung ohne die notwendigen Verträge stattfindet.

Werden Aufsichtsbehörden auf konkrete Verstöße hingewiesen, ist ein zeitnahes Handeln schon aus personellen Gründen nicht immer möglich. Eine wirksame datenschutzrechtliche Kontrolle von grenzüberschreitenden Auftragsdatenverarbeitungen setzt deshalb eine deutliche Erhöhung der personellen und technischen Ausstattung der Aufsichtsbehörden gegenüber dem heutigen Stand voraus. Dieses zeichnet sich derzeit auch mit Blick auf das neue europäische Datenschutzrecht nicht ab.

Verbessert werden müssten auch die Handlungsmöglichkeiten von Beschäftigten für die Fälle, in denen Arbeitgeber_innen die bestehenden datenschutzrechtlichen Vorschriften nicht einhalten oder bewusst verletzen. Führt die Einschaltung interner Stellen wie betrieblichen Datenschutzbeauftragten oder des Betriebsrats nicht zu einer Abhilfe, stehen Beschäftigte vor der Alternative, entweder die zuständige staatliche Aufsichtsbehörde einzuschalten bzw. das Arbeitsgericht anzurufen oder aber den mit der Verletzung datenschutzrechtlicher Vorgaben verbundenen Eingriff in ihre Persönlichkeitsrechte aus Angst vor arbeitsrechtlichen Nachteilen weiter hinzunehmen. Der zweiten Alternative wird aus Sorge vor beruflichen Nachteilen in vielen Fällen der Vorzug gegeben.

Zu einer Veränderung dieser unbefriedigenden Situation könnte etwa ein besonderer Kündigungsschutz führen, der immer dann greift, wenn Beschäftigte die Einhaltung datenschutzrechtlicher Standards intern oder durch die Einschaltung der zuständigen staatlichen Stellen einfordern. Dieser Kündigungsschutz könnte sich inhaltlich an den Schutzstandards orientieren, den es in anderen Staaten in einschlägigen Gesetzen zum Schutz sogenannter „Whistleblower“ gibt, die auf Missstände in Unternehmen hinweisen.

Darüber hinaus könnten die Handlungsmöglichkeiten von Beschäftigten zur Sicherstellung ihrer datenschutzrechtlichen Position auch dadurch verbessert werden, dass ein „datenschutzrechtliches Verbandsklagerecht“ geschaffen wird, das ggf. auch unabhängig von Anzeigen einzelner Beschäftigter ist. Dieses könnte an die allgemeinen Möglichkeiten anknüpfen, die Artikel 80 DSGVO enthält (vgl. Kapitel 5.1 Abschnitt b). Die damit geschaffenen Möglichkeiten könnten dadurch gestärkt werden, dass die Höhe möglicher individueller Schadensersatzansprüche entsprechend der Vorgabe zu Geldbußen in Artikel 83 Abs. 1 DSGVO so ausgestaltet wird, dass sie ebenfalls wirksam, verhältnismäßig und abschreckend ist. Hinzukommen müsste ein besonderer Kündigungsschutz von Beschäftigten, die sich gegen Datenschutzverstöße des Arbeitgebers/der Arbeitgeberin wenden.

6.2 STÄRKUNG KOLLEKTIVRECHTLICHER MÖGLICHKEITEN

(a) Ausweitung der Zuständigkeit

Nach § 80 Abs. 1 Nr. 1 BetrVG gehört es zu den allgemeinen Aufgaben des Betriebsrats, darüber zu wachen, dass die zugunsten der Arbeitnehmer_innen geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden. Auskunftspflichtig in allen einschlägigen Fragen ist der Arbeitgeber/die Arbeitgeberin. Mit Blick auf diese kollektivrechtliche Kontrollpflicht stellt sich bezogen auf die datenschutzrechtliche Situation bei unternehmensübergreifenden Datenverarbeitungen das Problem, dass die gesetzlichen Möglichkeiten von Betriebsräten durch das sogenannte „Territorialitätsprinzip“ geografisch auf Deutschland beschränkt sind. Damit haben sie beispielsweise bezogen auf die Verarbeitung von Beschäftigtendaten durch Auftragnehmer_innen in anderen Staaten keine direkten Kontrollmöglichkeiten. Sie können lediglich vom Arbeitgeber/von der Arbeitgeberin verlangen, dass dieser seinerseits/diese ihrerseits als Auftraggeber_in mit Auftragnehmer_innen verbindlich vereinbart, dass Betriebsräte die ihnen per Gesetz oder aufgrund einer kollektivrechtlichen Vereinbarung zustehenden Rechte tatsächlich wahrnehmen können.

Diese Situation setzt den Handlungsmöglichkeiten von Betriebsräten in der Praxis enge Grenzen: Während Arbeitgeber_innen ihre Arbeitsprozesse unabhängig von staatlichen Grenzen und nationalen Gesetzen gestalten können, müssen sich Betriebsräte damit begnügen, die Rechte der von ihnen vertretenen Belegschaften ausschließlich in Deutschland gestalten und schützen zu können. Damit klafft zwischen den tatsächlichen Gestaltungsmöglichkeiten, die Arbeitgeber_innen für die Verarbeitung von Beschäftigtendaten haben, und dem durch das BetrVG begründeten gesetzlichen Mitwirkungs- und Mitbestimmungsrahmen von Betriebsräten zulasten der Beschäftigten eine immer größer werdende Lücke. Diese Situation ist in einem vereinten Europa und im Angesicht der flexiblen digitalen Gestaltungsmöglichkeiten nicht mehr zeitgemäß.

Die identifizierte Lücke könnte dadurch geschlossen werden, dass die einschlägigen Mitwirkungs- und Mitbestimmungsrechte bezogen auf Beschäftigtendaten unabhängig von der geografischen Situation entlang der gesamten datenschutzrechtlichen „Produktionskette“ zur Anwendung kommen. Eine solche Ausweitung des Anwendungsbereichs des BetrVG folgt für die hier zu diskutierenden Fälle auch daraus, dass Arbeitgeber_innen durch die Übermittlung von Beschäftigtendaten an Stellen außerhalb Deutschlands den bestehenden kollektivrechtlichen Schutzrahmen reduzieren und damit unmittelbar in Grundrechte der Beschäftigten wie insbesondere in das Recht auf informationelle Selbstbestimmung eingreifen.

Der deshalb notwendige besondere Schutz macht zunächst einmal eine gesetzliche Durchbrechung des Territorialitätsprinzips für den Bereich des BetrVG notwendig, durch die Betriebsräten entsprechende Rechte zugestanden werden. In der Folge müssten Arbeitgeber_innen als verantwortliche Stelle bei der vertraglichen Vereinbarung von Verarbeitungs-

verträgen mit Auftragnehmer_innen sicherstellen, dass Betriebsräte ihre spezifischen Mitwirkungs- und Mitbestimmungsrechte auch dort geltend machen und beispielsweise Kontrollen vor Ort durchführen können.

Um entsprechende Kontrollen wirksam durchführen zu können, müssten Betriebsräten selbst entsprechend qualifiziert werden können. Darüber hinaus müssten die Möglichkeiten zur Einbindung fachlich qualifizierter interner und externer Expert_innen gestärkt werden, die das Vertrauen des Betriebsrats besitzen (ähnlich BMAS 2017: 159).

De facto bedeutet die geforderte Ausweitung des Territorialitätsprinzips, dass dem durch das europäische Datenschutzrecht ausdrücklich garantierten freien Datenverkehr eine kollektivrechtliche Komponente an die Seite gestellt wird, die darauf zielt, dass kollektivrechtlich vorgesehene Mitwirkungs- und Mitbestimmungstatbestände an allen Stellen beeinflusst und kontrolliert werden können, an denen die Verarbeitung von Beschäftigtendaten erfolgt. Eine solche Ausweitung kollektivrechtlicher Möglichkeiten ist insbesondere dann legitim, wenn eine kollektivrechtliche Vereinbarung Erlaubnisnorm für die Datenverarbeitung ist.

(b) Mitbestimmungsrecht zum Datenschutz

Ein Mitbestimmungsrecht zum Datenschutz, mit dem Betriebsräte die Ausgestaltung des Beschäftigtendatenschutzes initiativ mitgestalten könnten, enthält das BetrVG nicht. Auf der Grundlage des Mitbestimmungsrechts in § 87 Abs. 1 Nr. 6 BetrVG können Betriebsräte Einzelaspekte des Datenschutzes lediglich mittelbar regeln (BMAS 2017). Dieses Mitbestimmungsrecht ist einschlägig, wenn im Betrieb technische Einrichtungen eingeführt oder angewendet werden, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer_innen zu überwachen. Es besteht nach der Rechtsprechung unabhängig davon, ob eine subjektive Überwachungsabsicht von Arbeitgeber_innen besteht. Entscheidend für die Anwendbarkeit der Vorschrift ist lediglich, dass objektiv eine Eignung zur Überwachung von Verhalten und Leistung der Arbeitnehmer_innen vorliegt. Vom Anwendungsbereich des Mitbestimmungsrechts werden in der Praxis alle IT-Systeme erfasst, die in irgendeiner Form Beschäftigtendaten erheben, verarbeiten und nutzen.

Die Unabhängigkeit von einer subjektiven Überwachungsabsicht versetzt Betriebsräte auf der Basis von § 87 Abs. 1 Nr. 6 BetrVG in die Lage, bestehende Kontrollrisiken, durch die Persönlichkeitsrechte der Beschäftigten unverhältnismäßig beeinflusst werden können, für technischen Einrichtungen auszuschließen oder zumindest zu reduzieren. Auf der Grundlage dieses Mitbestimmungsrechts können sie etwa verlangen, dass bei der Ausgestaltung und Einstellung technischer Einrichtungen alle zwingenden bzw. maßgeblichen datenschutzrechtlichen Vorschriften beachtet werden. Ist dies nicht der Fall und besteht ein Widerspruch zu einschlägigen Datenschutzvorschriften, kann eine Einführung oder Änderung einer technischen Einrichtung auch nicht über eine Einigungsstelle erzwungen werden. Damit können Betriebsräte die Einhaltung datenschutzrechtlicher Vorschriften zur Grundlage der Mitbestimmung gemäß § 87 Abs. 1 Nr. 6 BetrVG machen, wenn es sich um IT-Systeme handelt, mit denen Beschäftigtendaten verarbeitet werden. Dies sichert zumindest mittelbar die Einflussnahme auf den datenschutzrechtlichen Gestaltungsrahmen, begründet aber kein allgemeines Mitbestimmungsrecht, das von bestimmten IT-Systemen unabhängig ist. Damit können Betriebsräte gegen einen unwilligen Arbeitgeber/eine unwillige Arbeitgeberin beispielsweise ein unternehmensweites Konzept zur Datenlöschung, dass auf die effektive Umsetzung des in Artikel 17 DSGVO enthaltenen „Rechts auf Vergessenwerden" zielt, nicht in einer Einigungsstelle durchsetzen.

Zudem führt die auf der Grundlage von § 87 Abs. 1 Nr. 6 BetrVG bestehende indirekte Möglichkeit der Einflussnahme auf datenschutzrechtliche Aspekte in der betrieblichen Praxis immer wieder zu einem weiteren Problem: Da Betriebsvereinbarungen als datenschutzrechtliche Erlaubnisnormen nach § 4 Abs. 1 BDSG die die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten auch außerhalb der durch § 32 Abs. 1 Satz 1 BDSG vorgegebenen Erforderlichkeit legitimieren können, sehen sich Betriebsräte vielfach schon heute mit entsprechenden Wünschen von Arbeitgeber_innen konfrontiert, ohne das zugleich eine angemessene datenschutzrechtliche Absicherung der Beschäftigten erfolgt. Diese Situation wird sich aufgrund der hervorgehobenen Erwähnung kollektivrechtlicher Vereinbarungen in Artikel 88 Abs. 1 DSGVO und in § 26 Abs. 4 „BDSG-neu" künftig noch intensivieren.

Wollen Betriebsräte vor diesem Hintergrund bestimmte Formen der Verarbeitung (etwa die Verarbeitung von Beschäftigtendaten bei einer Konzerntochter außerhalb Europas) bezogen auf ein neues IT-System nicht per Betriebsvereinbarung legitimieren, kann es ihnen passieren, dass Arbeitgeber_innen eine Einigungsstelle anrufen, um ihre Ziele durchzusetzen. Da eine Einigungsstelle in diesen Fällen alle relevanten Aspekte regeln muss, kann es vorkommen, dass dort unternehmensübergreifender Verarbeitungen einschließlich der Übermittlung an Auftragnehmer_innen außerhalb des Anwendungsbereichs des deutschen oder des europäischen Datenschutzrechts vom Arbeitgeber/von der Arbeitgeberin zusammen mit dem/der Vorsitzenden der Einigungsstelle auch gegen die Position des Betriebsrats legitimiert werden.

Versuchen hingegen Betriebsräte in einer Einigungsstelle den Vorsitzenden/die Vorsitzende davon zu überzeugen, dass bezogen auf ein IT-System ein höherer Datenschutzstandard per Spruch einer Einigungsstelle geschaffen werden muss, halten Arbeitgeber_innen diesem Ansinnen regelmäßig das Argument entgegen, dass es kein „Mitbestimmungsrecht auf Datenschutz" gibt und dass eine solche Lösung deshalb nicht „spruchfähig" ist. Und tatsächlich ist es so, dass diese Aussage für sich zutreffend ist. Betriebsräte können aufgrund des Fehlens eines einschlägigen Mitbestimmungsrechts die Umsetzung datenschutzrechtlicher Regeln und die Gestaltung bestehender Spielräume durch den Arbeitgeber/die Arbeitgeberin außerhalb der Regelung eines bestimmten IT-Systems weder initiativ gestalten noch gegen dessen/deren Willen in einer Einigungsstelle durchsetzen. Zu datenschutzrechtlichen Themen ist Betriebsräten damit im Streitfall der Gang zur Einigungsstelle ebenso verwehrt wie die Wahrnehmung eines Initiativrechts, wenn Arbeitgeber_innen untätig bleiben. Um Betriebsräten entsprechende Möglichkeiten einzuräumen, müsste der Katalog der Tatbestände der sozialen Mitbestimmung des § 87 Abs. 1 BetrVG um ein Mitbestimmungsrecht zum Datenschutz erweitert werden,

das im Ergebnis das Grundrecht der Beschäftigten auf informationelle Selbstbestimmung in der digitalen Arbeitswelt unmittelbar absichern und stärken würden (BMAS 2017).

Ein solches Mitbestimmungsrecht ist auch mit Blick darauf unumgänglich, dass die DSGVO zum Thema Datenverarbeitung im Beschäftigungskontext in Artikel 88 Abs. 1 DSGVO ausdrücklich die Möglichkeit vorsieht, dass die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen[5] spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen. Nach der in Artikel 88 Abs. 1 DSGVO folgenden Aufzählung können spezifische Vorschriften auch Aussagen zum Schutz des Eigentums der Arbeitgeber_innen oder der Kund_innen beinhalten. Nach Artikel 9 Abs. 2 Buchstabe a) DSGVO können zudem durch Kollektivvereinbarungen beispielsweise auch Regelungen für die Verarbeitung datenschutzrechtlich herausragend geschützter besonderer Kategorien personenbezogener Daten getroffen werden. Davon, dass die entsprechenden kollektivrechtlichen Regelungen nur bezogen auf bestimmte IT-Systeme getroffen werden können, ist in der DSGVO nicht die Rede. Schon dies spricht für die Notwendigkeit eines neuen Mitbestimmungsrechts zum Datenschutz.

In dieselbe Richtung weist § 26 Abs. 4 „BDSG-neu". Dort ist festgelegt, dass die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Kollektivvereinbarungen zulässig sein kann. Auch diese ausdrückliche kollektivrechtliche Möglichkeit wird nicht auf Tatbestände beschränkt, für die im BetrVG Mitbestimmungsrechte benannt sind. Die amtliche Begründung zu § 26 „BDSG-neu" belässt es diesbezüglich vielmehr bei der allgemeinen Feststellung, dass Kollektivvereinbarungen den Verhandlungsparteien die Ausgestaltung eines auf die betrieblichen Bedürfnisse zugeschnittenen Beschäftigtendatenschutzes ermöglichen sollen (Deutscher Bundestag 2017: 98). Was fehlt, ist eine an den Persönlichkeitsrechten der Betroffenen orientierte deutliche Begrenzung der Regelungsbefugnisse der Betriebsparteien. Diese Forderung ist insbesondere mit Blick auf die Möglichkeit angebracht, dass per Betriebsvereinbarung künftig auch weitgehende Vereinbarungen zum Umgang mit besonderen Kategorien personenbezogener Daten getroffen werden können. Damit fallen den Betriebsparteien bezüglich besonders sensibler Beschäftigtendaten umfassende Regelungsbefugnisse zu, beispielsweise zur Gesundheit oder zur Weltanschauung (etwa im Zusammenhang mit sogenannten „Antiterror-Screenings"), aber auch zur Gewerkschaftszugehörigkeit (etwa bezogen auf tarifliche Ansprüche) oder zur Sexualität (etwa bezogen auf Sanitärbereiche), ohne dass zugleich die Sicherung des Datenschutzes durch Kontrollmechanismen adäquat gestärkt wird.

Mit Blick auf grundlegende datenschutzrechtliche Vorgaben, die sowohl im BDSG als auch in der DSGVO zu wichtigen Themen wie „Transparenz", „Zweckbindung" und „Datenminimierung" enthalten sind (§ 3a BDSG oder künftig Artikel 5 Abs. 1 DSGVO), aber auch auf das durch Artikel 17 DSGVO als „Recht auf Vergessenwerden" ausgestaltete starke Löschungsrecht werden Betriebsräte eine wirksame Ausgestaltung des betrieblichen Datenschutzes nur erreichen können, wenn sie Gestaltungsvorschläge und hiermit verbundene Forderungen unabhängig von einer einzuführenden oder zu ändernden technischen Einrichtung geltend machen und durchsetzen können.

Ein neues Mitbestimmungsrecht zum Beschäftigtendatenschutz muss insbesondere für die Fälle einschlägig sein, in denen anwendbare Datenschutzvorschriften Arbeitgeber_innen im betrieblichen Rahmen Gestaltungsspielräume eröffnen. In Betracht kommen beispielsweise die folgenden Tatbestände der DSGVO:

- Artikel 5 Abs. 1 DSGVO beinhaltet allgemeine datenschutzrechtliche Grundsätze, die bei der Umsetzung aller normativen Vorgaben der DSGVO beachtet werden müssen. Hierzu gehört insbesondere die „Rechtmäßigkeit" und die „Zweckbindung" der Verarbeitung, die „Datenminimierung", die Wahrung der „Richtigkeit" von Informationen, eine „Speicherbegrenzung" durch Löschungen sowie die Sicherung der „Integrität und Vertraulichkeit" von Daten. Vor diesem Hintergrund müsste es das geforderte neue Mitbestimmungsrecht Betriebs- und Personalräten beispielsweise ermöglichen, für die Verarbeitung von Beschäftigtendaten die notwendige „Zweckbindung" durch abschließende Benennung von zulässigen Verwendungszusammenhängen kollektivrechtlich festsetzen zu können. Der Grundsatz der „Datenminimierung" ließe sich garantieren, wenn Arbeitgeber_innen im Sinne einer „Beweislastumkehr" kollektivrechtlich verpflichtet werden könnten, die Erforderlichkeit der Verarbeitung von Beschäftigtendaten im Streitfall substantiiert darzulegen. Ist eine solche Darlegung nicht möglich, müsste eine Erhebung und Verarbeitung von Daten im Zweifelsfall unterbleiben.

- In Ausfüllung des in Artikel 5 Abs. 1 Buchstabe e) DSGVO genannten Grundsatzes der „Speicherbegrenzung" müsste ein Mitbestimmungsrecht zum Beschäftigtendatenschutz insbesondere die Ausgestaltung von umfassenden Löschkonzepten ermöglichen. Dazu wäre es notwendig, nicht nur zeitliche Begrenzungen der Speicherdauer mitbestimmen zu können, sondern auch die Ausgestaltung von übergreifenden Löschkonzepten. Darüber hinaus müsste es Betriebs- und Personalräten zur Umsetzung des durch Artikel 17 DSGVO begründeten „Rechts auf Vergessenwerden" möglich sein, verbindliche und wirksame Löschungsmechanismen überall dort durchzusetzen, wo Beschäftigtendaten aus ihrem Zuständigkeitsbereich verarbeitet werden, insbesondere auch in anderen Konzernunternehmen.

- Soll die Erhebung und Verarbeitung von Beschäftigtendaten auf der Grundlage einer individuellen Einwilligung erfolgen, müsste das neue Mitbestimmungsrecht sich auf die Ausgestaltung von Einwilligungsprozessen durch Beschäftigte gemäß Artikel 7 DSGVO beziehen. Anzustre-

---

5 Kollektivvereinbarungen im Sinne von Art. 88 Abs. 1 DSGVO sind Tarifverträge, Betriebsvereinbarungen und Dienstvereinbarungen (Deutscher Bundestag 2017: 101).

ben ist, dass individuelle Einwilligungen von Arbeitgeber_innen bei Beschäftigten überhaupt nur dann eingefordert werden können, wenn der zuständige Betriebs- oder Personalrat dem Verfahren bzw. den vom Arbeitgeber/von der Arbeitgeberin angestrebten Zwecken der Verarbeitung zugestimmt hat. Ggf. könnte ein Widerspruchsrecht vorgesehen werden, dessen Ausübung der Erhebung und Verarbeitung auf der Grundlage einer individuellen Einwilligung entgegensteht.

– Vom neuen Mitbestimmungsrecht erfasst werden müssten auch die vom Arbeitgeber/von der Arbeitgeberin gestaltbaren konkreten Maßnahmen zum Schutz der Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO. In diesem Rahmen müssten kollektivrechtlich beispielsweise technische Gestaltungen erzwingbar sein, bei denen die Verarbeitung von Beschäftigtendaten standardmäßig pseudonymisiert und verschlüsselt erfolgt. Abweichungen von diesem Schutzstandard sollten hingegen ausnahmsweise nur dann zulässig sein, wenn die Verwendung von Klarnamen oder unverschlüsselten Daten unumgänglich ist.

– Die von Arbeitgeber_innen gemäß Artikel 35 DSGVO durchzuführenden Datenschutz-Folgenabschätzung und die Umsetzung der hieraus folgenden Schutznotvorkehrungen in die betriebliche Praxis sollte ebenfalls vom neuen Mitbestimmungsrecht erfasst werden. Dies würde Betriebs- und Personalräten etwa die Möglichkeit eröffnen, die Zustimmung zu Einführungen oder Änderungen von IT-Systemen davon abhängig zu machen, dass Risiken oder Schwachstellen abgestellt werden, die im Rahmen der Datenschutz-Folgenabschätzung erkannt worden sind.

Redaktionell lässt sich das hier postulierte Mitbestimmungsrecht in die Tatbestände des § 87 Abs. 1 BetrVG einfügen. Dies würde nicht nur der neuen kollektivrechtlichen Bedeutung dieses Rechts gerecht, sondern würde Betriebsräten zugleich aufgrund seiner Ausgestaltung als Initiativrecht in die Lage versetzen, eigene Vorstellungen ggf. auch durch Anrufung der Einigungsstelle wirksam durchzusetzen.

7

FAZIT

Welche spezifischen Veränderungen die Digitalisierung für die Arbeitswelt in der Zukunft mit sich bringen wird, lässt sich seriös allenfalls mit einem Zeithorizont von ein paar Jahren prognostizieren. Wer dies bezweifelt, muss die Frage beantworten, warum etwa vor zehn Jahren niemand konkret vorhersagen konnte, welche Auswirkungen das Smartphone von Apple auf fast alle Formen der Arbeitserbringung haben würde.

Relativ präzise benennen lassen sich hingegen die Auswirkungen von aktuellen technischen Entwicklungen auf die Arbeitswelt und die hieraus folgenden Effekte. Herausragende Treiber sind hier die universellen und geografisch ungebundenen Möglichkeiten der Arbeitserbringung, die für immer mehr Tätigkeiten zur Verfügung stehen. Die Kombination von SaaS und Cloud-Computing auf der einen und Cloud- oder Crowdworking auf der anderen Seite legt den Gedanken nah, dass die heute noch weitgehend standardmäßige Arbeit an festen Orten und in festen Betriebsgebäuden für viele Beschäftigte bald der Vergangenheit angehören wird.

Eine weitere Konsequenz dieser Entwicklungslinie könnte auch der Wegfall konventioneller Vertragsbeziehungen für Formen der abhängigen Beschäftigung sein. Weltweit agierende Cloud- und Crowdworker_innen werden nämlich beispielsweise regelmäßig nicht auf der Grundlage eines dauerhaften Arbeitsvertrags tätig, sondern im Rahmen von flexiblen Dienst- oder Werkverträgen. Diese unterliegen zudem nicht mehr zwingend dem nationalen Recht. Der heute gesetzlich garantierte arbeits-, sozial- oder datenschutzrechtliche Schutzrahmen wird bei der Arbeit in „digitalen Wolken" damit allenfalls fragmentarisch fortbestehen, ohne dass die so Beschäftigten diesen Verlust durch eine adäquat höhere Bezahlung kompensieren können.

Dieser hoch flexiblen neuen digitalen Arbeitswelt steht für den Bereich des Beschäftigtendatenschutzes ein normatives System gegenüber, das gemessen an den vielfältigen Optionen, die die Digitalisierung für die Ausgestaltung von Prozessen und Organisationen mit sich bringt, immer noch sehr „analog" ist. Das soll nun aber nicht bedeuten, dass ein wirksamer gesetzlicher Datenschutz gar nicht mehr möglich ist. Im Gegenteil: Klare gesetzliche Ge- und Verbote sind für Anwender_innen immer dann eine gute Orientierung, wenn der Wille besteht, bestehende Handlungsoptionen auch nur im zulässigen Rahmen zu nutzen. Und sie sind nur dann wirksam, wenn die Einhaltung von Verboten auch erkennbar kontrolliert und durchgesetzt wird. Für die neue digitale Welt bedeutet das: Beim Fahren auf der Datenautobahn werden die bestehenden gesetzlichen Regeln und Begrenzungen von allen Stellen, die personenbezogene Daten erheben oder verarbeiten, durchgängig beachtet und umgesetzt werden, wenn Abweichungen von zwingenden gesetzlichen Vorgaben schnell erkannt und wirksam geahndet werden. Mit Blick auf die durchaus abschreckenden Geldbußen, die Artikel 83 DSGVO vorsieht, könnten entsprechende Kontrollmaßnahmen durchaus einen positiven Effekt haben. Ob sie erfolgen, wird die Zukunft zeigen.

Bezogen auf den Bereich des Beschäftigtendatenschutzes zeichnet sich derzeit kein Trend ab, dass Arbeitgeber_innen die Rechte ihrer Beschäftigten zukünftig mehr und intensiver als heute wahren und schützen werden. Mit Blick auf die beschriebenen neuen Analyse- und Auswertungsmöglichkeiten, die es etwa im Bereich von Big Data oder Data-Mining gibt, steht damit zu befürchten, dass in der Summe Eingriffe in Persönlichkeitsrechte der Beschäftigten seitens der Arbeitgeber_innen eher zu- als abnehmen werden. Diese Gefahr besteht insbesondere innerhalb von grenzüberschreitenden Unternehmens- und Konzernstrukturen, wenn wirksame Regelungs- und Kontrollmechanismen fehlen. Sie wird dadurch verschärft, dass Betriebs- und Personalräten bisher keine neuen Mitwirkungs- und Mitbestimmungsrechte zur Verfügung stehen, die bezogen auf die Digitalisierung der Arbeitswelt wirksame Handlungs- und Durchsetzungsoptionen eröffnen. Damit ist der Gesetzgeber gefordert, einen wirksamen Ausgleich herzustellen zwischen den unterschiedlichen Interessen der Arbeitgeber_innen, die digitale Techniken in den unterschiedlichen Zusammenhängen und Konstellationen einsetzen und nutzen wollen, und der Beschäftigten, die Wert auf den Schutz ihrer Grundrechte und ihrer Arbeitsplätze legen. Nur wenn dies gelingt, werden alle Beteiligten von den Vorteilen profitieren, die Daten als „Öl des 21. Jahrhunderts" beinhalten.

Abkürzungsverzeichnis

App	Application
ArbZG	Arbeitszeitgesetz
BAG	Bundesarbeitsgericht
BAGE	Bundesarbeitsgerichtsentscheidungen
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BMAS	Bundesministerium für Arbeit und Soziales
BVerfGE	Bundesverfassungsgerichtsentscheidungen
BYOD	Bring Your Own Device
DSAnpUG	Datenschutz-Anpassungs- und Umsetzungsgesetz
DSGVO	Datenschutz-Grundverordnung
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
EFZG	Entgeltfortzahlungsgesetz
IT	Informationstechnik
MDM	Mobile Device Management
SaaS	Software as a Service

Literaturverzeichnis

BAG 30.8.1995 – 1 ABR 4/95.

BAG 27.3.2003 – 2 AZR 51/02.

BAG 29.6.2004 – 1 ABR 21/03.

BAG 22.09.2016a – 2 AZR 848/15.

BAG 13.12.2016b – 1ABR 7/15.

BfDI (o. J.): Safe Harbor and Schrems-Urteil des EuGH, https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/SafeHarbor.html?__lang=en (26.6.2017).

Bitkom 2015: Zukunft der Consumer Electronics, Berlin.

BMAS 2017: Weißbuch Arbeiten 4.0, Berlin.

Brandt, Jochen 2016: Bring dein Eigenes mit, in Arbeitsrecht im Betrieb (3), S. 34–35.

Briegleb, Volker; Heise-Online 2015: IFA 2015: Das Internet der Dinge treibt die Branche, 2.9.2015, https://www.heise.de/newsticker/meldung/IFA-2015-Das-Internet-der-Dinge-treibt-die-Branche-2801955.html (26.6.2017).

Bussche, Axel von dem; Voigt, Paul (Hrsg.) 2014: Konzerndatenschutz: Rechtshandbuch, München.

BVerfG 1983: BVerfGE 65: Urteil vom 15.12.1983, 1 ff.

Däubler, Wolfgang 2015: Gläserne Belegschaft?, Frankfurt.

Däubler, Wolfgang 2016: Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses, in: Däubler, Wolfgang; Klebe, Thomas; Wedde, Peter; Weichert, Thilo (Hrsg.): Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG, Frankfurt, S. 593–657.

Däubler, Wolfgang; Kittner, Michael; Klebe, Thomas; Wedde, Peter (Hrsg.) 2016: Betriebsverfassungsgesetz: Mit Wahlordnung und EBR-Gesetz, Frankfurt.

Däubler, Wolfgang; Klebe, Thomas; Wedde, Peter; Weichert, Thilo (Hrsg.) 2016: Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG, Frankfurt.

Däubler-Gmelin, Herta 2014: Der Ärger geht weiter: Mitarbeiter-Screening, EU-Terrorlisten, AEO-Zertifizierung, in Computer und Arbeit (4), S. 13–16.

Deutscher Bundestag 2017: Drucksache 18/1135, Saarbrücken.

EuGH 6.10.2015 C-362/14.

EU-Parlament und -Rat 24.10.1995 Richtlinie 95/46/EG.

Europäische Kommission 2010: Beschluss vom 5.2.2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern nach der Richtlinie 95/46/EG.

FAZ.NET 2016: „Computer kennen keinen Nasenfaktor", 15.4.2016, www.faz.net/aktuell/berufchance/arbeitswelt/christoph-kull-von-workday-ueber-software-in-der-arbeitswelt-14166411.html (26.6.2017).

Greve, Silke 2016: Das ist bei Social Media zu regeln, in Computer und Arbeit (11), S. 49–51.

Greve, Silke; Wedde, Peter 2014: Social-Media-Guidelines, Frankfurt.

Höller, Heinz-Peter 2016: Mining the Enterprise Social Graph, in Computer und Arbeit (5), S. 8–13.

Höller, Heinz-Peter; Thannheiser, Achim 2015: Mobile Device Management: Basics und Tipps zur Regelung der mobilen Kommunikation, in Computer und Arbeit (11), S. 4–10.

Höller, Heinz-Peter; Wedde, Peter 2016: Neue Technik – neue Anforderungen, in: Wedde, Peter (Hrsg.): Handbuch Datenschutz und Mitbestimmung, Frankfurt, S. 297–391.

Klebe, Thomas 2016: Mitbestimmungsrechte, in: Däubler, Wolfgang; Kittner, Michael; Klebe, Thomas; Wedde, Peter (Hrsg.): Betriebsverfassungsgesetz: Mit Wahlordnung und EBR-Gesetz, Frankfurt, S. 1.723 – 1.877.

Leimeister, Jan M.; Zogaj, Shkodran; Blohm, Ivo 2015: Crowdwork – digitale Wertschöpfung in der Wolke, in: Benner, Christiane (Hrsg.): Crowdwork – Zurück in die Zukunft: Perspektiven digitaler Arbeit, Frankfurt, S. 9 – 42.

Mert, Akif 2016: Compliance in der Praxis, in Computer und Arbeit (1), S. 18 – 20.

Neuerer, Dietmar 2017: Bundesregierung zerstreitet sich über Datenschutz, in: Handelsblatt, 11.1.2017, http://www.handelsblatt.com/politik/deutschland/merkel-gegen-datensparsamkeit-bundesregierung-zerstreitet-sich-ueber-datenschutz/19237484.html (26.6.2017).

Rozek, Heike 2015: Social Media als Arbeitsmittel: Reichlich Regelungsbedarf für die Interessenvertretung, in Computer und Arbeit (2), S. 4 – 9.

Sassenberg, Thomas; Bamber, Niclas 2006: Betriebsvereinbarung contra BDSG?, in Datenschutz und Datensicherheit 30 (4), S. 226 – 229.

Schwemmle, Michael; Wedde, Peter 2012: Digitale Arbeit in Deutschland, Bonn.

Seifert, Achim 2014: Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses, in: Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz: Kommentar, Baden-Baden, S. 1.436 – 1.525.

Siebenhüter, Sandra 2016: Migration 4.0, in Computer und Arbeit (6), S. 18 – 21.

Simitis, Spiros 2014a: Datenerhebung und -speicherung für eigene Geschäftszwecke, in: Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz: Kommentar, Baden-Baden, S. 1.182 – 1.272.

Simitis, Spiros 2014b: Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen, in: Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz: Kommentar, Baden-Baden, S. 504 – 535.

Simitis, Spiros (Hrsg.) 2014c: Bundesdatenschutzgesetz: Kommentar, Baden-Baden.

Stach, Bert 2015: Ab in die Wolke, in Arbeitsrecht im Betrieb Extra (9), S. 23 – 25.

Steinwender, Frank 2013: Flöhe hüten 2.0 – Mobile Geräte im Sinne der Beschäftigten verwalten, in Computer und Arbeit (9), S. 4 – 6.

Strube, Sebastian 2015: Vom Outsourcing zum Crowdsourcing, in: Benner, Christiane (Hrsg.): Crowdwork – Zurück in die Zukunft: Perspektiven digitaler Arbeit, Frankfurt, S. 75 – 92.

Taeger, Jürgen 2013: Datenerhebung und -speicherung für eigene Geschäftszwecke, in: Taeger, Jürgen; Gabel, Detlev (Hrsg.): BDSG und Datenschutzvorschriften des TKG und TMG, Frankfurt, S. 796 – 885.

Taeger, Jürgen; Gabel, Detlev (Hrsg.) 2013: BDSG und Datenschutzvorschriften des TKG und TMG, Frankfurt.

Tiemeyer, Ernst 2015: Chancen durch Big Data: Einsatzfelder, Potenziale und Perspektiven, in Computer und Arbeit (3), S. 22 – 26.

Trümner, Ralf 2016: §1 Errichtung von Betriebsräten, in: Däubler, Wolfgang; Kittner, Michael; Klebe, Thomas; Wedde, Peter (Hrsg.): Betriebsverfassungsgesetz: Mit Wahlordnung und EBR-Gesetz, Frankfurt, S. 200 – 276.

Wedde, Peter 1995: Digitalisierung der Arbeit – das Ende des Arbeitsrechts, Computerinformation (7), S. 43 ff.

Wedde, Peter 2004: Die wirksame Einwilligung im Arbeitnehmerdatenschutzrecht, in Datenschutz und Datensicherheit 28 (3), 169 – 174.

Wedde, Peter 2014: Konzernweite Datenverarbeitung für eigene Geschäftszwecke auf der Grundlage von § 28 Abs. 1 Satz 1 Nr. 2 BDSG, in: Bussche, Axel von dem; Voigt, Paul (Hrsg.): Konzerndatenschutz: Rechtshandbuch, München, S. 177 f.

Wedde, Peter 2015: Interaktives Intranet: Soziale Firmennetzwerke als Arbeitsmittel der Zukunft, in Computer und Arbeit (4), S. 4 – 9.

Wedde, Peter 2016a: Der analysierte Arbeitnehmer, in Computer und Arbeit (5), S. 14 – 16.

Wedde, Peter 2016b: Datenerhebung und -speicherung für eigene Geschäftszwecke, in: Däubler, Wolfgang; Klebe, Thomas; Wedde, Peter; Weichert, Thilo (Hrsg.): Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG, Frankfurt, S. 491 – 549.

Wedde, Peter 2016c: Anti-Terror-Screening, in Arbeitsrecht im Betrieb (4), S. 19 – 22.

Wedde, Peter 2016d: Die unterschätzte Macht der Mitbestimmung, in Computer und Arbeit (1), S. 8 – 13.

Wedde, Peter (Hrsg.) 2016e: Handbuch Datenschutz und Mitbestimmung, Frankfurt.

Wedde, Peter; Klöver, Karen 1993: Outsourcing – Das Ende der Mitbestimmung?, in Computer und Arbeit (2), S. 93 – 98.

Weichert, Thilo 2016: Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung, in: Däubler, Wolfgang; Klebe, Thomas; Wedde, Peter; Weichert, Thilo (Hrsg.): Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG, Frankfurt, S. 153 – 160.

Weichert, Thilo; Schuler, Karin 2016: Privacy Shield – kein grundrechtskonformer Ersatz für Safe Harbor, Dokumentation und Bewertung, Kiel/Bonn 2016, www.netzwerk-datenschutzexpertise.de/sites/default/files/doku_2016_02_privacy_shield.pdf (26.6.2017).

Wilke, Matthias 2006: Data Mining – Rasterfahndung im Betrieb, in Arbeitsrecht im Betrieb (3), 155 – 162.

Wolff, Amadeus; Brink, Stefan 2015: Beck'scher Online-Kommentar Datenschutzsrecht, München, (1.8.2015).

Impressum:

Friedrich-Ebert-Stiftung
Herausgeberin: Abteilung Wirtschafts- und Sozialpolitik
Godesberger Allee 149, 53175 Bonn
Fax 0228 883 9205, www.fes.de/wiso

Bestellungen/Kontakt: wiso-news@fes.de

ISBN: 978-3-95861-853-4

Titelmotiv: © dpa Picture Alliance; gonin/fotolia.com
Gestaltungskonzept: www.stetzer.net
Layout: www.pellens.de
Druck: www.bub-bonn.de

ABTEILUNG WIRTSCHAFTS- UND SOZIALPOLITIK

WEITERE VERÖFFENTLICHUNGEN ZUM THEMA

Digitale Plattformen: Ein neues Handlungsfeld für die Daseinsverantwortung des Staates?
WISO direkt – 09/**2017**

Industrie 4.0 und der rheinische kooperative Kapitalismus
WISO direkt – 03/**2017**

Digitalisation and Low-Skilled Work
WISO Diskurs – 19/**2016**

The Future of Low-Skilled Industrial Work
WISO direkt – 25/**2016**

The Impacts of Digitalisation on the Working Environment
WISO direkt – 26/**2016**

Innovationsstrategien in Zeiten der Digitalisierung: Ein Vergleich der Innovationspolitik in Finnland, Schweden und Deutschland
Gute Gesellschaft – Soziale Demokratie #2017plus – 2016

Gute Digitale Arbeit: Auswirkungen der Digitalisierung im Dienstleistungsbereich
WISO Diskurs – 16/**2016**

Folgen der Digitalisierung für die Arbeitswelt
WISO direkt – 17/**2016**

Digitalisierung und Einfacharbeit
WISO Diskurs – 12/**2016**

Die Zukunft einfacher Industriearbeit
WISO direkt – 12/**2016**

Policies for Innovation in Times of Digitalization
Good Society – Social Democracy 2017plus – 2016

#DigiKon15 – die digitale Gesellschaft: Impulse zum Digitalisierungskongress
Gute Gesellschaft – Soziale Demokratie #2017plus – 2015

Herausforderung Verbraucherdatenschutz in der digitalen Welt
Gute Gesellschaft – Soziale Demokratie #2017plus – 2015

Verhandelbare Flexibilität? Die Gewerkschaften vor neuen Aufgaben in der digitalen Arbeitswelt
WISO direkt – 29/**2015**

Soziale Innovationspolitik für die Industrie 4.0
Gute Gesellschaft – Soziale Demokratie #2017plus – 2014

FRIEDRICH EBERT STIFTUNG

Volltexte dieser Veröffentlichungen finden Sie bei uns im Internet unter

www.fes.de/wiso