Arbeit 4.0 und Beschäftigtendatenschutz

Herausforderungen und rechtlicher Anpassungsbedarf

TransWork

INPUT consulting

Impressum:

INPUT Consulting – Gemeinnützige Gesellschaft
für Innovationstransfer, Post und Telekommunikation mbH
Theodor-Heuss-Straße 2
70174 Stuttgart
www.input-consulting.de

Autor:
Dr. Edgar Rose (Carl von Ossietzky Universität Oldenburg)

Gestaltung:
Regine Lieb, klip GmbH

Die vorliegende Publikation entstand im Rahmen des Verbundprojekts »TransWork – Transformation der Arbeit durch Digitalisierung«, Teilvorhaben »Entwicklung von Gestaltungs- und Regulierungslösungen vernetzter Arbeitsformen«.
Das Forschungs- und Entwicklungsprojekt TransWork wird mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) in der Fördermaßnahme »Arbeit in der Digitalisierten Welt« gefördert und vom Projektträger Karlsruhe (PTKA) betreut.
Förderkennzeichen des Teilvorhabens »Entwicklung von Gestaltungs- und Regulierungslösungen vernetzter Arbeitsformen«: 02L15A161.
Die Verantwortung für den Inhalt dieser Publikation liegt beim Autor.

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

BETREUT VOM

PTKA
Projektträger Karlsruhe
Karlsruher Institut für Technologie

Förderschwerpunkt
Arbeit in der
digitalisierten Welt

Stuttgart, April 2021

Inhalt

0. EINLEITUNG

Zu Beginn der 20er Jahre des 21. Jahrhunderts steht der Beschäftigtendatenschutz vor außergewöhnlichen Belastungsproben. Denn die aktuellen Bestrebungen und die dafür vorhandenen technischen Möglichkeiten einer allseitigen Digitalisierung der Arbeitswelt lassen die Erfassung personenbezogener Daten im Arbeitsverhältnis in Umfang und Eingriffstiefe geradezu explodieren. Für alle Funktionalitäten der Wertschöpfung durch menschliche Arbeit einschließlich des darauf bezogenen Managements werden in schneller Folge immer neue technische Lösungen mit immer höheren Kapazitäten der Datenverarbeitung angeboten und angewandt. In der juristischen Fachdebatte wird dies nicht bestritten, aber weithin vertreten, dass diese Herausforderungen mit den herkömmlichen rechtlichen Mitteln – jedenfalls bei kreativer Anwendung – sinnvoll zu beherrschen seien.[1] Skeptische Stimmen sehen hingegen erheblichen Bedarf, die Regelungsinstrumente deutlich zu schärfen.[2] Auch in diesem Beitrag wird die vorherrschende Einschätzung in Frage gestellt.

Vorgelegt werden in dieser Publikation insgesamt 5 Teilstudien. In *Kapitel 1* werden die absehbaren Auswirkungen der Digitalisierungsbestrebungen auf die Verarbeitung von Beschäftigtendaten an drei Beispielen untersucht. Untersucht werden aktuelle Trends der Digitalisierung der Arbeitsprozesse, des Personalmanagements und des Arbeitsschutzes. In *Kapitel 2* folgt eine explorative Studie zu den Zielen des Beschäftigtendatenschutzes. Es geht in einer Reihe von Thesen um den viel zu selten betrachteten Wert des Datenschutzes für Beschäftigte. *Kapitel 3* enthält den juristischen Untersuchungsschwerpunkt unter der Frage, welches Potenzial das geltende Recht für einen wirksamen Beschäftigtendatenschutz auch künftig bietet. In einem ersten Teil wird hier zunächst umrissen, was der Begriff Beschäftigtendatenschutz an Regelungsinstrumenten umfasst. Es geht um weit mehr als um § 26 BDSG. Im zweiten Teil werden dann ausgewählte Einzelregelungen analysiert. *Kapitel 4* fasst zunächst die wissenschaftliche Diskussion der letzten 5 Jahre zusammen, um aus den öffentlich vorliegenden Beiträgen und Expertisen die Sicht der juristischen Wissenschaft auf die Defizite des geltenden Rechts und erforderliche Anpassungen zu ermitteln. Regelungsideen werden diskutiert, ergänzt und zusammengestellt. Schließlich wird in *Kapitel 5* eingangs untersucht, wie der europarechtliche Regelungsspielraum für erforderliche Anpassungen gesteckt ist, um vor diesem Hintergrund anhand von vier Regelungsprojekten Handlungsmöglichkeiten des Gesetzgebers zu benennen.

Diese rechtswissenschaftliche Studie zu den neuen Herausforderungen und dem regulatorischen Anpassungsbedarf beim Beschäftigtendatenschutz durch die immer weiter fortschreitende Digitalisierung der Arbeitswelt wurde als Auftragsarbeit von Dr. Edgar Rose (Carl von Ossietzky Universität Oldenburg) im Rahmen des vom Bundesministerium für Bildung und Forschung geförderten Projekts „TransWork – Transformation der Arbeit durch Digitalisierung“ verfasst. Das Projekt Transwork ist ein gemeinsames Verbundvorhaben von Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO (Stuttgart), ifaa – Institut für angewandte Arbeitswissenschaft e.V. (Düssel-

[1] *Dzida*, NZA 2017, 541 (546); *Hofmann*, ZD 2016, 12 (17); *Hornung/Hofmann*, Datenschutz als Herausforderung der Arbeit in der Industrie 4.0, in: Hirsch-Kreinsen/Ittermann/Niehaus, 2. Aufl., 2018, S. 233 (248 f.); *Jaspers/Jacquemain,* RDV 2019, 232 (235); *Kort*, RdA 2018, 24 (33) sowie bei unterstützenden Eingriffen des Gesetzgebers auch *Dietrich/Bosse/Schmitt*, Kontrolle und Überwachung von Beschäftigten, DuD 2021, 5 (10).

[2] Aus unterschiedlichen Gründen skeptisch: *Haußmann/Thieme*, NZA 2019, 1612 (1620); *Krause*, NZA-Beilage 2017, 53 (58); *Krause*, Digitalisierung und Beschäftigtendatenschutz, BMAS Forschungsbericht 482, 2017; *Martini/Botta*, NZA 2018, 625 (636 f.); *Weichert*, NZA 2020, 1597 (1599 f.).

dorf), RWTH Aachen, Institut für Arbeitswissenschaft (IAW), ver.di-Vereinte Dienstleistungsgewerkschaft (Berlin) und INPUT Consulting gGmbH (Stuttgart). Das Teilvorhaben „Entwicklung von Gestaltungs- und Regulierungslösungen vernetzter Arbeitsformen“, in dem auch Fragen des Beschäftigtendatenschutzes thematisiert werden, wird im Transwork-Projektverbund von INPUT Consulting gGmbH bearbeitet.

1. HERAUSFORDERUNGEN

Das *erklärte Ziel* der gegenwärtigen technischen Entwicklung besteht darin, alle Aspekte der primären und der sekundären Leistungserbringung quer durch alle wirtschaftlichen Sektoren zu digitalisieren.[3] Angestrebt wird programmatisch z. B. von der „Plattform Industrie 4.0“[4] „die Verfügbarkeit aller relevanten Informationen in Echtzeit durch Vernetzung aller an der Wertschöpfung beteiligten Instanzen sowie die Fähigkeit aus den Daten den zu jedem Zeitpunkt optimalen Wertschöpfungsfluss abzuleiten.“ Dieser eine Satz macht eindrucksvoll und paradigmatisch deutlich, welche enorme Bedrohung für den Beschäftigtendatenschutz hier anrollt, wenn (nochmal im Einzelnen)

- alle relevanten Informationen
- aller an der Wertschöpfung beteiligten Instanzen
- in Echtzeit vernetzt
- und zwecks jederzeitiger Optimierung

analysiert werden sollen.

Denn solange Menschen in den Unternehmen arbeiten, ist klar, dass nicht alle, aber ein großer Teil dieser Informationen in Form von personenbezogenen Daten vorliegt. Nur dem Umstand, dass die Umsetzung der weitreichenden Digitalisierungspläne an den Arbeitsplätzen viel Zeit braucht, teilweise auf Skepsis stößt und häufig in der Praxis noch stockt, ist es zu verdanken, dass ein begrenztes Zeitfenster dafür verbleibt, die Belange des Datenschutzes bereits bei Einführung der 4.0-Technik wirksam einfließen zu lassen.

In diesem Kapitel wird zunächst eine Bestandsaufnahme der aktuellen Gefährdungslage für die informationelle Selbstbestimmung der Beschäftigten vorgenommen. Dabei seien drei zentrale inhaltliche Schwerpunkte herausgegriffen, in denen der Beschäftigtendatenschutz vor besonderen Herausforderungen steht:

- Die *Digitalisierung der Arbeitsprozesse* in der Produktion[5] und vielen Dienstleistungsbereichen[6] lässt zwei aktuelle Tendenzen erkennen: Big Data und autonome Systeme. Big Data heißt hier vor allem, dass allgegenwärtige Sensorik vernetzt im IoT permanent Daten sammelt, die mit ständig verbesserter Analysesoftware zielgerichtet ausgewertet werden, um sie dem Arbeitsprozess wieder zur Verfügung zu stellen. Autonome Systeme gehen einen Schritt weiter, weil die permanente Datenanalyse unmittelbar in Aktion umgesetzt wird. Autonome Fahrzeuge oder kollaborative Roboter (Cobots) sollen selbsttätig, aber in unmittelbarer Interaktion mit Menschen sinnvoll agieren können.
- Die *Digitalisierung des Personalmanagements*[7] bei der Findung, Förderung und Motivation von Talenten schreitet voran. Ein neues Leitbild einer wissenschaftlich-analytischen

[3] *Bauer/Hofmann*, Arbeit, IT und Digitalisierung, in: Hofmann (Hrsg.), Arbeit 4.0 – Digitalisierung, IT und Arbeit, 2018, S. 1 f.; *Lang*, Quo vadis Digitale Revolution, in: Hermeier/Heupel/Fichtner-Rosada (Hrsg.), Arbeitswelten der Zukunft, 2019, S. 5.
[4] So schon 2015 im Ergebnisbericht der *Plattform Industrie 4.0* (Hrsg.), Umsetzungsstrategie Industrie 4.0, 2015, S. 8.
[5] Siehe Beiträge in: *Hirsch-Kreinsen/Ittermann/Niehaus* (Hrsg.), Digitalisierung industrieller Arbeit, 2. Aufl., 2018.
[6] Siehe Beiträge in: *Ernst/Zühlke-Robinet/Finking/Bach* (Hrsg.), Digitale Transformation – Arbeit in Dienstleistungssystemen, 2020.
[7] *Huff/Götz*, NZA-Beilage 2019, 73.

Personalpolitik greift Platz.[8] Betriebliche (und außerbetriebliche) Datenbestände sollen für Big Data-Analysen fruchtbar gemacht werden, um die Belegschaft zu optimieren.

- Die *Digitalisierung des Arbeitsschutz- bzw. Gesundheitsschutzmanagements*[9] muss hier zur ständigen Verbesserung der Sicherheit und des Gesundheitsschutzes am Arbeitsplatz mitziehen. Der Arbeitgeber ist verpflichtet, den aktuellen Stand der Technik zu gewährleisten. Hier geht es um besonders sensible Gesundheitsdaten. Das gilt verstärkt, seitdem die psychische Gesundheit im Arbeitsschutz ernsthaft berücksichtigt wird.[10]

Die nachfolgende Analyse konzentriert sich auf diesen drei Feldern methodisch auf Herausforderungen, die für den Beschäftigtendatenschutz besonders relevant sind und wird daher von den Fragen geleitet:

- Werden personenbezogene Daten in besonderem Umfang oder besonderer Eingriffstiefe (Stichwort: sensible Daten) verarbeitet?
- Werden diese Daten in betrieblichen Netzen geteilt, insbesondere mit solchen zur gleichen Person zusammengetragen?
- Werden diese Daten über einen unmittelbaren Zweck hinaus gespeichert und analysiert?
- Gibt es Anlass, den Personenbezug der Daten im Verarbeitungsprozess beizubehalten?

1.1 DIE DIGITALISIERUNG DER ARBEITSPROZESSE

Die Diskussion um die aktuelle Digitalisierungswelle ist keineswegs neu. Sie hat bereits im Jahre 2011 unter dem Schlagwort Industrie 4.0 begonnen, das später um den Begriff Arbeit 4.0 ergänzt worden ist, als klar wurde, dass sich nicht nur die Technik verändern wird.[11]

In diesem Sinne digitalisiert werden sollen nicht nur die primären Produktions- und Dienstleistungsprozesse, sondern auch alle darauf bezogenen administrativen und logistischen Funktionen. Digitalisiert werden soll schließlich auch die Unternehmensführung als solche in ihren Entscheidungs- und Lenkungstätigkeiten, auch wenn die Letztentscheidung noch vielfach beim Menschen verbleiben mag.[12]

1.1.1 TECHNISCHE TRENDS

Wie immer, wenn in Betriebswirtschaft und Arbeitswissenschaften ein neuer Hype[13] losgebrochen wird, ergießen sich viele bunte Buzzwords durch die Fachmedien, die hier nur beispielhaft aufgegriffen werden sollen. Die „vierte industrielle Revolution", heißt es,[14] werde durch eine noch nie da gewesene Vernetzung über das Internet und durch die Verschmelzung der physischen mit der virtuellen Welt, dem Cyberspace, zu so genannten „Cyber-Physical Systems" (CPS) gekennzeichnet. Grundlage der nächsten Innovationswelle sei das „Internet der Dinge (IoT), Daten und Dienste", ein „Internet of Everything", in dem Subjekte und Objekte gleichermaßen in Echtzeit

[8] *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner (Hrsg.), Arbeit 4.0 aktiv gestalten, 2018, S. 108.
[9] Vgl. die Beiträge in: *Matusiewicz/Kaiser* (Hrsg.), Digitales Betriebliches Gesundheitsmanagement, 2018.
[10] *Balikcioglu*, NZA 2015, 1424, 1425; *Sasse/Schönfeld*, RdA 2016, 346; *Stück*, ArbRAktuell 2015, 515.
[11] *BMAS* (Hrsg.), Weißbuch Arbeiten 4.0, 2017.
[12] Vgl. *Weber/Kiefer/Jobst*, NZG 2018, 1131.
[13] Industrie 4.0 als Hype beschreiben *Wilkesmann/Stenden/Schulz*, Industrie 4.0 – Hype, Hope oder Harm, Arbeit, 2018, S. 129 (133).
[14] *Kagermann*, Chancen von Industrie 4.0 nutzen, in: Bauernhansl et al. (Hrsg.), Industrie 4.0 in Produktion, Automatisierung und Logistik, 2014, S. 603.

kommunizieren können.[15] Die digitale Transformation werde dann vor allem durch „Hyperkonnektivität", „Autonomie" und „Mensch-Maschine-Interaktion" angetrieben.[16]

Hirsch-Kreinsen[17] weist allerdings völlig zutreffend daraufhin, dass der Hype nicht nur Hype ist, sondern eine reale Grundlage habe; denn jenseits aller rhetorischen Übertreibungen greife ein technologischer Entwicklungsschub mit ungeahnten strukturellen Konsequenzen Platz. Der Kern der Entwicklung sei, dass die Leistungsfähigkeit der Hardware in den letzten Jahren ebenso dramatisch gestiegen ist, wie ihre Kosten gefallen sind.

Mit der dadurch greifbaren Möglichkeit, jeden Raum, jeden Arbeitsplatz, jedes Gerät, jede Maschine, jedes Fahrzeug, jedes Produkt und jede Person mit Sensoren kostengünstig auszustatten,[18] die Daten erfassen, auswerten und vor allem übermitteln können, kann jene digitale Transformation, die in den Medien und im Handel bereits weitgehend stattgefunden hat, auf den Produktionssektor und weitere bisher schwach digitalisierte Dienstleistungssparten übertragen werden. So wird das Versprechen realistisch, dass erhebliche Effizienzsteigerungen durch enorme Datenmengen („Big Data") und ständig verbesserte Datenanalysemethoden erreicht werden können.

Für den Beschäftigtendatenschutz ist das eine schlechte Nachricht. Streift man alle utopischen Phantasien des 4.0-Hypes ab, so bleibt als realer Kern, dass es ständig technisch einfacher und zugleich billiger wird, eine wachsende Zahl arbeitsbezogener Daten nicht nur zu erheben, sondern auch sinnvoll zu vernetzen und vielfältig zu verwerten.

Unterschieden werden müssen allerdings zwei Entwicklungen:

- der unmittelbare Informationsaustausch zwischen technischen Einrichtungen (Internet of Things – IoT), der durch allgegenwärtige Sensorik für jeden Betrieb (bzw. Unternehmen, Konzern, Lieferkette) auswertbare Big Data-Pools erzeugt,
- die fortschreitende Einführung autonom lernender Software (Künstliche Intelligenz - KI), die die Dinge (Geräte, Fahr- und Flugzeuge, Maschinen) zum Leben erwecken kann.

Die zweite Entwicklung fordert weit mehr, als Daten zu erfassen und dann, um Rationalisierungspotenziale sichtbar zu machen, auszuwerten. Hier wird es in Zukunft darum gehen, KI durch intensive Interaktion Mensch-Maschine zu trainieren. Einerseits soll menschliches Know-how auf die Maschinen übertragen werden. Zugleich gilt es, die Mensch-Maschine-Interaktion durch ständigen Datenfluss zu verbessern. So müssen bewegliche Systeme die Zusammenarbeit Hand-in-Hand mit dem Menschen durch ständige Datenanalyse erlernen und fortgesetzt beherrschen. Im Weißbuch Arbeit 4.0 des BMAS hieß es schon 2017, dass hochentwickelte Sensorik eine räumlich immer engere Zusammenarbeit von Mensch und Roboter möglich mache, da die Maschinen mit verbesserten Technologien der Spracherkennung, Bilderkennung, Emotionsmessung sowie der Erfassung von Blickbewegungen und Gesten das Verhalten ihrer Anwender*innen zunehmend

[15] Ebenda S. 604.
[16] *Jacobs/Kagermann/Sattelberger/Lange*, Zukunft der Arbeit: Die digitale Transformation gestalten, in: Werther/Bruckner (Hrsg.), Arbeit 4.0 aktiv gestalten, 2018, S. 24 f.
[17] *Hirsch-Kreinsen,* Einleitung: Digitalisierung industrieller Arbeit, in: ders./Ittermann/Niehaus (Hrsg.), Digitalisierung industrieller Arbeit, 2. Aufl., 2018, S. 13 (14).
[18] Vgl. *Cernavin/Lemme*, Technologische Dimensionen der 4.0-Prozesse, in: Cernavin/Schröter/Stowasser, Prävention 4.0, 2018, S. 21 (24).

genauer registrieren können.[19] Diese kurze Aufzählung macht bereits deutlich, von welchem Ausmaß und welcher Eingriffstiefe der personenbezogenen Datenverarbeitung beim künftigen Einsatz kollaborativer Roboter[20] gerechnet werden muss.

Es besteht heute weitgehend Einigkeit darüber, dass die Potenziale der Digitalisierung erst durch eine partnerschaftliche Kooperation zwischen Mensch und Technik voll ausgeschöpft werden können.[21] Mensch-Technik-Schnittstellen sind zukünftig von zentraler Bedeutung. Vielfach hat die Vorstellung, Roboter würden den Menschen schlicht ersetzen, mit der absehbaren Realität wenig zu tun. Vielmehr geht es derzeit darum, dass eine enge Kooperation zwischen Mensch und Technik ermöglich wird, damit sich die Stärken der Technik – beispielsweise Wiederholbarkeit, Genauigkeit und Ausdauer – und die besonderen menschlichen Fähigkeiten wie Kreativität und Flexibilität optimal ergänzen.[22]

Das ist eine weitere schlechte Nachricht für den Beschäftigtendatenschutz, denn der künftig tatsächlich kollaborative Roboter kann gar nicht anders – funktional und aus Sicherheitsgründen, als ständig alle für ihn erkennbaren Lebensäußerungen seiner menschlichen Kollaborationspartner*innen auszuwerten.[23] Dass er dabei nicht vernetzt sein soll, widerspräche dem aktuellen Digitalisierungsparadigma.

1.1.2 EINZELASPEKTE

Mit den technischen Möglichkeiten der Erfassung von Beschäftigtendaten wachsen auch die betriebswirtschaftlichen Gründe, dies zu tun. Das führt zu einem sich selbst verstärkenden Effekt. Bestand der Urgrund des Beschäftigtendatenschutzes in der Begrenzung der Verhaltens- und Leistungsüberwachung durch Technik (siehe § 87 Abs. 1 Nr. 6 BetrVG), so haben aktuelle Überwachungstechnologien wichtige weitere Zwecke zu erfüllen. Im ersten Schritt geht es darum, teilautomatisierten Arbeitsprozesse zu kontrollieren, Funktionsstörungen frühzeitig zu erkennen und Verbesserungsmöglichkeiten zu identifizieren. Im nächsten Schritt wird diese Überwachung automatisiert. Selbstlernende Systeme reagieren selbst auf Anzeichen von Funktionsstörungen, sie trainieren und verbessern sich selbst, sie entscheiden letztlich selbst, welche Daten benötigt und auf welche Weise ausgewertet werden. Das heißt aber nicht, dass die Daten einfach verborgen im System verbleiben. Schon aus rechtlichen Gründen etwa der Produkthaftung kann kein Management diese selbsttätigen Prozesse einfach sich selbst überlassen, sondern braucht Methoden bzw. Formen der Hyperüberwachung. Auf allen Ebenen sind dabei immer auch Beschäftigte im Blickfeld. Denn wo der Mensch die mögliche Fehlerquelle ist, muss diese auch identifiziert werden können.

[19] BMAS (Hrsg.), Weißbuch Arbeiten 4.0, 2017, S. 68.
[20] Siehe auch *Steil/Maier*, Kollaborative Roboter: universale Werkzeuge in der digitalisierten und vernetzten Arbeitswelt, in: Maier/Engels/Steffen (Hrsg.), Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, 2020, S. 323 ff.; *Buxbaum/Kleutges*, Evolution oder Revolution? Die Mensch-Roboter-Kollaboration, in: Buxbaum (Hrsg.), Mensch-Roboter-Kollaboration, 2020, S. 15 ff.
[21] Ebenda.
[22] *Bauer/Hämmerle/Bauernhansl/Zimmermann*, Future Work Lab – Arbeitswelt der Zukunft, in: Neugebauer (Hrsg.), Digitalisierung, 2018, S. 179 (181 f.).
[23] *Steil/Maier*, Kollaborative Roboter: universale Werkzeuge in der digitalisierten und vernetzten Arbeitswelt, in: Maier/Engels/Steffen (Hrsg.), Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, 2020, S. 323 (337 f.).

a) Überwachung der Arbeitsprozesse, insbesondere: Videoüberwachung

In der aktuellen Terminologie müsste wohl anstatt von Videoüberwachung von optischer Sensorik gesprochen werden. Die Videoüberwachung gehört einerseits zu den ältesten Themen des betrieblichen Datenschutzes und ist schon Gegenstand vielfältiger Urteile der Arbeitsgerichtsbarkeit gewesen.[24] Andererseits ist das Thema hochaktuell. Denn erstens nehmen derzeit die Fähigkeiten der Bildauswertung rasant zu (Stichworte: Gesichtserkennung, Emotionsanalyse, Intelligente Videoüberwachung)[25]. Zweitens gehört es zu den Charakteristika (teil)autonomer Technik, sie vielfach mit optischer Sensorik auszustatten. Bei einem e-Golf Level 4 Automatisierungsgrad sind 11 Laserscanner, 7 Radare sowie 14 Kameras an Bord.[26] Hochsensible optische Sensorik wird unweigerlich auch zur Ausstattung künftiger kollaborativer Roboter gehören.

Außerhalb des Feldes der optischen Überwachung kann vielfältige Sensorik Arbeitsprozesse zwecks Verhaltens- bzw. Leistungsüberwachung aufzeichnen,[27] z. B.:

- Dokumentation der Bildschirmanzeige- bzw. Tastaturnutzung durch entsprechende Programme in den PCs, Tablets und sonstigen elektronischen Devices, die Beschäftigte für die Arbeit nutzen bzw. mit sich führen. Das beginnt bei reiner Leistungskontrolle oder der Abschreckung hinsichtlich privater Nutzung und setzt sich in inhaltlicher Kontrolle (z. B. Fraud Detection) fort.
- Akustische Aufnahmen, insbesondere Sprachaufnahmen am Telefon, die vorwiegend bei Call-Center-Mitarbeiter*innen eingesetzt werden. Zur reinen Überwachungsfunktion kann hier die Analyse von Emotionen bis hin zur Persönlichkeitsdurchleuchtung treten.
- Ortungssysteme auf Basis von GPS-Verfolgung insbesondere für die Fahrzeugflotte in der Logistik oder im Außendienst (gern auch bei Fahrrädern) oder RFID-Tags z. B. in der Dienstkleidung, die Aufenthaltsorte auf dem Betriebsgelände anzeigen.[28] Werden diese Aufenthaltsorte dokumentiert ergeben sich Bewegungsprofile.
- Zu erwähnen ist weiter, dass Beschäftigte zunehmend elektronische Tools bei sich tragen. Das wichtigste Gerät ist das Smartphone. Hinzu kommen vor allem Smart Watches und diverse Activity Tracker, die etwa Schritte zählen oder den Puls messen. Angesichts der raschen technischen Entwicklung ist die mögliche Aussagekraft dieser Tools nicht zu unterschätzen. Werden sie in den betrieblichen Datenfluss eingebunden, können sie zum Überwachungstool werden.[29]

Nichts davon ist grundsätzlich neu. Das neue Problem ist die aktuell platzgreifende Zielsetzung, alle relevanten Datenquellen zu vernetzen und die Daten für Auswertungszwecke zu verknüpfen. Es liegt auf der Hand, hierbei auch Überwachungsdaten einzubeziehen. Nicht der misstrauische Arbeitgeber oder Vorgesetzte ist hierbei die treibende Kraft, sondern die zu erprobende intelligente Analysetechnik zur Prozessoptimierung. Je mehr Daten sie bekommt, desto besser soll sie werden. Neu ist außerdem, dass die Auswertung ständig dahingehend optimiert wird, aus den vorhandenen Daten weitreichende Rückschlüsse z. B. auf Stärken und Schwächen einzelner Be-

[24] Siehe schon BAG v. 7. 10. 1987 - 5 AZR 116/86, NZA 1988, 92; im Überblick *Däubler*, Gläserne Belegschaften, 8. Aufl., 2019, S. 207 ff.; *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, S. 277 ff.
[25] *Heldt*, MMR, 2019, 285.
[26] www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/autonomes-fahren/technik-vernetzung/aktuelle-technik/
[27] *Däubler*, Gläserne Belegschaften, Frankfurt a.M., 8. Aufl., 2019, S. 219 ff.; *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, S. 277 ff.; *Krause*, Digitalisierung und Beschäftigtendatenschutz, BMAS Forschungsbericht 482, 2017, 12 ff.
[28] Eingehend *Däubler*, Gläserne Belegschaften, 8. Aufl., 2019, Rn. 318 ff.; *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, Rn. 1225 ff.
[29] Siehe schon *Kopp/Sokoll*, NZA, 2015, 1352.

schäftigter, auf Beratungs- oder Schulungsbedarf oder auf Fälle kritischer Überbelastung zu ziehen (siehe unten 1.2). Unter Anwendung des aktuellen Digitalisierungs-Paradigmas bekommen also traditionelle Überwachungstechniken eine völlig neue Qualität. Zugleich wird die Aussagekraft der gewonnenen Daten ständig gesteigert.

b) Elektronische Assistenz

Elektronische Assistenzsysteme sind ein sehr weites Feld. Es beginnt beim stationären PC am Büroarbeitsplatz und reicht über diverse mobile Bildschirmgeräte bis hin zu vielfältigen speziellen Entwicklungen, um bestimmte Tätigkeiten zu erleichtern, z. B. Datenbrillen, Drohnen, Hebevorrichtungen, Spezialanzüge. Datenschutzrechtlich besonders interessant werden diese, wenn sie personalisiert sind und womöglich noch vernetzt sind.

Als einfaches Beispiel sei hier das in der Logistik verbreitete Gerät eines Strichcodescanners mit Display angesprochen.[30] Das Gerät registriert bei Auslieferungsarbeiten, welche Pakete an Bord sind, berechnet die Route und führt zum Zielort. Ähnliches geschieht in der Lagerarbeit, bei der das System zum richtigen Regalfach führt und die Entnahme überwacht.

Ein einfaches Beispiel für Datenbrillen ergibt sich aus Lagertätigkeiten zur Zusammenstellung von Teilen für die Produktion. Beschäftigte werden vom Brillendisplay zum nächsten Lagerplatz geführt. Gang und Regalfach werden angezeigt. Die Navigationshilfe gleicht persönliche Standortdaten mit den Zieldaten ab. Über das System werden außerdem die einzelnen Arbeitsschritte automatisch dokumentiert.[31]

In beiden Beispielen sollen offensichtlich Fehler der Beschäftigten (falscher Weg, falsches Teil) reduziert werden. Sehr zutreffend wird von „geführter Arbeit“ gesprochen.[32] Ein falscher Griff fällt sofort auf, aber auch eine Verspätung bleibt nicht unentdeckt. Individuelle Zeitreserven können nur um den Preis erarbeitet werden, dass auch das System erfährt, dass und wie es noch schneller geht. Das Unternehmen eignet sich auf diese Weise ununterbrochen das Know-how der Beschäftigten an.

Etwas anders sieht es aus, wenn es um die Unterstützung hochqualifizierter Arbeit geht oder das Assistenzsystem zugleich auch der Arbeitssicherheit oder dem Gesundheitsschutz dient (dazu unten 1.3).

c) Robotik

Das Thema „Robotik“ ist vom vorherigen der „elektronischen Assistenz“ nicht scharf zu trennen, zumal der Trend der Stunde „kollaborative Roboter“ sind,[33] also genau solche, die eng mit dem Menschen zusammenarbeiten sollen. Der Begriff steht hier für das derzeit intensiv beforschte Thema der mobilen, per Sensorik wahrnehmenden Maschine, die aus diesen Wahrnehmungen

[30] *Zanker*, Digitalisierung in der Logistik – Beschäftigung und Qualifikation im Wandel, in: Ernst/Zühlke-Robinet/Finking/Bach (Hrsg.), Digitale Transformation – Arbeit in Dienstleistungssystemen, 2020, S. 55 (59 f.).
[31] *Varadinek/Indenhuck/Surowiecki*, Rechtliche Anforderungen an den Datenschutz bei adaptiven Arbeitsassistenzsystemen, 2018, S. 91.
[32] *Zanker*, Digitalisierung in der Logistik – Beschäftigung und Qualifikation im Wandel, in: Ernst/Zühlke-Robinet/Finking/Bach (Hrsg.), Digitale Transformation – Arbeit in Dienstleistungssystemen, 2020, S. 55 (60).
[33] Vgl. die Beiträge in: *Buxbaum* (Hrsg.), Mensch-Roboter-Kollaboration, 2020.

Aktivitäten ableitet. Ob diese Maschine dabei nur komplexe Handlungsanweisungen ausführt oder auch selbstständig Handlungsimpulse ableitet, sei dahingestellt.

Zwei Probleme beschäftigen die Forschung und Entwicklung in der Robotertechnologie vorrangig: Sicherheit und Wandlungsfähigkeit.[34] Herkömmliche Industrieroboter arbeiten in abgesperrten Zonen, die nur abgeschaltet zu Programmier- oder Wartungszwecken betreten werden. Sie müssen aufwändig von Spezialisten programmiert werden, wenn sie eine neue Tätigkeit ausführen sollen.

Kollaborative Roboter (Cobots) sollen nicht nur im gleichen Raum, sondern direkt mit Menschen zusammenarbeiten. Seit kurzem stehen *flexible Leichtbauroboter* zur Verfügung, die z. B. unvorhergesehenen Kollisionen ausweichen können. Damit werden das Anreichen von Teilen oder einfache Montageschritte realistisch, solange dem Roboter feste Rollen und Arbeitsschritte zugeordnet werden.[35] Aktuell werden auch Fortschritte hinsichtlich höherer Wandlungsfähigkeit der Roboter gemacht. So vermeldet die VDI-Z am 6.7.20: Dank eines neuen Hilfsmittels schaffen es auch ungeübte Mitarbeiter*innen, Industrieroboter einfach und ohne Programmierkenntnisse zu teachen.[36]

In der Fachliteratur wird betont, dass aktuell Maschinen noch weit davon entfernt seien, intelligent und sicher mit Menschen zusammenarbeiten zu können.[37] Noch sind es Visionen, dass Roboter durch Beobachten des Menschen oder eigenes Probieren selbst Handlungsmuster erlernen, menschliches Verhalten antizipieren oder sich flexibel auf überraschende Situationen einstellen können. Es wird aber zielstrebig daran gearbeitet.

Unter Aspekten des Beschäftigtendatenschutzes ist der Cobot der näheren Zukunft vor allem ein zusätzliches Sensorsystem, das unter jeweilig relevanten Aspekten die kollaborierenden Beschäftigten zeitweise oder ständig „beobachtet". So wird etwa der Teile anreichende Roboter die Arbeitsfortschritte des Menschen wahrnehmen, um das richtige Teil zum richtigen Zeitpunkt bereit zu halten. Aus Sicherheitsgründen wird dabei jede Annäherung des Menschen zu registrieren sein.

Instruktiv ist ein Beispiel von *Steil/Maier*.[38] Sie nehmen an, dass in einer hybriden Montage Roboter und Mitarbeiter*innen gemeinsam ein Teil einsetzen und dass dazu beide Seiten gleichzeitig das Teil greifen und bewegen. Dann werde der Roboter, schon aus Sicherheitsgründen, die Kräfte messen, die die Mitarbeiter*innen aufbringen, und sein eigenes Kraftprofil darauf einstellen. Der Roboter könne weiter auch implizit die Tagesform der Mitarbeiter*innen messen und schon eine einfache Auswertung der Daten könne zeigen, ob sie mit der Zeit schwächer oder langsamer werden. In Kombination mit Kamerabild, Arbeitsablauf, Erfolg etc. und vielleicht aufgezeichneten Gesprächen ergäbe sich leicht ein umfassendes Bild von Gesundheitszustand und Wohlbefinden.

[34] *Steil/Maier*, Kollaborative Roboter: universale Werkzeuge in der digitalisierten und vernetzten Arbeitswelt, in: Maier/Engels/Steffen (Hrsg.), Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, 2020, S. 323 (324 f.).
[35] Ebenda S. 326 f.
[36] VDI-Z vom 6.7.20: Roboter programmieren endlich leicht gemacht – dank eines neuartigen Tools, www.ingenieur.de/fachmedien/vdi-z/automatisierung-vdi-z/roboter-programmieren-endlich-leicht-gemacht-dank-eines-neuartigen-tools/.
[37] *Buxbaum/Häusler*, in: Buxbaum (Hrsg.), Mensch-Roboter-Kollaboration, 2020, 293 (296).
[38] *Steil/Maier*, Kollaborative Roboter: universale Werkzeuge in der digitalisierten und vernetzten Arbeitswelt, in: Maier/Engels/Steffen (Hrsg.), Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, 2020, S. 323 (337).

Insbesondere in der Einführungsphase, so könnte man das Beispiel fortführen, würden derartige Daten auch nicht einfach dem Vergessen preisgegeben, sondern zu Optimierungszwecken sorgfältig bewahrt, über längere Zeiträume verglichen, an den Hersteller weitergeleitet und ausgewertet.

Mit Blick auf die fernere Zukunft wird das *Cobot-Teaching* flexibler und zunehmend intelligenter Maschinen eine bedeutende Rolle gewinnen. Angestrebt wird, dass das Teaching nicht durch spezielle Programmierung besonderer Fachkräfte, sondern zunehmend „on the job" durch diejenigen Beschäftigten geschieht, die dann auch mit dem Roboter zusammenarbeiten.[39] Intuitive sprachliche und bildliche Verfahren werden entwickelt. Dies kann durchaus positive Auswirkungen auf die Anreicherung von Anforderungen und Qualifikation der Beschäftigten haben. Zugleich wird der Fluss personenbezogener Daten intensiviert, insbesondere wenn, wofür manches spricht, die Maschine auf jeweilige Kooperationspartner*innen personalisiert wird.[40]

1.2 DIE DIGITALISIERUNG DES PERSONALMANAGEMENTS

„Goldgräberstimmung im Personalmanagement?" wird in den einschlägigen Fachmedien gefragt, die die ständig verbesserten Analysetools für die schnell wachsenden Datenmengen aus Bewerbungs- und Arbeitsprozessen betrachten.[41] Für die Belange des Beschäftigtendatenschutzes ist dies ein hoch brisantes Feld im Kontext der Arbeit 4.0 Dynamik. Denn beim Thema Personal geht es *zwangsläufig um personenbezogene Daten*. Anders als bei der Digitalisierung der Produktion, des Vertriebs oder von Dienstleistungstätigkeiten können anfallende Beschäftigtendaten für die Zwecke eines digitalisierten Personalmanagements allenfalls zum kleineren Teil anonymisiert werden. Denn oftmals macht gerade der Personenbezug die Daten für das Personalmanagement interessant.

Die Digitalisierung von Managementaufgaben ist fester Bestandteil der digitalen Zukunftspläne.[42] Damit sind nicht etwa nur die mit wenig Spielraum vorgegebenen Routinearbeiten der Unternehmensverwaltung gemeint, die einem erneuten Automatisierungsschub unterliegen. Vielmehr soll auch die unternehmerische Entscheidungsfindung gerade bei komplexer oder unsicherer Datenlage zunehmend durch Big Data-Analytik bzw. durch Künstliche Intelligenz maßgeblich vorbereitet werden. Personalentscheidungen bilden hierbei keine Ausnahme – im Gegenteil. Wie in der Fachliteratur vielfältig nachzulesen ist,[43] steht das Personal- oder synonym HR-Management allenthalben unter Druck, die wachsenden Datenmengen der 4.0-Prozesse auch zur Verbesserung der eigenen Entscheidungstätigkeit zu nutzen.

[39] *Wöllhaf*, Mensch-Roboter-Kollaboration – Wichtiges Zukunftsthema oder nur ein Hype?, in: Buxbaum (Hrsg.), Mensch-Roboter-Kollaboration, 2020, 109 (113).
[40] *Steil/Maier*, Kollaborative Roboter: universale Werkzeuge in der digitalisierten und vernetzten Arbeitswelt, in: Maier/Engels/Steffen (Hrsg.), Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, 2020, S. 323 (337 f.).
[41] *Weibel/Schafheitle/Ebert*, Goldgräberstimmung im Personalmanagement? Wie Datafizierungs-Technologien die Personalsteuerung verändern, OrganisationsEntwicklung 3/2019, S. 23-29.
[42] Zum Wandel des Managements siehe *Baudach/Hellge/Schröder/Zink*, Organisationen und Führung 4.0, in: Zink (Hrsg.) 2019, S. 143-186; *Franken/Franken*, Wandel von Managementfunktionen im Kontext der Digitalisierung, in: Hirsch-Kreinsen/Ittermann/Niehaus (Hrsg.), 2. Aufl., 2017, S. 99-120.
[43] Aus der Publikationsflut zur Digitalisierung des HR Managements können hier nur wenige Beispiele genannt werden: *Gärtner*, Smart HRM – Digitale Tools für die Personalarbeit, 2020; *Reindl/Krügl*, People Analytics in der Praxis, Freiburg 2017; *Ternés/Wilke* (Hrsg.), Agenda HR – Digitalisierung, Arbeit 4.0, New Leadership, 2018;

Bevor auf die Phänomene der Digitalisierung des HR-Managements näher eingegangen wird, seien kurz die wesentlichen Funktionen des Bereichs zusammengefasst. Im Personalmanagement besteht das Kerngeschäft aus vier Aufgaben mit diversen Unteraufgaben:[44]

- An erster Stelle ist die *„Personalgewinnung"* zu nennen. Seitdem qualifizierte Arbeitskräfte in vielen Bereichen knapp sind, sehen sich die Unternehmen in einem „War for Talents". Spezialisierte Fachleute betreiben mit hohem Aufwand „Recruiting". Grundlage des Recruiting ist die Personalplanung, in der festgelegt wird, wie viele Beschäftigte mit welchen Fähigkeiten bzw. Talenten benötigt werden. Darauf folgt die Anwerbung von Beschäftigten, die je nach Lage auf dem jeweiligen Arbeitsmarkt weit mehr als eine simple Stellenausschreibung erfordern kann. Bewerben sich mehr Personen, als benötigt werden, findet ein Auswahlprozess mit anschließendem Einstellungsangebot an die Besten statt.
- An zweiter Stelle seien die Funktionen des *„Personaleinsatzes"* und der „Personalentwicklung" zusammengefasst. Beim Personaleinsatz geht es um die Integration in das Unternehmen und ins Team. Es erfolgt eine Feinsteuerung der Aufgabenzuweisungen. Es gilt Talente zu entdecken, aber auch Hindernisse der Arbeitsentfaltung aus dem Weg zu räumen. Die weitere Personalentwicklung knüpft daran an. Es geht v. a. um Aus- und Weiterbildung sowie um Karrierechancen innerhalb des Unternehmens, die in der Regel wiederum mit Auswahlprozessen verbunden sind. Es kann auch um die Anpassung der Tätigkeiten bzw. Arbeitszeiten an veränderte Lebensumstände oder Gesundheitszustände gehen. Wichtiges Instrument ist Kommunikation z. B. in Personalentwicklungsgesprächen.
- An dritter Stelle geht es um die Aufgaben der *„Personalmotivation"* und der Entgeltgestaltung. Die Personalmotivation soll sicherstellen, dass der oder die Beschäftigte nicht nur bestens geeignet und qualifiziert ist, sondern auch tatsächlich die erwartete Leistung erbringt. Wichtig ist für viele Unternehmen auch das Ziel, Beschäftigte trotz vielfältiger Alternativen auf dem Arbeitsmarkt zum Bleiben zu motivieren. Die Maßnahmen der Personalmotivation umfassen ein weites Spektrum von der emotionalen Bindung durch Corporate Identity, über Methoden und Stile der Personalführung, Teambildung, Förderung eines freundlichen Betriebsklimas bis hin zum klassischen Setzen von Anreizen, die ihrerseits weit ausdifferenziert sein können, z. B. durch beschäftigtengerechte Arbeitszeiten, interessante oder angesehene Arbeitstätigkeit, gesundheitsförderliche Arbeitsbedingungen und natürlich durch Vergütung in unterschiedlicher Form. Die Felder Personalmotivation und Entgeltgestaltung haben daher eine große Schnittmenge. Ob allerdings Motivation am besten mit Leistungsentgelten und wenn ja mit welcher Variante oder mit fixen Zeitentgelten erzielt werden kann, ist seit Jahrzehnten Gegenstand endloser Fachdebatten.[45]
- An vierter Stelle steht die *„Beendigung"* von Beschäftigungsverhältnissen. So dürfen Konjunkturschwankungen nicht dazu führen, dass benötigte Talente verloren gehen. Anzustreben ist vielmehr, sich von den „Low Performern" zu trennen. Hier geht es verstärkt auch um rechtliche Hürden der Kündigungsschutzgesetzgebung, denn Gekündigte

[44] Als Beleg für die hier genannten Einzelaufgaben kann auf fast jedes Lehrbuch zum Personalmanagement verwiesen werden, z. B. *Huf*, Personalmanagement, 2020; *Stock-Homburg/Groß*, Personalmanagement, 4. Aufl., 2019; aus psychologischer Sicht auch *Treier*, Wirtschaftspsychologische Grundlagen für Personalmanagement, 2019.

[45] Aktuell wird Arbeit 4.0 teilweise als Anlass verstanden, zum Fixentgelt zurückzukehren, vgl. *Kienbaum/Gunnesch/Pacher*, Geld und Vergütung im Zeitalter der Digitalisierung: Wie sieht das Performance Management von morgen aus?, in: Fortmann/Kolocek (Hrsg.) 2018, S. 27 (43 ff.).

scheuen den Gang zum Gericht oft nicht. Digitalisierung kann hier auch LegalTech bedeuten.

Soll eine Digitalisierung der Entscheidungsfindung auf all diesen Feldern des Personalmanagements in fachlich seriöser Weise stattfinden, so sind in die erforderliche Analyse personenbezogene Daten in großer Zahl und mit hoher Aussagekraft über die Persönlichkeit der Beschäftigten einzubeziehen. Die früheren Phasen der Digitalisierung bedeuteten für das Personalwesen kaum mehr als elektronische Aktenführung, Tabellenkalkulation, E-Mail-Verkehr und Internetzugang sowie im Recruiting vielleicht elektronisch geführte Bewerbungssysteme. Wenn jetzt aber das Management selbst als Leitungs- und Entscheidungstätigkeit digitalisiert wird, ist dies nur auf Basis von „Big Data" möglich. In diesem Zusammenhang bedeutet das *„Big Personal Data"*. Um welche Beschäftigtendaten es dabei genau geht, soll mit Blick auf die einzelnen Felder und die dort üblichen oder aufkommenden Anwendungen erkundet werden.

1.2.1 PERSONALGEWINNUNG

Ein Großteil der Diskussion um die Digitalisierung des HR-Managements bezieht sich auf das „Recruiting". Das dürfte zwei Gründe haben.

Die Personalgewinnung auf dem offenen Arbeitsmarkt findet unter vergleichsweise *hoher Unsicherheit* statt, da das Unternehmen mit den Bewerber*innen in der Regel keine Erfahrungen hat. Um diesen Informationsmangel zu beheben, bieten seit einigen Jahren „Big Data-Analysen" einen möglichen Ausgleich an. Voraussetzung ist, dass tatsächlich "Big" Data über die interessanten Personen zur Verfügung steht. Denkbar ist, personenbezogene Daten im Netz zu suchen (a) sowie im Bewerbungsverfahren gezielt weitere Daten zu erzeugen (b), um auf dieser Grundlage aussagekräftige Analysen über die Qualität der Bewerber*innen durchzuführen.

Der zweite Grund betrifft *hohe Kosten*, die durch Fehlgriffe des Recruiting entstehen können. Dabei spielt das knappe Arbeitskräfteangebot, das in vielen Bereichen höher qualifizierter Arbeit seit einigen Jahren besteht (Fachkräftemangel), eine verschärfende Rolle. Der vielerorts erheblich gestiegene Aufwand für das Recruiting steigert auch den Erfolgsdruck. Vor diesem Hintergrund setzt sich ein HR-Management, das die aktuellen digitalen Analysemethoden, die unter dem Stichwort „People Analytics" (und tendenziell synonym „Workforce Analytics", „HR-Analytics")[46] geführt werden, nicht verwendet, dem Vorwurf aus, fachlich nicht auf dem Stand der Kunst zu arbeiten.

a) Analyse externer Daten

Externe Daten, die für die Personalgewinnung von Interesse sein können, sind alle personenbezogenen Daten, die im Internet über mögliche oder tatsächliche Bewerber*innen gefunden werden können. Es ist also zu unterscheiden zwischen der Suchen nach Bewerber*innen und der Suche nach Daten über Bewerber*innen, die insbesondere bei der Digitalisierung der Personalauswahl helfen sollen.

[46] Zu „People Analytics" *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner (Hrsg.), Arbeit 4.0 aktiv gestalten, 2018, S. 107-132; zu HR-Analytics *Wirges/Ahlbrecht/Neyer*, HR-Analytics, 2020.

Eingesetzt werden Anwendungen, die eine aktive Talentsuche (Talent Mining) im Netz ermöglichen.[47] In HR Lehrbüchern wird dies unter der Rubrik „Active Recruiting" oder „Active Sourcing" geführt.[48] Hintergrund ist die Annahme, dass es viele Beschäftigte gibt, die zwar nicht aktiv nach einem neuen Job suchen, aber – richtig angesprochen – durchaus für einen Arbeitgeberwechsel zu gewinnen sind.[49] Beim Talent Mining werden vor allem in den Sozialen Medien verschiedener Art externe Personen nach bestimmten Anforderungen identifiziert, die für die Personalgewinnung des jeweiligen Unternehmens interessant sind. Dabei sind die berufsbezogenen Plattformen XING und LinkedIn erste Wahl. Aber auch andere Dienste wie Facebook oder Twitter werden nicht verschmäht. So finden sich in der Fachliteratur auch detaillierte Hinweise für das „Talent Mining" bei Twitter.[50] Im Zuge der Digitalisierung gibt es selbstverständlich auch Software, die diese Art der Suche unterstützen kann, und auch Dienstleister, die den Unternehmen ihre Hilfe dabei anbieten.

Liegen Bewerbungen vor, so ist das Hauptproblem des Unternehmens, die am besten für die offenen Stellen geeigneten Bewerber*innen auszuwählen. Von Interesse sind hierbei oft Informationen, die über die direkt tätigkeitsbezogenen Qualifikationen und Fertigkeiten hinausgehen. Auch die Persönlichkeitsstruktur der Einzustellenden soll zum Unternehmen passen. Gerade über Charaktermerkmale soll das Internet häufig Auskunft geben können. Erste Eindrücke finden sich oft schon beim schlichten Nachschauen per Suchmaschine im Netz, ob über Bewerber*innen etwas Interessantes zu finden ist.[51] Typischerweise finden sich im Netz beachtliche Datenmengen, die einzelnen Personen zugeordnet werden können. Das beginnt bei Profilen, die berufs- oder freizeitbezogen auf Social Media Plattformen hinterlegt werden. Hinzu kommen Texte, Bilder und Videos, die personenbezogen im Netz geteilt werden, sowie zahlreiche weitere Spuren im Netz (z. B. Likes), die etwas über die Person aussagen können.

Hochbrisant ist für das Personalmanagement nun die Behauptung, die bereits von einer ganzen Reihe von psychologischen Studien untermauert werden soll,[52] dass aus diesen Netzaktivitäten recht zuverlässige Feststellungen über die Persönlichkeitsstruktur ihrer Urheber herausgelesen werden können. Mehr noch: Per Software soll diese Persönlichkeitsanalyse schnell und billig mit Methoden der Sprachanalyse durchgeführt[53] und perspektivisch auch für die Bewerberauswahl bei der Personalgewinnung eingesetzt werden können.[54] In der Tat haben diese psychologischen bzw. psychometrischen Forschungsergebnisse in der deutschsprachigen HR-Literatur bereits Niederschlag gefunden.[55] Automatisierte linguistische Analysetechniken, die Persönlichkeitsmerkmale der Bewerber*innen zur Verbesserung und Erleichterung der Personalauswahl bestimmen, werden breit fachlich kritisch diskutiert.[56] Eine realistische Anwendungsmöglichkeit wird eher

[47] *Tallgauer/Festing/Fleischmann*, Big Data im Recruiting, in: Verhoeven (Hrsg.) 2020, S. 25 (29 f.).
[48] *Dannhäuser*, Trends im Recruiting, in: ders. (Hrsg.), 4. Aufl., 2020, S. 1 (5 ff.); *Huf*, Personalmanagement, 2020, S. 41; Stock-Homburg/Groß, Personalmanagement, 4. Aufl., 2019, S. 234 f.
[49] *Dannhäuser*, Trends im Recruiting, in: ders. (Hrsg.), 4. Aufl., 2020, S. 1 (5).
[50] *Braehmer*, Warum Sie auf Twitter im Recruiting nicht verzichten dürfen, in: Dannhäuser (Hrsg.), 4. Aufl., 2020, 283 (310 ff.).
[51] In der Praxis häufig laut *Holtbrügge*, Personalmanagement, 7. Aufl., 2018, S. 130.
[52] *Kulkarni/Kern/Stillwell/Kosinsk/Matz/Ungar/Skiena/Schwartz*, Latent human traits in the language of social media: An openvocabulary approach, 2018, PLoS ONE 13(11): e0201703; *Pang/Eichstaedt/Buffone/Slaff/Ruch/Ungar*, The language of character strengths: Predicting morally valued traits on social media. Journal of Personality, 2020, 88: 287–306.
[53] *Park/Schwartz/Eichstaedt/Kern/Kosinski/Stillwell/Ungar/Seligman*, Automatic personality assessment through social media language. Journal of Personality and Social Psychology, 2015, 108(6), 934–952; Pang/Eichstaedt/Buffone/Slaff/Ruch/Ungar, The language of character strengths: Predicting morally valued traits on social media. Journal of Personality, 2020, 88: 287–306.
[54] *Guilfoyle/Bergman/Hartwell/Powers*, Social Media, Big Data, and Employment Decisions: Mo' Data, Mo' Problems?, in: Landers/Schmidt, 2016, S. 127 (141).
[55] *Tallgauer/Festing/Fleischmann*, Big Data im Recruiting, in: Verhoeven (Hrsg.) 2020, S. 25 (31).
[56] Ebenda, S. 25 (32 ff.); Weckmüller/Büttner, Big Data in der Personalauswahl, Personalmagazin 3/2017, S. 26-28.

nicht bei externer Social Media Data, sondern bei Sprachdaten, die im Bewerbungsverfahren erzeugt werden, gesehen.[57]

b) Erzeugung von Daten im Bewerbungsverfahren

Es ist keineswegs neu, dass im Bereich höherer Qualifikation in einem aufwändigen Auswahlverfahren vielfältige Daten erzeugt, gesammelt und ausgewertet werden. So sind mehrtägige Assessment-Center[58] zur eignungspsychologischen Analyse viel älter als der IT-Einsatz im Recruiting. Relativ neu ist dagegen die softwarebasierte Analyse der gesammelten Daten hinsichtlich der Eignung der Bewerber*innen.

Einer Digitalisierung der Personalauswahl kommt es sehr entgegen, dass die Testverfahren bereits seit vielen Jahren auf immer höherem Niveau systematisiert worden sind. Unterschieden werden u. a. Intelligenztests, Persönlichkeitstests oder Verhaltenstests z. B. durch Rollenspiele, Arbeitsproben, Computersimulationen.[59] An die damit gemachten Erfahrungen kann die Entwicklung digitaler Analysetools anknüpfen, mit denen eine Verbesserung der Auswahlqualität erreicht werden soll.

Beispielhaft seien *Persönlichkeitstests* angeführt, in denen international anerkannt die „Big5"-Persönlichkeitseigenschaften (Extraversion, Neurotizismus, Verträglichkeit, Gewissenhaftigkeit, Offenheit für Erfahrungen) per Befragung erfasst werden können. Sie können aber auch aus unterschiedlichen Verhaltens- oder Textdaten per Software elektronisch ermittelt werden – und zwar angeblich zuverlässiger als durch Menschen. So hat ein Forschungsteam um den Associate Professor in Organizational Behavior an der Stanford University Michal *Kosinski* zeigen können, dass Computer, denen eine ausreichende Zahl an Facebook Likes der Getesteten zur Verfügung steht, Persönlichkeitsbeurteilungen nach den „Big5" treffsicherer durchführen können als Menschen anhand klassischer Fragebögen.[60] Eine Reihe weiterer Untersuchungen von *Kosinski* und anderen haben die Möglichkeit einer verlässlichen Persönlichkeitsbeurteilung durch Software z. B. auch durch digitale Sprachanalysen bestätigt.[61]

Da Internetaktivitäten wie Likes oder Social Media-Posts nicht für alle Bewerber*innen gleichermaßen herangezogen werden können und zudem eine Auswertung als rechtlich oder ethisch zweifelhaft betrachtet werden könnte und nach neueren Erkenntnissen auch tatsächlich[62] wird, bevorzugen es viele Unternehmen, die digital auszuwertenden Daten im Bewerbungsverfahren selbst zu erzeugen. Auch dabei spielt das Internet eine zentrale Rolle, denn *Online-Assessments*[63] gewinnen ständig an Bedeutung. Das „Recruiting" hofft, dass diese freiwilligen und oft spieleri-

[57] *Fellner*, Moderne Personalauswahl, 2019, S. 3 f.
[58] Zum aktuellen Stand der Durchführung von Assessment-Centern siehe z. B. *Stock-Homburg/Groß*, Personalmanagement, 4. Aufl., 2019, S. 209 ff.
[59] *Stock-Homburg/Groß*, Personalmanagement, 4. Aufl., 2019, S. 209.
[60] *Youyou/Kosinski/Stillwell*, Computer-based personality judgments are more accurate than those made by humans, Proceedings of the National Academy of Science of the United States of America (PNAS), vol. 112 no. 4, 1036–1040.
[61] *Park/Schwartz/Eichstaedt/Kern/Kosinski/Stillwell/Ungar/Seligman*, Automatic personality assessment through social media language. Journal of Personality and Social Psychology, 2015, 108(6), 934–952; zur Analyse von Characterstärken anhand von Tweets bei Twitter *Pang/Eichstaedt/Buffone/Slaff/Ruch/Ungar*, The language of character strengths: Predicting morally valued traits on social media, Journal of Personality 2020, 88: 287–306.
[62] Bewerber*innen bewerten die Heranziehung von Social Media-Daten und anderen Spuren, die sie im Netz hinterlassen haben, deutlich negativ nach einer Studie von *Kanning/Kraul/Litz*, Einstellungen zu digitalen Methoden der Personalauswahl, Journal of Business and Media Psychology, 2019, 10: 1, S. 57-71 (64 f.).
[63] *Gärtner*, Smart HRM – Digitale Tools für die Personalarbeit, 2020, S. 73.

schen Verfahren (Recrutainment) auf wesentliche höhere Akzeptanz stoßen als allgemeine bewerberbezogene Spurensuche im Netz.

Unilever bittet seit 2016 Hochschulabsolventen an, ein vierstufiges Bewerbungsverfahren zu durchlaufen.[64] Zunächst wird im Netz ein Fragebogen verknüpft mit dem LinkedIn Profile ausgefüllt. Dann gilt es, online bestimmte Spiele zu durchlaufen. Wer diese Hürde genommen hat, muss anhand von Interviewfragen ein Video von sich produzieren. Im vierten Schritt schließlich erfolgt die Einladung der Auserwählten in ein „Discovery Centre", in dem reale geschäftstypische Herausforderungen durchlebt werden. Die so gewonnenen Daten der Bewerber*innen werden autonom von einer Software analysiert, um die am besten geeigneten Personen herauszufiltern.

Diverse Anwendungen, die eine Sprach- oder Videoanalyse für Zwecke des Recruiting durchführen, sind auf dem Markt erhältlich. IBM Watson Personality Insights wird häufig genannt, das mindestens 3500 Wörter für den Persönlichkeitstest benötigt.[65] Werden die Bewerber*innen zudem gebeten, in einem Video Fragen zu beantworten, so wird vielfach nicht nur der Inhalt der Antworten bewertet. Vielmehr soll besondere Software (HireVue, TribePad)[66] aus Gestik, Mimik, Stimmlage usw. Schlüsse ziehen können.[67] Dabei interessiert dann nicht so sehr die berufsspezifische Qualifikation der Analysierten, die sich auch aus Zeugnissen oder Fortbildungszertifikaten ermitteln lässt. Es interessieren vielmehr Charaktereigenschaften wie Einfühlungsvermögen und Kontaktfähigkeit, die z. B. aus einer gut qualifizierten eine besonders erfolgreiche Verkäuferin machen.[68]

Insgesamt hat das HR-Management mindestens zwei Entscheidungen zu treffen. Erstens ist zu klären, auf welche Persönlichkeits- oder Qualifikationsmerkmale es bei der jeweiligen Stellenbesetzung entscheidend ankommen soll. Zweitens ist festzustellen, welche Bewerber*innen dem am besten entsprechen. Nicht nur bei der Beurteilung der einzelnen Kandidat*innen, sondern schon bei der Festlegung und Gewichtung der Kriterien im Vorfeld können Big Data-Analysen helfen. In Betracht kommt, besonders erfolgreiche Beschäftigte auf Stellen, die der zu besetzenden Stelle entsprechen, zu testen, um daraus abzuleiten, welche Merkmale für das Unternehmen besonders relevant sein sollen.[69] Im Beispiel von Unilever hat man bekannte „High Performer" aus der bestehenden Belegschaft das Online-Assessment durchlaufen lassen, um mit diesen die Bewerber-Performance digital abzugleichen.[70]

Die digitalen Recruiting-Anwendungen erzeugen damit personenbezogene Daten vorrangig von Bewerber*innen aber auch von bereits Beschäftigten. Noch brisanter dürfte sein, dass über Bewerber*innen Daten auf mehreren Ebenen erzeugt werden. Erstens geht es um Daten, die die Betroffenen kennen oder jedenfalls kennen können. Diese ergeben sich direkt aus den Texten, die sie einreichen, aus ihren Antworten auf Interviewfragen, bei Tests jeglicher Art oder aus ihrem Auftreten bei Rollenspielen, bei virtuellen Arbeitsproben oder in eingereichten Videos usw. Zweitens werden diese Daten digital analysiert und dabei auch den Betroffenen selbst verborgene Aussagen, versteckte Verhaltensweisen oder psychologisch definierte Persönlichkeitsmerkmale

[64] Direkt einsehbar unter https://www.unilever.com/news/news-and-features/Feature-article/2016/game-on-our-graduate-recruitment-drives-gone-digital.html, dazu *Tallgauer/Festing/Fleischmann*, Big Data im Recruiting, in: Verhoeven (Hrsg.) 2020, S. 25 (31).
[65] *Gärtner*, Smart HRM – Digitale Tools für die Personalarbeit, 2020, S. 74.
[66] Ebenda.
[67] *Verhoeven*, Künstliche Intelligenz im Recruiting, in: Verhoeven (Hrsg.) 2020, S. 113 (122).
[68] Siehe dieses Beispiel bei *Diercks*, Online-Assessment, in: Verhoeven (Hrsg.) 2020, S. 79 (97).
[69] *Dzida*, NZA 2017, 541 (541 f.).
[70] *Gärtner*, Smart HRM – Digitale Tools für die Personalarbeit, 2020, S. 75 f.

ans Licht gebracht. Drittens werden als Ziel des Prozesses Werturteile über die Qualifikation oder auch die Persönlichkeitsstruktur gefällt, die mehr oder auch weniger erfreulich ausfallen können. Das heißt, es entstehen systematisch neue personenbezogene Daten, die die Betroffenen nicht kennen.

1.2.2 PERSONALEINSATZ UND PERSONALENTWICKLUNG

Während sich das Recruiting mit den Daten von Bewerber*innen und damit von (zunächst) Außenstehenden befasst, geht es bei den weiteren Funktionen des Personalmanagements tatsächlich um Beschäftigtendaten. Das HR Management möchte das Potenzial der Eingestellten maximal im Interesse des Unternehmens entfalten. Dazu gilt es, Talente dort zu platzieren, wo sie ihre größte Wirkung zeigen können. Oft müssen Teams zusammengestellt werden, die möglichst gut kooperieren sollen. Es gilt ebenso, die Qualifikation der Beteiligten für die gestellten Aufgaben durch Aus- und Fortbildung gezielt zu verbessern. Betriebliche Bildungsangebote sollen an den Interessen, Karriereambitionen und Begabungen jeweiliger Mitarbeiter*innen zielorientiert anknüpfen.[71]

Für die Erfüllung dieser Aufgaben hat das Personalmanagement schon immer personenbezogene Daten der Beschäftigten analysiert. Die Masse an auswertbaren Daten ist allerdings in den letzten Jahren sprunghaft gestiegen und die Software, die die zielgerichtete Analyse entsprechender Daten unterstützt, wird ständig verbessert.[72]

Genau daran knüpft das HR-Konzept „People Analytics“ an. Es handelt sich dabei nicht um eine bestimmte Software, sondern – wie die Protagonisten[73] betonen – um ein breit angelegtes Konzept, empirisches Wissen über die Belegschaft eines Unternehmens zu mehren und nach wissenschaftlichen Methoden zu analysieren, um Managemententscheidungen zu verbessern. Angestrebt wird nicht nur eine regelmäßige Bestandsaufnahme des Ist-Zustandes nach HR-Kennzahlen, sondern die Ermittlung von Kausalzusammenhängen. Die Frage wäre dann, ob z. B. ein bestimmtes offensives Konzept der Bildung und Stärkung von Teams tatsächlich die Fluktuation senkt. Dabei wird vor schlichten Korrelationen gewarnt.[74] Nicht weil nach Einführung des neuen Konzepts die Fluktuation abgenommen hat, kann bereits auf Kausalität geschlossen werden. Dazu sind zusätzliche Daten erforderlich. An dieser Stelle wird das Personalmanagement dann oft feststellen, dass trotz des umfänglich vorhandenen Datenmaterials aus der IoT-Sensorik, aus personalisierten Assistenzsystemen usw. die entscheidenden Daten für die ambitionierte Fragestellung leider doch fehlen. Zusätzliche Erhebungen mit weiteren personenbezogenen Daten müssen durchgeführt werden. In der Fachliteratur wird z. B. „die wiederholte Messung der Variablen zu verschiedenen Zeitpunkten“ empfohlen, um besser Kausalität beurteilen zu können.[75] Andere empfehlen die Durchführung von Feldexperimenten, bei denen Maßnahmen für eine Teilgruppe ergriffen werden, die mit einer Kontrollgruppe ohne Maßnahme verglichen wird.[76] Aus wissenschaftlicher Sicht sind solche Bemühungen, Fehlschlüsse zu vermeiden, sehr zu begrüßen. Aus

[71] *Nürnberg*, SPA 2019, 149 (151).
[72] *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner (Hrsg.), Arbeit 4.0 aktiv gestalten, 2018, S. 108.
[73] Z. B. *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner (Hrsg.), Arbeit 4.0 aktiv gestalten, 2018, S. 108; *Reindl/Krügl*, People Analytics in der Praxis, Freiburg 2017, S. 15; *Wirges/Ahlbrecht/Neyer*, HR-Analytics, 2020, S. 5 ff.
[74] *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner (Hrsg.), Arbeit 4.0 aktiv gestalten, 2018, S. 110 f.; *Biemann/Englmaier/Sliwka/Weller*, People Analytics – Personaldaten als Erfolgsfaktor, PERSONALquarterly 3/2017, S. 8 (9 ff.).
[75] *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner (Hrsg.), Arbeit 4.0 aktiv gestalten, 2018, S. 111.
[76] *Biemann/Englmaier/Sliwka/Weller*, People Analytics – Personaldaten als Erfolgsfaktor, PERSONALquarterly 3/2017, S. 8 (11).

Datenschutzsicht sind sie offensichtlich problematisch, weil sich auch hier der Datenhunger selbst vorantreibt.

Bei den Maßnahmen der Personalentwicklung stellen sich – ähnlich wie beim Recruiting – häufig Auswahlentscheidungen. Im Vergleich zur Einstellungsauswahl gibt es jedoch den großen Unterschied, dass es mit den Kandidat*innen einer innerbetrieblichen Auswahl intensive Erfahrungen aus u. U. jahrelanger Zusammenarbeit gibt. Klassischerweise stehen diese Erfahrungen mehr oder weniger zuverlässig im „Bauchgefühl" der Personalverantwortlichen zur Verfügung.[77] Bei einer digital unterstützen Entscheidungsfindung bleibt jedoch kaum eine andere Wahl, als dass Potenzial, Qualifikation, Arbeitshaltung und andere Charaktermerkmale der Kandidat*innen in Gestalt personenbezogener Daten elektronisch verfügbar gemacht werden müssen. Fair und unvoreingenommen mag die technische Unterstützung vielleicht[78] ab einem bestimmten Reifegrad sein, datenschutzfreundlich ist sie sicher nicht.

Zur Personalentwicklung gehört auch jegliche Variante des Feedbacks, das Beschäftigte erhalten, um Stärken oder Schwächen ihres Arbeitsverhaltens deutlich zu machen. Sie können ihr Arbeitsverhalten daran orientieren.[79] Zugleich können zielgerichtet Personalentwicklungsmaßnahmen wie Fortbildungen daran ansetzen. Neben dem Lerneffekt wird dem Feedback auch ein wichtiger Motivationseffekt zugeschrieben, wenn etwa nach Zielvereinbarungen die Zielerreichung beurteilt wird.[80] Feedback, so wird geraten,[81] sollte möglichst schnell erfolgen, damit der Zusammenhang vom Empfänger durchschaut werden kann. Der Trend heißt „Instant Feedback".[82] Digitale Feedbacksysteme sind im Einsatz und können sehr zeitnah das Urteil von Vorgesetzten, Kolleg*innen oder Kund*innen u. U. mit vorformulierten Bewertungen wiedergeben.[83] Erfolgt das Feedback bzw. Rating aus allen Richtungen wird es als 360-Grad-Feedback bezeichnet.[84] Der Einsatz eines solchen Systems bei Zalando mit Namen Zonar, das Peer-to-Peer-Ratings vorsieht, hat zu erheblicher öffentlicher Empörung geführt. Nach Einschätzung einer Studie der Hans-Böckler-Stiftung sei das System mit hohem Aufwand verbunden und erzeuge zahlreiche nicht intendierte Effekte wie eine Verschlechterung des Betriebsklimas, Stress und psychologische Belastungen auf Seiten der Beschäftigten.[85]

Es wäre allerdings verfehlt, eine solche Anwendung, die schlicht auf Erhöhung des Leistungsdrucks setzt, mit den wissenschaftlichen Ansprüchen von „People Analytics" zu verwechseln. Dennoch ist klar, dass sich „People Analytics" nicht auf abstrakte Wissenschaftlichkeit zurückziehen kann, für die die Daten konkreter Personen leicht verzichtbar wäre. Auch wissenschaftlich ist von Interesse, wie sich bestimmte Personen im Zeitverlauf entwickeln.[86] Geht es um hochwertiges Feedback, ist der Personenbezug jedenfalls unverzichtbar.

[77] *Reindl/Krügl*, People Analytics in der Praxis, 2017, S. 29 f.
[78] Diskriminierung durch automatisierte Personalauswahl ist ein noch unbewältigtes Thema, siehe z. B. *Hartmann*, EuZA 2019, 421.
[79] *Trost*, Neue Personalstrategien zwischen Stabilität und Agilität, 2018, S. 156.
[80] Ebenda, S. 151.
[81] *Armutat*, Leistungsmanagement: Das Ganze im Blick, in: Armutat et al. (Hrsg.), Personalmanagement in Zeiten von Demografie und Digitalisierung, 2018, S. 261 (274).
[82] Ebenda, S. 261 (275).
[83] *Gärtner*, Smart HRM – Digitale Tools für die Personalarbeit, 2020, S. 103 f.
[84] *Staab/Geschke*, Ratings als arbeitspolitisches Konfliktfeld – Das Beispiel Zalando, HBS Study 429, 2019, S. 14 f.
[85] Ebenda, S. 56.
[86] Womit effektiver Verschlüsselungstechnik nicht von vornherein der Rang abgesprochen werden soll, siehe *Huff/Götz*, NZA-Beilage, 2019, 73 (75).

1.2.3 PERSONALMOTIVATION UND ENTGELTGESTALTUNG

Personalentwicklung allein führt nicht zum Ziel, wenn Beschäftigte nicht bereit sind, ihr Potenzial im Sinne des Unternehmens abzurufen und kontinuierlich einzusetzen. Diesem Zweck dienen die HR-Instrumente, die auch unter dem Begriff „Performance-Management" zusammengefasst werden. Reine Überwachungstools werden dabei eher nicht genannt, obgleich überhaupt kein Zweifel daran bestehen kann, dass Motivation nicht nur durch freundliche Anreize, sondern auch durch Leistungsdruck erzielt sowie durch hartnäckige Überwachung hergestellt werden kann und wird.

a) Überwachungstechnik

GPS-Tracker, RFID-Chips (auch unter der Haut), Keylogger und Überwachungskameras sind nur einige Beispiele für Überwachungstechnik (siehe oben Kap. 1.1.2 a), die eingesetzt wird, um Motivation durch Beobachtungsdruck zu erzeugen.[87] Die Beobachtungsstrategie, die hinter dem Einsatz dieser Technik steht, kann durchaus unterschiedlich ausgeprägt sein. Beobachtung kann eingebunden sein in eine betriebliche Feedbackkultur oder Ansatzpunkte für sinnvolle individuelle oder teambezogene Coachings oder Fortbildungsangebote liefern. Wenn dies punktuell und ohne Sanktionen geschieht, wirft dies zwar datenschutzrechtliche Fragen auf. Der erzeugte Beobachtungsdruck hält sich aber in Grenzen. Eine andere Strategie setzt darauf, dass die Beobachtung als solche Druck erzeugt, ein vom Arbeitgeber erwünschtes Arbeitsverhalten an den Tag zu legen.

Ein Unternehmen, das sich entschieden hat, Überwachungsdruck zur Verhaltenssteuerung einzusetzen, wird gern zu Überwachungskameras greifen. Obgleich es sich bei Kameras um Technik des vergangenen Jahrhunderts handelt, bieten sie den Vorteil, besonders stark auf die Erfassten zu wirken. Denn das sichtbare *„Auge der Kamera"* wirkt unmittelbar auf die Beobachteten, wie Studien gut belegen.

Hintergrund ist die von *Duval/Wicklund*[88] begründete sozialpsychologische Theorie objektiver Selbstaufmerksamkeit („objective self-awareness"). Unterschiedliche Stimuli können Menschen in den Zustand gesteigerter Selbstaufmerksamkeit versetzen. Dazu zählt keineswegs nur Beobachtung durch andere. Auch ein Spiegel, ein Fragebogen mit persönlichen Fragen oder sogar der Gedanke an Gott[89] sind hierzu geeignet. Aber auch jede Form, in der man Objekt der Beobachtung anderer ist, eignet sich dafür hervorragend. Blicke können genügen, wie in zahlreichen Studien belegt.[90] Kameras dürften den Effekt verstärken. Der entscheidende Punkt ist, dass nach der Theorie objektiver Selbstaufmerksamkeit Menschen im Zustand gesteigerter Selbstaufmerksamkeit ihr Selbst hinsichtlich Verhalten, Charakterzüge oder Einstellungen mit Standards korrekten Verhaltens, korrekter Charakterzüge oder korrekter Einstellungen automatisch abgleichen.[91] Wird bei diesem Abgleich eine Diskrepanz festgestellt, so die Theorie, wird dies als unangenehm empfunden. Die Person reagiert mit dem Wunsch, das Selbst mit den Standards in Einklang zu bringen. Im Allgemeinen dürften daher Bemühungen einsetzen, das abweichende Verhalten usw.

[87] Siehe den Überblick bei *Krause*, Digitalisierung und Beschäftigtendatenschutz, BMAS Forschungsbericht 482, 2017, S. 8 ff.
[88] Grundlegend: *Duval/Wicklund*, A theory of objective self-awareness, 1972; zur weiteren Entwicklung: *Silvia/Duval*, Objective Self-Awareness Theory: Recent Progress and Enduring Problems, Personality and Social Psychology Review 5, 2001, S. 230.
[89] *Gervais/Norenzayan*, Like a camera in the sky? Thinking about God increases public self-awareness and socially desirable responding, Journal of Experimental Social Psychology 48, 2012, S. 298 (299).
[90] Im Überblick *Conty/George/Hietanen*, Watching Eyes effects: When others meet the self, Consciousness and Cognition 45, 2016, S. 184.
[91] *Silvia/Duval*, Objective Self-Awareness Theory: Recent Progress and Enduring Problems, Personality and Social Psychology Review, 5, 2001, S. 230 (231).

an die Standards anzupassen, da sich Verhalten in der Regel leichter ändern lässt als Verhaltensstandards. Diese Reaktion ist in vielen Experimenten nachgewiesen.[92] So konnte eine Kamera auf öffentlichen Toiletten die Zahl derer, die sich die Hände vor dem Verlassen wuschen, deutlich erhöhen.[93] Unter Beobachtungsdruck, so wird verallgemeinernd geschlossen, wird pro-soziales Verhalten[94] und die Bereitschaft, sich an Regeln zu halten,[95] aktiviert.

Auf das Beschäftigungsverhältnis bezogen bedeutet dies, dass bei Beschäftigten, die sich insbesondere durch Kameras beobachtet fühlen, regelmäßig der innere Wunsch aktiviert wird, sich an gesetzte Regeln und Vorgaben zu halten, auch wenn keine Sanktionen für Abweichungen drohen. Möglicherweise wird auch versucht, den Beobachtungsdruck durch angekündigte Sanktionen oder Anreize zu erhöhen. Allerdings wird auch immer die Gefahr angeführt, durch überzogenen Beobachtungsdruck Motivation zu untergraben. So oder so, bis hierher sind dies keine Phänomene der aktuellen Digitalisierungsphase. Neu ist, dass allgegenwärtige Sensorik, wozu auch optische Sensoren/Kameras gehören, zu den Merkmalen der 4.0-Prozesse gehört. So müssen sich Roboter, um z. B. eng mit Menschen umgehen zu können, auch mit optischen Sensoren orientieren. Ein autonomes Fahrzeug etwa wird eng mit Kameras bestückt. Sollen die System KI-ausgerüstet selbst lernen, so helfen moderne Tools der Bildanalyse, die z. B. dem Roboter erlauben, bestimmte Personen zu erkennen oder auch deren Gestik und Mimik zu interpretieren. “Self awareness“ dürfte auch in diesem Zusammenhang seitens des Beobachteten relevant sein. Die Daten, die hierbei anfallen können, sind nicht nur umfangreich, sondern auch – insbesondere, wenn Gestik und Mimik interpretiert werden – von hoher Eingriffstiefe in die Persönlichkeit der Erfassten.

b) Anreizsysteme und Entgeltgestaltung

Bei individuellen Anreizsystemen, zu denen zweifellos auch Entgeltsysteme gehören, die Entgeltbestandteile nach Leistungsgesichtspunkten berechnen, sind personenbezogene Daten unter zwei Gesichtspunkten erforderlich. Erstens geht es um die schlichte Durchführung des jeweiligen Systems. Es muss zutreffend dokumentiert werden, ob die jeweilige Person tatsächlich die Kriterien für einen bestimmten Vorteil z. B. eine Zulage, Prämie oder höhere Gehaltsgruppe erfüllt hat. Das ist im Prinzip nicht neu. Neu ist auch schon seit langem nicht mehr, dass diese Dokumentation elektronisch stattfindet und damit der Missbrauch der Daten zu anderen Zwecken als der reinen Abrechnung erleichtert wird. Neu wäre aber, dass die steigende Menge und Aussagekraft an Daten, die im Arbeitsprozess anfallen, für wesentlich komplexere Systeme der Leistungsbewertung herangezogen werden können. Die Forderung nach Entgeltgerechtigkeit dürfte durchaus dafür sprechen, dass qualitative Aspekte der Leistungserbringung stärker berücksichtigt werden. Für den Beschäftigtendatenschutz hätte das zweifellos den Nachteil, dass mehr und aussagekräftigere Daten personalisiert erhoben und wenigstens für eine gewisse Zeit gespeichert werden müssten.

Sofortige Anonymisierung der Daten ist auf dem Feld rechtssicherer Entgeltabrechnung keine Option. Solange Konflikte um die individuelle Richtigkeit im Raum stehen können, muss perso-

[92] Ebenda, S. 233.
[93] *Munger/Harris*, Effects of an observer on handwashing in a public restroom, Perceptual and Motor Skills 69, 1989, 733 (734).
[94] *Conty/George/Hietanen*, Watching Eyes effects: When others meet the self, Consciousness and Cognition 45, 2016, S. 184 (186).
[95] *Ariel/Sutherland/Henstock/Young/Drover/Sykes/Megicks/Henderson*: Paradoxical effects of self-awareness of being observed: testing the effect of police body-worn cameras on assaults and aggression against officers, Journal of Experimental Criminology 14, 2018, S. 19 (22).

nenbezogen bzw. allenfalls pseudonymisiert nachvollziehbar sein, auf welcher Datengrundlage eine bestimmte Person die jeweilige Leistung erhalten hat. Das kann sich bei einer üblichen Ausschlussfrist auf drei Monate beschränken. Bei der sehr beliebten Leistungsvergütung nach individueller Leistungsbeurteilung[96] kann auch über längere Zeiträume die personenbezogene Speicherung aussagekräftiger personenbezogener Daten unvermeidlich sein.

Zweitens geht es darum, die Anreizwirkung der Entgeltsysteme zu prüfen und zu verbessern. Unter „People Analytics"-Gesichtspunkten wird gefragt werden, ob ein Anreizsystem tatsächlich eine spürbare Anreizwirkung hat und wie diese optimiert werden kann. Das wird umso relevanter, als die fortschreitende Digitalisierung neue Anforderungen begründen wird, die gezielte Anreize erfordern können. Will man das betrieblich erforschen, wären weit größere und gehaltvollere Mengen an personenbezogenen Daten erforderlich, als für die rein routinemäßige Abwicklung von Leistungsentgelten nötig sind.

1.2.4 BEENDIGUNG DER BESCHÄFTIGUNG

Auch wenn es sehr umstritten ist, wie viele Menschen im Zuge der fortschreitenden Digitalisierung ihren Arbeitsplatz verlieren werden, so ist doch klar, dass es auch die Aufgabe des Personalmanagements sein wird, in größerem Stil Beschäftigungsverhältnisse zu beenden. Ein zentraler Aspekt wird dabei immer wieder die Frage der für das Unternehmen günstigsten Kündigungs- bzw. Beendigungsauswahl sein. Die nach dem Kündigungsschutzgesetz vorgeschriebene „soziale Auswahl" führt oftmals nicht dazu, dass gerade die Talente und Leistungsträger gehalten werden. Daher geht es für das Personalmanagement oft darum, die gesetzlichen Vorgaben zu umgehen – z. B. durch Aufhebungsverträge. Geklärt werden muss dann, wem diese angeboten werden. Die Gefahr besteht, dass gerade gut qualifizierte Beschäftigte Aufhebungsverträge annehmen, weil sie auf schnelle Anschlussbeschäftigung hoffen können.[97]

Erneut sind also auch hier, Auswahlentscheidungen auf Grundlage des zu analysierenden Personaldatenpools zu treffen. Zugleich ist eine Wahl des rechtlichen Mittels zu treffen, wobei im Zuge der Digitalisierung LegalTech-Anwendungen bei der Optimierung der Transaktionskostenbilanz helfen können. Auch hierzu werden zahlreiche personenbezogene Daten aus der Beschäftigungskarriere der Betroffenen benötigt.

1.3 DIE DIGITALISIERUNG DES ARBEITSSCHUTZES

Die Corona-Pandemie 2020/21 hat ein Schlaglicht auf das bis dahin selten thematisierte Konfliktfeld geworfen, das zwischen Arbeitsschutz- und Datenschutzzielen besteht.[98] Die Erfassung der Körpertemperatur oder der Ergebnisse eines Tests bzw. Schnelltests auf eine SARS-CoV-2-Virusinfektion bis hin zum Vorliegen eines Impfnachweises wirft die Frage auf, ob und wie lange solche sensiblen Gesundheitsdaten vom Arbeitgeber gespeichert werden dürfen. Auch z. B. die Videoüberwachung zur Kontrolle von Personenabständen beschäftigte sogar die Gerichtsbarkeit.[99] Erkrankt ein Beschäftigter an Covid-19 muss er Angaben zur Art seiner Erkrankung machen, damit

[96] Zur hohen Verbreitung *Arnhold/Butschek/Grunau/Kampkötter/Petters/Sliwka*, Bericht zum Forschungsmonitor „Variable Vergütungssysteme", BMAS Forschungsbericht 507, 2018, S. 19 ff.
[97] *Holtbrügge*, Personalmanagement, 7. Aufl., 2018, S. 166.
[98] *Naber/Schulte*, NZA 2021, 81; *Wünschelbaum*, NZA 2020, 612.
[99] ArbG Wesel, Beschl. v. 24.4.2020 – 2 BVGa 4/20, ZD 2020, 368.

seine betrieblichen Kontakte geklärt werden.[100] Eine Fülle personenbezogener Daten gilt es dabei im Interesse des Arbeits- bzw. Gesundheitsschutzes zu verarbeiten.

Die seit Inkrafttreten des Arbeitsschutzgesetzes 1996 fortlaufend auf Basis europäischer Richtlinien modernisierten Regelungen zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit haben eine wachsende Zahl rechtlicher Pflichtaufgaben des Managements definiert, die nur mit einer umfangreichen betrieblichen Arbeitsschutzverwaltung bewältigt werden können. Schon lange vor Industrie 4.0, IoT und KI wurden hierzu in großem Umfang Daten elektronisch verarbeitet, die zu einem hohen Anteil Personenbezug aufweisen.

Ein Beispiel liefern *arbeitsmedizinische Vorsorgeuntersuchungen*, die in der ArbMedVV geregelt sind. Durchgeführt werden diese nach § 3 Abs. 2 ArbMedVV von einem Arzt oder einer Ärztin, die selbstverständlich der ärztlichen Schweigepflicht unterliegen. Aber zu organisieren hat sie nach § 3 Abs. 1 ArbMedVV der Arbeitgeber, der daher nach Abs. 4 auch eine Vorsorgekartei zu führen hat, die ausdrücklich automatisiert geführt werden kann. Personenbezogen wird gespeichert, dass, wann und aus welchem Anlass die Vorsorge stattgefunden hat. Das Untersuchungsergebnis erfährt der Arbeitgeber regelmäßig nicht, es sei denn, es erfordert weitere Maßnahmen des Arbeitsschutzes. Aber auch ohne Ergebnis werden sensible Daten archiviert, die bis zum Ausscheiden der Beschäftigten aufzubewahren sind.

Ein weiteres Beispiel liefern *Arbeitsunfälle*, die erstens gemäß § 6 Abs. 2 ArbSchG betrieblich zu dokumentieren sind. Dabei geht es um sensible auf die Gesundheit bezogene Daten mindestens einer Person. Zweitens hat der Arbeitgeber gemäß § 193 Abs. 1 SGB VII Arbeitsunfälle dem Unfallversicherungsträger anzuzeigen. Dabei ist aus der Anlage 1 der Unfallversicherungs-Anzeigeverordnung ein Formular zu verwenden, in der selbstverständlich u. a. der Name der betroffenen Person, eine Schilderung des Unfallhergangs, verletzte Körperteile und auch die Namen von Zeugen anzugeben sind. Drittens sind Arbeitsunfälle Anlass für eine Aktualisierung der Gefährdungsbeurteilung nach § 5 ArbSchG, die ihrerseits zu dokumentieren ist und oft auch in Schulungen zur Arbeitssicherheit nach § 12 ArbSchG mündet.

Das alles ist absolut sinnvoll und erforderlich. Denn für den Arbeitsschutz ist es gerade funktional, dass Gefährdungen, die sich in Unfällen oder Berufskrankheiten zeigen, nicht geheim gehalten, sondern möglichst kommuniziert werden, um sie künftig zu vermeiden. Es gilt gerade, in künftigen Unterweisungen die Unfallgefahren anhand konkreter Vorfälle zur Sprache zu bringen, um eindrucksvoll davor zu warnen. Ein reichhaltiger Informationsfluss ist ein Qualitätskriterium einer guten Arbeitsschutzorganisation. Dass dabei auch sensible Gesundheitsdaten eine Rolle spielen, liegt in der Natur der Sache. Arbeitsschutz und Datenschutz liegen offensichtlich und schon seit langem sehr deutlich im Konflikt.[101] Allerdings wird den hochrangigen Belangen des Arbeitsschutzes regelmäßig Vorrang eingeräumt. Denn laut BVerfG[102] zählt der Schutz der Bevölkerung vor Gesundheitsgefahren zu den überragend wichtigen Gemeinschaftsgütern – im Unterschied zum Schutz der informationellen Selbstbestimmung.[103]

Dabei ist der Einsatz von klassischer elektronischer Kommunikations- und Dokumentationstechnik wie E-Mail, elektronische Personalakte[104] oder elektronische Unfallmeldung (seit 2002) inzwi-

[100] *Lutz/Born*, DB 2020, 1162; *Sagan/Brockfeld*, NJW 2020, 1112.
[101] Dazu grundlegend *Rose*, in: Festschrift für Taeger, 2020, S. 393 ff.
[102] BVerfG v. 30.7.2008 – 1 BvR 3262/07 u. a., NJW 2008, 2409 (2412).
[103] *Rose*, in: Festschrift für Taeger, 2020, S. 399 f.
[104] *Kort*, ZD 2015, 3.

schen auch im Arbeitsschutz selbstverständlich. Bei der aktuellen Entwicklung der Digitalisierung geht es im Arbeitsschutz jedoch nicht um eine solche Umstellung auf elektronische Medien. Es geht um etwas völlig anderes. Die Methoden und Maßnahmen der praktischen Durchführung des Arbeitsschutzes am Arbeitsplatz werden selbst digitalisiert. Dabei können zwei Phänomene unterschieden werden. Digitale Technik wird eingesetzt

- zur Ermittlung und Beurteilung physischer und psychischer Gefährdungen (1.3.1) und
- zur Vermeidung oder Reduzierung solcher Gefährdungen (1.3.2).

1.3.1 ERMITTLUNG UND BEURTEILUNG

Bei der Ermittlung und Beurteilung von Gefährdungen sind zwei Tendenzen für den Datenschutz besonders relevant. Einerseits ist es für die Optimierung des Arbeitsschutzes möglich und sinnvoll geworden, die Überwachung der Sicherheit von Arbeitsräumen und Arbeitsprozessen durch ständig verbesserte *Sensortechnik in hoher Einsatzdichte* deutlich zu intensivieren. Andererseits sind *psychische Belastungen* machtvoll in den Blickpunkt des Arbeitsschutzes getreten, deren Ermittlung und Beurteilung im Vergleich zu den klassischen physischen Belastungen nach völlig anderen, in der Regel wesentlich persönlichkeitsnäheren Daten verlangt.

a) Sensorik

Die drei Tendenzen, dass digitale Sensorik immer leistungsfähiger, immer kleiner und vor allem immer kostengünstiger wird,[105] erlaubt es, jeglichem Funktionsgegenstand die Fähigkeit zu verleihen, relevante Messergebnisse aus der Umwelt zu gewinnen. Messdaten jeglicher Art von Geräuschen, Bewegungen und Erschütterungen bis hin zu radioaktiver Strahlung sollen von den digital vernetzten „Dingen" in großer Zahl erhoben, geteilt und analysiert werden. Viele Rückschlüsse auf Gesundheitszustände und Gesundheitsgefahren sind möglich. Dabei helfen Fortschritte auf dem Gebiet der Interpretation von Sensordaten, dass deren Aussagekraft fortlaufend gesteigert wird. Als Beispiel sei die Untersuchung des Lidschlagverhaltens des menschlichen Auges als Indikator für Stress genannt.[106]

Im nächsten Schritt soll KI der Sensorik kognitive Fähigkeiten[107] verleihen, mit denen letztendlich in Echtzeit Messergebnisse aus den Prozessen zur autonomen Anpassung an eine dynamische Umwelt führen sollen. Eine zentrale Aufgabe der Sensorik ist regelmäßig die Überwachung der eingesetzten Technik. KI-Systeme sollen lernen, Ausfälle der Technik vorherzusagen und damit den reibungslosen Betrieb zu unterstützen.[108] Technische Ausfälle, insbesondere wenn es um Sicherheitstechnik geht, sind oft mit Gefährdungen verbunden. Entsprechende intelligente Sensorik dient also auch dem Erkennen (und Abwenden) von Sicherheitsrisiken.

Zur dynamischen Umwelt gehören selbstverständlich auch menschliche Akteure, deren Verhalten oder Fehlverhalten als mögliche Gefährdung zu antizipieren sind. Bei der Mensch-Roboter-Kollaboration führt die Maschine eine permanente „Beobachtung" der relevanten Gefährdungen durch, um die körperliche Unversehrtheit des Menschen durch sensorgestützte Schutzsysteme

[105] *Cernavin/Lemme*, in: Cernavin/Schröter/Stowasser (Hrsg.), Prävention 4.0, 2018, S. 24 ff.
[106] *Reßut/Hoppe*, Erfassung von individuellem Beanspruchungserleben bei kognitiven Belastungssituationen mittels Mustererkennung im Lidschlagverhalten, ZArbWiss 2020, 249 ff.
[107] Vgl. *Bauckhage/Bauernhansl/Beyerer/Garcke*, in: Neugebauer (Hrsg.), Digitalisierung, 2018, S. 239 ff.
[108] *Apt/Priesack*, KI und Arbeit – Chance und Risiko zugleich, in: Wittpahl (Hg.), Künstliche Intelligenz, 2019, 221 (229).

und eine intelligente Steuerungselektronik zu gewährleisten.[109] Personenbezogenes Lernen der Maschine, das z. B. individuelle Bewegungsabläufe in Rechnung stellt, ist hierbei hilfreich.[110]

Im Interesse des Arbeitsschutzes ist es also eine vielversprechende Chance, die umfangreiche Sensorik, die ohnehin allgegenwärtig eingesetzt wird oder auf dem Markt günstig verfügbar ist, auch zur Ermittlung und Beurteilung von Gefährdungen einzusetzen. So können Messungen im Hinblick auf Gefährdungen etwa durch Lärm oder durch Stäube kontinuierlich und – wo sinnvoll – flächendeckend durchgeführt werden.[111] Je näher die Messtechnik dem Menschen kommt, fallen auch verstärkt personenbezogene Daten an. Das gilt vor allem für am Körper getragene Sensoren. Intelligente Schutzkleidung für Feuerwehrleute, die Vitalfunktionen misst, war bereits 2012 Gegenstand einer datenschutzrechtlichen Beurteilung.[112] Als aktuelles Beispiel soll hier das BAuA-Projekt F 2494 „Personalisiertes KI-basiertes Körpersensornetzwerk zur physischen Echtzeit-Beanspruchungsermittlung älterer Beschäftigter (BIONIC)“ dienen, das 2021 abgeschlossen werden soll. Um Muskel-Skelett-Erkrankungen besser vorzubeugen zu können, soll ein personenbezogenes sensorisches System entwickelt werden, das die Körperhaltung von Beschäftigten durch einen intelligenten Chipsatz in der Arbeitskleidung erfasst und analysiert.[113]

b) Psyche

Die psychische Gesundheit ist ein recht neuer Gegenstand des Arbeitsschutzes, der in der Praxis erhebliche Irritationen auslöst. In der Gefährdungsbeurteilung sind nach § 5 Abs. 3 Ziff. 6 ArbSchG psychische Belastungen seit 2013 explizit zu berücksichtigen. Implizit war dies auch schon vorher der Fall, fand jedoch sehr selten statt, sodass der Gesetzgeber quer durch das Arbeitsschutzrecht klarstellend tätig geworden ist (siehe auch § 4 Ziff. 1 ArbSchG, § 3 Abs. 1 Satz 3 ArbStättV). Auch jetzt verläuft die Umsetzung noch schleppend,[114] obwohl die Zahl der mit psychischen Erkrankungen begründeten Fehlzeiten weiter wächst.[115] Gründe für die mangelnde Umsetzung werden u. a. in den komplexen Beurteilungs- und Gestaltungsproblemen gesehen, weil die Ursache-Wirkungs-Beziehungen bei Gefährdungen für die Psyche nur schwer zu präzisieren sind, so dass die tradierten Verfahrensweisen des technischen Arbeitsschutzes nicht greifen.[116] Keine Frage, mit Mess- und Grenzwerten sind die Probleme psychischer Fehlbeanspruchung nicht zu beherrschen.

Die Gemeinsamen Deutschen Arbeitsschutzstrategie (GDA) empfiehlt stattdessen, zum Zweck der Gefährdungsbeurteilung nach § 5 ArbSchG standardisierte schriftliche Mitarbeiterbefragungen, Beobachtungen mit Interviews oder moderierte Analyseworkshops zur Ermittlung der psychischen Belastung der Arbeit durchzuführen.[117] Auch die Ergebnisse solcher Verfahren müssen gemäß § 6 ArbSchG zusammen mit ihrer Beurteilung und den ergriffenen Schutzmaßnahmen in

[109] *Corves et al*, Robotik 4.0, in: Frenz (Hg.), Handbuch Industrie 4.0: Recht, Technik, Gesellschaft, 2020, S. 569 (580).
[110] *Steil/Maier*, Kollaborative Roboter: universale Werkzeuge in der digitalisierten und vernetzten Arbeitswelt, in: Maier/Engels/Steffen (Hrsg.), Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, 2020, S. 323 (337 f.).
[111] Kostengünstige Staubsensoren bestehen Eignungstest laut *BAuA* Projekt F 2405, www.baua.de/DE/Aufgaben/Forschung/Forschungsprojekte/f2405.html.
[112] *Roßnagel/Jandt/Skistims/Zirfas*, Datenschutz bei Wearable Computing, 2012.
[113] *BAuA* Projekt F 2494, www.baua.de/DE/Aufgaben/Forschung/Forschungsprojekte/f2494.html.
[114] *Beck*, Arbeit, 2019, 125, 128.
[115] Siehe z. B. *DAK*, Psychoreport 2019, S. 2 und 3, www.dak.de/dak/download/190725-dak-psychoreport-pdf-2125500.pdf.
[116] *Beck*, Arbeit, 2019, 125, 127 f. und 133 ff.
[117] *GDA*-Arbeitsprogramm Psyche, Empfehlungen zur Umsetzung der Gefährdungsbeurteilung psychischer Belastung, 3. Aufl., 2017.

eine gesetzlich verpflichtende Dokumentation einfließen. Es fällt auf, dass von Datenschutz dabei keine Rede ist.

Aus Sicht des Datenschutzes ist zuzugeben, dass die in Anlage 1 der GDA-Empfehlungen[118] enthaltene Liste der psychischen Belastungsfaktoren der Arbeit, die der Ermittlung der Belastungen in den Betrieben als Leitfaden zugrunde gelegt werden soll, sehr deutlich formuliert, dass es bei der Gefährdungsbeurteilung nicht darum gehen soll, *individuelle* psychische Befindlichkeiten abzufragen. Vielmehr sollen *objektive Belastungsfaktoren* der Arbeit ermittelt werden. Es soll also eindeutig nicht darum gehen, überforderte Beschäftigte zu identifizieren, die dann um ihren Arbeitsplatz fürchten müssen. Es wird daher auch dringend geraten, genau dies vor und während des Prozesses wiederkehrend zu betonen.[119] Doch die Art der genannten Erhebungsinstrumente (Fragebogen, Interview, Workshop) ist systematisch weit offen für persönliche Stellungnahmen – spätestens beim Punkt 3 der abzufragenden Belastungsfaktoren: „Soziale Beziehungen". Es genügt bei psychischen Belastungen (anders als bei schlechtem Licht, belasteter Raumluft, hohem Lärm usw.) gerade nicht, objektive Faktoren zu ermitteln. Denn ob, welche und vor allem wie dringlich Maßnahmen ergriffen werden müssen, hängt hier regelmäßig entscheidend davon ab, wie individuelle Beschäftigte auf die Belastungen reagieren. Brisante personenbezogene Daten sind dabei unvermeidlich und zudem auch systematisch zu dokumentieren.

Im Interesse des Datenschutzes ist es daher anerkennenswert, wenn die Deutsche Gesetzliche Unfallversicherung (DGUV) in ihrer Handreichung zur Gefährdungsbeurteilung psychischer Belastungen nicht nur darauf dringt, möglichst objektiv Belastungen und eben nicht individuelle Dispositionen zu erheben, sondern auch Anonymität, soweit es geht, sicherzustellen.[120] Doch wird dies in der Praxis nur begrenzt gelingen können,[121] zumal sich die Akteure in einem ständigen Zielkonflikt zwischen Datenschutz und der Überzeugungskraft des von ihnen ermittelten Faktenmaterials befinden.

Voraussichtlich werden psychische Gesundheitsgefahren weiter zunehmen. Denn die Digitalisierung bietet nicht nur zunehmend wichtige Instrumente bei der Bewältigung von Gefährdungen am Arbeitsplatz, sie bringt auch selbst spezifische Gefährdungen mit sich. Fast immer geht es dabei um psychische Fehlbeanspruchungen, die befürchtet werden. So wird angenommen, dass nicht wenige Menschen eine enge Kooperation mit cyberphysischen Systemen (CPS) als negativen Stress erleben könnten, weil Phänomene wie Intransparenz, Komplexität, Fremdsteuerung oder Überwachung in den Vordergrund treten.[122] Zudem wird die Informationsüberflutung am Arbeitsplatz vielfach als Folge der Digitalisierung und ernstes gesundheitliches Problem diskutiert (mögliche Folge: Burnout).[123] Selbst das Tragen von Datenbrillen soll u. U. Stressfaktor sein.[124]

Es passt in die Logik der fortschreitenden Digitalisierung, dass die psychische Fehlbeanspruchung selbst zum Objekt allgegenwärtiger Sensorik gemacht werden soll. Kollege Cobot fragt nicht nur freundlich nach dem Befinden, sondern nimmt auch gleich die erforderlichen Messungen vor.

[118] Ebenda, S. 17 ff.
[119] *Gilbert/Kirmse/Pietrzyk/Steputat-Rätze*, Gestaltungshinweise für die praktische Umsetzung der Gefährdungsbeurteilung psychischer Belastung, ZArbWiss 2020, 89 (95).
[120] *DGUV* (Hrsg.), Gefährdungsbeurteilung psychischer Belastungen, IAG Report 1/2013, S. 21 ff.
[121] Die Erhebungsinstrumente Workshop bzw. Begehung erlauben keine vollständige Anonymität, so zutreffend *Gilbert/Kirmse/Pietrzyk/Steputat-Rätze*, Gestaltungshinweise für die praktische Umsetzung der Gefährdungsbeurteilung psychischer Belastung, ZArbWiss 2020, 89 (95).
[122] *Frost/Sandrock*, Neue Belastungsarten in der Arbeitswelt 4.0, ifaa – Factsheet, 2019, www.arbeitswissenschaft.net/fileadmin/Downloads/Factsheet_Belastungsarten.pdf; *Baumann/Cernavin/Frost/Georg/Große/Hasselmann/Icks/Schröter/Zittlau*, in: Cernavin/Schröter/Stowasser, 2018, S. 13.
[123] *Junghanns/Kersten*, Informationsüberflutung am Arbeitsplatz – Gesundheitliche Konsequenzen, ZblArbeitsmed 2020, 8.
[124] *Holz/Herold/Friemert/Hartmann/Harth/Terschüren*, Datenbrillen am Arbeitsplatz – Informationsdichte am Auge, ZblArbeitsmed, 2021, 24.

Tatsächlich soll es in der „kognitiven Neuroergonomie“ Experimente geben, durch Hirnstrommessungen mittels kleiner mobiler EEG-Geräte mentale Zustände der Beschäftigten zu erfassen und hinsichtlich psychischer Belastungen auszuwerten.[125] Wie schon erwähnt, könnte aber auch die Beobachtung des Lidschlages dafür ausreichen.[126]

1.3.2 BEHERRSCHUNG VON GEFÄHRDUNGEN DURCH ASSISTENZSYSTEME

Das gegenwärtig dynamischste Feld der Digitalisierung des Arbeitsschutzes stellt die rasche Entwicklung und Weiterentwicklung von vielfältigen technischen Geräten dar, die u. a. die menschliche Wahrnehmung, Aufmerksamkeit, Reaktions- und Entscheidungsfähigkeit unterstützen.[127] Gefährdungen wird oft schon dadurch begegnet, dass bei der Arbeit weniger Fehler passieren. Das Feld reicht von Smart-Devices, die durch Informationen während der Arbeit auf Gefahren hinweisen oder durch Instruktionen sicheres Arbeiten anleiten, über Arbeitsplätze, die sich automatisch auf die Bedürfnisse des jeweiligen Beschäftigten einrichten (Licht, Temperatur, Arbeitsposition), bis hin zur physischen Unterstützung, die Arbeiten in Zwangshaltung oder schweres Heben dem Roboter überträgt.[128]

Zwangsläufig funktionieren digitale Assistenzsysteme in zwei Richtungen, indem sie einerseits Personen und Prozesse unterstützen und andererseits Daten über diese Personen und Prozesse erheben.[129] Es liegt in der Logik der 4.0-Arbeitsprozesse, die erhobenen Daten auch zu teilen, damit durch deren Analyse Ressourcen und Prozesse weiter optimiert werden können. Dabei ist es auch sinnvoll, personalisierte Hilfestellung zu geben. Denn es geht darum, dass möglichst jederzeit die dafür befähigte Person mit der zutreffenden unterstützenden Technik am geforderten Einsatzort zeitgerecht zur Verfügung steht.[130]

Besonders datenschutzkritisch sind Systeme, die entweder besonders viele oder besonders aussagekräftige Verhaltens- bzw. Vitaldaten von Beschäftigten erfassen, insbesondere wenn sie das nicht nur zeitlich punktuell, sondern dauerhaft tun. Geräte, die Beschäftigte als „Wearables“ oder „Smart Clothes“ bei sich tragen, gilt es daher besonderer kritisch zu beobachten.[131] Einige Beispiele müssen hier genügen:

- *Smart Glasses* konnten sich als Alltagsgegenstand im öffentlichen Raum nicht durchsetzen, in der Arbeitswelt sieht das anders aus.[132] Vor allem für die Logistik, z. B. zur Orientierung in großen Warenlager und für Zwecke der Einarbeitung werden Datenbrillen empfohlen.[133] Die Assistenz im Interesse des Arbeitsschutzes spielt dabei eine untergeordnete Rolle. Unter Arbeitsschutzgesichtspunkten interessant ist allerdings ein Projekt,

[125] *Lindner*, Kognitive Neuroergonomie als Problem des Arbeitsrechts, NJOZ 2020, 321.
[126] *Reßut/Hoppe*, Erfassung von individuellem Beanspruchungserleben bei kognitiven Belastungssituationen mittels Mustererkennung im Lidschlagverhalten, ZArbWiss 2020, 249 ff.
[127] *Varadinek/Indenhuck/Surowiecki*, Rechtliche Anforderungen an den Datenschutz bei adaptiven Arbeitsassistenzsystemen, BAUA Projekt F 2412, 2018, S. 9.
[128] *Hasselmann*, in: Matusiewicz/Kaiser (Fn. 5), S. 57, 59; weiter ausdifferenziert bei *Cernavin/Lemme*, S. 39 f.
[129] *Cernavin/Lemme*, in: Cernavin/Schröter/Stowasser (Hrsg.), Prävention 4.0, S. 39.
[130] *Varadinek/Indenhuck/Surowiecki*, Rechtliche Anforderungen an den Datenschutz bei adaptiven Arbeitsassistenzsystemen, BAUA Projekt F 2412, 2018, S. 10.
[131] *Weichert*, NZA 2017, 565.
[132] *BAuA* (Hrsg.), Head-Mounted Displays – Arbeitshilfen der Zukunft. Bedingungen für den sicheren und ergonomischen Einsatz monokularer Systeme, 2016.
[133] *Werning et al.*, Smart Glasses als Assistenzsystem in der betrieblichen Einarbeitung, HMD Praxis der Wirtschaftsinformatik 2019, 612 ff.

Hörgeschädigte durch Visualisierung akustischer Informationen in der Datenbrille in die Lagerarbeit zu integrieren.[134] Der Vorteil der Datenbrillen im Vergleich zu Tablets liegt z. Zt. vor allem in der Möglichkeit, beide Hände bei der Arbeit frei zu haben, was der Eigensicherung z. B. auf Gerüsten förderlich sein kann. Zunehmend aber wird die Brille Bilddaten in ihrem Sichtfeld analysieren und den Nutzer vor Gefährdungen warnen können.

- Unter dem Begriff *Smart Clothes* wird mit Sensorik ausgestattete Schutzkleidung verstanden, die z. B. zugleich Gefahrstoffe in der Atemluft detektieren und Vitalfunktionen überwachen kann. Auch psychische Befindlichkeiten der tragenden Person sollen messbar sein, sodass Zustände der Überforderung signalisiert werden können.[135]
- Deutlich ist der Arbeitsschutzzweck auch bei digitalen *Exoskeletten*, die das im Arbeitsschutz hochbrisante Problem des Heben und Tragens schwerer Lasten betreffen. „German Bionic" bietet das Modell Cray X nunmehr – vorgestellt auf der Hannover Messe 2019 – mit IoT-Technik an. Aufgesetzt wie ein großer Wanderrucksack unterstützt das Exoskelett beim Heben von schweren Lasten. Der Rücken wird dabei um bis zu 20 kg entlastet.[136] Verletzungsrisiken und Ausfallzeit würden signifikant reduziert, behauptet der Hersteller.[137]
- Verbreiteten Einsatz finden bereits *Bodycams* durch die Polizei[138] und private Sicherheitsdienste. Der Schutz der Einsatzkräfte bei der Arbeit vor tätlichen und verbalen Übergriffen ist dabei das erklärte Ziel. Daten werden bei dieser Technik nicht nur über das Verhalten der Anwender selbst erfasst, sondern vor allem von Personen, von denen Übergriffe ausgehen könnten, sowie von zufällig anwesenden Passanten.
- *Cobots* (kollaborative Roboter) tragen Nutzer zwar nicht in der Hosentasche. Doch eine persönliche Zuordnung findet durchaus statt. Cobots sollen Menschen bei gefährlichen, physisch anspruchsvollen oder monotonen Arbeiten entlasten und so Gefährdungen reduzieren.[139] Auch mithilfe moderner Sensorik und Feinsteuerung gilt es noch als weiter Weg, bis Mensch und Roboter tatsächlich anspruchsvollere Aufgaben „Hand-in-Hand" lösen können.[140] Doch wie nah der Kontakt auch ist. Bild- und Tondaten, die der Cobot vom Menschen aufzeichnet und analysiert, können diesem auch auf Distanz zahlreiche Daten zur Physis und Psyche der Person liefern.

1.3.3 RISIKEN UND CHANCEN

Die wissenschaftliche Diskussion über Arbeits- bzw. Gesundheitsschutz und menschengerechte Gestaltung der Arbeit in Zeiten umfassender Digitalisierung durchzieht wie ein roter Faden der analytische Befund einer Ambivalenz aus Risiken und Chancen. In einem Diskussionsbeitrag an der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin heißt es,[141] dass zum Teil vermutet werde, dass digitale Technik in einem digitalen Taylorismus münde, der die Autonomie in der Arbeitswelt systematisch verringere, während andere annähmen, dass digitale Technik Autono-

[134] *Abend*, IAB-Forum 17. Januar 2019, www.iab-forum.de/mehr-durchblick-dank-datenbrille-wie-virtuelle-realitaet-die-berufliche-teilhabe-verbessern-kann/.
[135] Smart Clothing for Human Performance Evaluation untersuchen *Scataglini/Truyen/Perego/Gallant/Van Tiggelen/Andreoni*, in: BAuA (Hrsg.), Proceedings of the 5th International Digital Human Modeling Symposium, 2017, S. 9 ff.
[136] *Pluta*, golem.de 3. April 2019, www.golem.de/news/german-bionic-aktives-exoskelett-cray-x-hilft-beim-heben-1904-140431.html.
[137] www.presseportal.de/pm/126129/4623363, 15.6.2020.
[138] *Kersting/Naplava/Reutemann/Heil/Scheer-Vesper*, Die deeskalierende Wirkung von Bodycams im Wachdienst der Polizei Nordrhein-Westfalen: Abschlussbericht, 2019, S. 22; *Rose*, in: Festschrift für Taeger, 2020, S. 406 ff.
[139] *Adolph/Kirchhoff/Geilen,* in: Maier/Engels/Steffen (Hrsg.), Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, 2020, S. 29.
[140] *Steil/Maier*, in: Maier/Engels/Steffen (Hrsg.), Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, 2020, S. 328.
[141] *Kirchner/Meyer/Tisch*, Digitaler Taylorismus für einige, digitale Selbstbestimmung für die anderen? Ungleichheit der Autonomie in unterschiedlichen Tätigkeitsdomänen, baua: Fokus, Juli 2020, S. 2.

mie systematisch erhöhe und eine digitale Selbstbestimmung am Arbeitsplatz ermögliche. Die Studie selbst kommt allerdings zu dem Ergebnis, dass im Zuge der Digitalisierung nicht ausschließlich das eine oder das andere stattfinde, sondern eine Polarisierung festzustellen sei, in der Arbeitsqualität gewonnen werde und verloren gehe. Gewinner seien vor allem wissensbezogene Tätigkeiten. Produzierende Tätigkeiten hätten auch noch oft geringere Vorteile. Verlierer seien vorwiegend unter den dienstleistenden Tätigkeiten zu finden.[142]

Arbeitsschutz 4.0 bietet in der Tat vielfertige Risiken und Chancen.[143] Zu den Chancen zählt vor allem die Ausgliederung monotoner, gefährlicher oder körperliche belastender Tätigkeit. Die leichtere Verfügbarkeit von sinnvollen Hilfestellungen (Information, Kommunikation) oder Warnungen bei Gefahren oder Fehlleistungen gehören ebenfalls dazu. Zu den Risiken gehören steigende Leistungserwartungen bei gleichzeitig leichterer Kontrolle des Leistungsverhaltens. Insbesondere hohe Anforderungen an die menschliche Informationsverarbeitung sind dabei ein zunehmendes Problem. Je nach Tätigkeitsprofil drohen zudem eine Reduzierung auf Resttätigkeiten, Fremdbestimmung oder Vereinzelung.

Diese *Ambivalenz der Digitalisierung*, die hier nicht weiter untersucht werden kann, stellt eine weitere nennenswerte Herausforderung für den Beschäftigtendatenschutz dar. Denn für Beschäftigte auf unterschiedlichen Arbeitsplätzen kann der Schutz personenbezogener Daten eine ganz unterschiedliche Relevanz haben. Mehr noch, selbst Beschäftigte auf gleichen Arbeitsplätzen können angesichts verknüpfter Chancen und Risiken zu ganz unterschiedlichen Einschätzungen kommen, inwieweit sie einer umfänglichen Verarbeitung ihrer personenbezogenen Daten bereitwillig oder ablehnend gegenüberstehen. Beschäftigtendatenschutz ist damit ein wenig dankbares Thema für kollektive Interessenvertretungen. Betriebs- und Personalräte drohen daher nicht nur wegen der Wucht ständig neuer Systeme personenbezogener Datenverarbeitung überfordert zu werden. Auch das Finden guter Kompromissregelungen, die Risiken begrenzen und Chancen nicht verbauen, ist ein sehr anspruchsvolles Problem.

1.4 ERGEBNIS

Die *Digitalisierung der Arbeitsprozesse* in der Produktion und Logistik führt wegen der zunehmend leistungsfähigen, miniaturisierten und zugleich kostengünstigen Sensorik dazu, dass tatsächlich dem 4.0-Paradigma entsprechend alle relevanten Informationen aller an der Wertschöpfung beteiligten Instanzen in Echtzeit vernetzt werden können. Es entstehen gewaltige betriebliche Big-Data-Pools, die von fortschreitend leistungsfähiger Software unter verschiedensten Gesichtspunkten analysiert werden können. Dabei fallen zwar in großen Mengen und mit hoher Aussagekraft personenbezogene Daten an, die jedoch regelmäßig nicht als solche gespeichert und ausgewertet werden müssen, um Prozesse zu optimieren. Allerdings ist das Zusammenspiel Mensch-Maschine ein zentraler Schwerpunkt der Entwicklung. Soll dieser optimiert werden, wird der Personenbezug der Daten vielfach wichtig. Um z. B. herauszufinden, warum ein Teil der Beschäftigten mit einer neuen Technik gut zurechtkommt, ein anderer Teil hingegen nicht, ist es schon hilfreich, diese Personenkreise unterscheiden zu können. Technik wird für ihren besseren Einsatz personalisiert oder muss lernen, Personen zu unterscheiden. Wird darüber hinaus die Sensorik

[142] Ebenda, S. 16 f.
[143] Siehe die Gegenüberstellung bei *Villwock/Serries/Voigtländer*, Arbeitsschutz 4.0, in: Fortmann/Kolocek (Hg.), Arbeitswelt der Zukunft, 2018, S. 299 (302).

gezielt zur Überwachung eingesetzt und sei es nur, um individuell Hilfestellung geben zu können, so ist der Personenbezug unverzichtbar.

Bei der *Digitalisierung des Personalmanagements* ist klar, dass es nicht nur um Big Data, sondern um Big Personal Data geht. Ausnahmsweise mögen People Analytics Studien auch mit anonymisierten Daten möglich sein. Aber allein um individuelle Entwicklungen im Zeitverlauf beurteilen zu können, muss klar sein, auf wen sich die Daten beziehen. Bei den zahlreichen Auswahlentscheidungen, die zu treffen sind (Einstellung, Förderung, Aufstieg, Kündigung), geht es sowieso nicht ohne klaren Personenbezug. Die Digitalisierung des Personalmanagements, das auf vorhandene betriebliche Big Data Pools zurückgreift, bei steigenden wissenschaftlichen Ansprüchen aber auch selbst Daten erheben wird, stellt die Belange des Beschäftigtendatenschutzes systematisch in Frage. Denn selbstverständlich interessiert man sich hier für den einzelnen Menschen. Hinzu kommt, dass gerade das Personalmanagement Ambitionen entwickeln könnte, tief in die Persönlichkeitsstruktur der Beschäftigten einzudringen, um z. B. perfekte Teams zusammenzustellen.

Auch bei der *Digitalisierung des Arbeitsschutz- bzw. Gesundheitsschutzmanagements* ist der Personenbezug häufig als solches von Bedeutung. Zusätzlich gibt es hier zwei besonders brisante Besonderheiten. Erstens geht es hier ständig um *besonders sensible* Gesundheitsdaten. Das gilt verstärkt, seitdem die psychische Gesundheit im Arbeitsschutz ernsthaft zu berücksichtigen ist. Der Konflikt ist hier zweitens noch dadurch geprägt, dass der Arbeitgeber ausdrücklich verpflichtet ist, Arbeitssicherheit nach modernsten Methoden zu gewährleisten. Digitalisierung ist hier – anders als im Personalmanagement – schlicht *gesetzliche Pflicht*. Der Arbeitgeber kann aus rechtlichen Gründen gar nicht anders, als die enorm wachsenden Datenpools daraufhin auszuwerten, um Sicherheits- und Gesundheitsgefahren gesetzestreu zu minimieren. Denn § 3 Abs. 1 Satz 3 ArbSchG verlangt permanent die Verbesserung des Schutzniveaus, wobei laut § 4 Ziff. 3 ArbSchG der Stand der Technik bei der Meidung oder Minimierung von Gefährdungen für die Beschäftigten zu berücksichtigen ist.

2. ZIELE

Datenschutz ist kein Zweck, sondern ein Mittel. Ständig genannte Zwecke oder Ziele[144] sind in diesem Zusammenhang der „Schutz der Privatsphäre“ oder „informationelle Selbstbestimmung“. Beide sind allerdings sehr abstrakt und als wichtige schutzwürdige Belange schwer greifbar. Dringend bedürfen sie der Konkretisierung. Es muss geklärt werden, um welche weiteren Interessen oder Werte es eigentlich dabei gehen soll. Zwar hat schon das BVerfG 1986 in seiner bahnbrechenden Entscheidung zur Volkszählung recht präzise beschrieben, welche gesellschaftlich relevanten Güter geschützt werden sollen.[145] Doch in der deutschsprachigen Diskussion um den Sinn des Datenschutzes ist seither wenig passiert. Es gibt wertvolle wissenschaftliche Einzelbeiträge, aber eine lebendige fächerübergreifende Diskussion, die auch das Alltagsverständnis erreicht, gibt es hierzu nicht.

Auch die Diskussion über Sinn und Zweck des Beschäftigtendatenschutzes ist seltsam unterentwickelt. Es gibt zwar ein verbreitetes Verständnis davon, dass der Beschäftigtendatenschutz eine besondere Rolle spielt.[146] Begründet wird dies zutreffend mit den enormen und ständig rasant steigenden Datenmengen, die über Beschäftigte im Betrieb verarbeitet werden (können), sowie mit dem Bedürfnis der betrieblichen Praktiker nach klaren und praxisnahen Regelungen.[147] Doch der tiefere Sinn, welche Probleme sich dahinter verbergen, die nach Schutzmaßnahmen verlangen, bleibt meist unbeleuchtet. Das führt dazu, dass Datenschutz ein eher bürokratisches, allseits mäßig beliebtes Dasein fristet.

Um diese wichtige Frage nicht nur mit Schlagworten zu beantworten, soll hier zunächst ein Rückgriff auf die allgemeinen Ziele des Datenschutzes insgesamt erfolgen, um dann deren Übertragbarkeit auf den Beschäftigtendatenschutz zu erörtern und Besonderheiten zu bestimmen. Es handelt sich um einen zweifellos vorläufigen und unvollständigen Versuch, zur Diskussion anzuregen.

2.1 ZIELE DES ALLGEMEINEN DATENSCHUTZES

Auf allgemeiner Ebene werden Sinn und Zweck des Datenschutzes darin gesehen, dass *Privatheit* und *informationelle Selbstbestimmung* des Individuums geschützt werden sollen.[148] Diese beiden Leitbegriffe bestimmen die internationale philosophische, sozialwissenschaftliche und vor allem juristische Debatte sowie die Rechtsprechung zum Datenschutz. Beide Belange haben eine große Schnittmenge, sind aber nicht deckungsgleich. Sie entstammen unterschiedlichen Rechtstraditionen und koexistieren infolge internationaler Bemühungen um ein länderübergreifendes Recht vor allem auf europäischer Ebene. Die begriffliche Abgrenzung ist selbst Gegenstand unabgeschlossener Debatten.[149] Klar ist aber, dass weder Privatheit noch informationelle Selbstbestimmung als letzte Zwecke betrachtet werden, sondern ihren Wert aus weitergehenden Zielsetzungen beziehen. Kurz zusammengefasst geht es um die Ermöglichung von Individualität, autonomer Lebensführung und verantwortlicher Partizipation des einzelnen Menschen im sozialen Kon-

[144] Ziel und Zweck werden hier synonym gebraucht.
[145] BVerfG v. 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, NJW 1984, 419 (422 ff.).
[146] *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, Rn. 21-26; *Kort*, RdA 2018, 24; *Krause*, NZA-Beilage 2017, 53 (58); *Krause*, Digitalisierung und Beschäftigtendatenschutz, BMAS Forschungsbericht 482, 2017, S. 46 ff.
[147] Überblick bei *Lurtz/Ruhmann*, Der lange Weg zu einem Beschäftigtendatenschutzgesetz?, ZD-Aktuell 2020, 07281.
[148] *Gusy/Eichenhofer*, BeckOK DatenschutzR, 33 Ed. 2020, BDSG § 1 Rn. 42-46.
[149] *Nebe*l, ZD 2015, 517.

text.[150] Politisch interpretiert geht es weiter um die Vielfalt der öffentlichen Meinungsbildung und um die Freiheit in der demokratischen Entscheidungsfindung.[151]

2.1.1 PRIVATHEIT

Im deutschen Recht gibt es kein „Right to Privacy". Eine Konkretisierung des allgemeinen Persönlichkeitsrechts stellt jedoch das Recht auf Privatsphäre dar,[152] das hohen Schutz in häuslicher Umgebung genießt. Nach Auffassung des BVerfG[153] im Fall „Caroline von Monaco" sei der Schutz der Privatsphäre thematisch und räumlich bestimmt. Er umfasse zum einen Angelegenheiten, die wegen ihres Informationsinhalts typischerweise als "privat" eingestuft würden, … Zum anderen erstrecke sich der Schutz auf einen räumlichen Bereich, in dem der Einzelne zu sich kommen, sich entspannen oder auch gehen lassen könne. … Im Kern gehe es um einen Raum, in dem er die Möglichkeit habe, frei von öffentlicher Beobachtung und damit der von ihr erzwungenen Selbstkontrolle zu sein, auch ohne dass er sich dort notwendig anders verhielte als in der Öffentlichkeit. Bestünden solche Rückzugsbereiche nicht mehr, so das BVerfG, könnte der Einzelne psychisch überfordert sein, weil er unausgesetzt darauf achten müsste, wie er auf andere wirke und ob er sich richtig verhalte. Ihm fehlten die Phasen des Alleinseins und Ausgleichs, die für die Persönlichkeitsentfaltung notwendig seien und ohne die sie nachhaltig beeinträchtigt würde. Diese Charakterisierung des Schutzes der Privatsphäre entspricht dem klassischen Verständnis vom „Right to Privacy" in den Vereinigten Staaten als „Right to be let alone" zum Schutz persönlicher Individualität.[154]

Im aktuellen Diskurs werden für das Paradigma der Privatheit jedoch weitergehend soziale und politische Zwecke genannt.[155] Ziel ist danach nicht mehr nur der Schutz von Rückzugsmöglichkeiten des Individuums. Weitergehend wird die Bedeutung der Privatsphäre für soziale Beziehungen thematisiert. Häufig wird das Problem beschrieben, dass das Individuum in unterschiedlichen Zusammenhänge unterschiedliche Rollen zu spielen habe.[156] Das kann nur gelingen, wenn die informationellen Barrieren zwischen verschiedenen Lebensbereichen kontrollierbar bleiben. Vertraute Beziehungen zu Familie und Freunden brauchen Privatsphäre, damit offen und angstfrei jegliches Anliegen geäußert und im Gespräch erwogen werden kann. Es geht dabei auch um die Chance, unkonventionelle Einstellungen, Ansichten oder Wünsche zunächst geschützt zu teilen. Weitergehend wird die Bedeutung der Privatsphäre für die demokratische Öffentlichkeit erörtert. Der öffentliche Meinungsstreit braucht unverzichtbar eine große Vielfalt der Ideen und Argumente auch weit außerhalb des Mainstreams. Die autonome Meinungsbildung des Individuums allein oder in vertrauten sozialen Beziehungen ist hierfür unverzichtbar.[157]

[150] *Gusy/Eichenhofer*, BeckOK DatenschutzR, 33 Ed. 2020, BDSG § 1 Rn. 44a.
[151] Z. B. *Boehme-Neßler*, Privacy: a matter of democracy. Why democracy needs privacy and data protection, International Data Privacy Law 2016, Vol. 6 No. 3, p. 222.
[152] Zu Konzept und Entstehung der Privatsphäre eingehend *Schwenke*, Private Nutzung von Smartglasses im öffentlichen Raum, S. 75 ff.
[153] BVerfG, Urt. v. 15.12.1999 – 1 BvR 653/96, GRUR 2000, 446 (450).
[154] Zur „Erfindung" des Rechts in den USA im Jahre 1890 durch Samuel Warren und Louis Brandeis siehe *Glancy*, The Invention of the Right to Privacy, Arizona Law Rev. 21, 1979, S. 1 (22).
[155] *Behrendt/Loh/Matzner/Misselhorn*, Einleitung, in: dies. (Hrsg.), Privatsphäre 4.0. Eine Neuverortung des Privaten im Zeitalter der Digitalisierung, 2019, 1 (6 f.).
[156] Z. B. *Becker/Seubert*, DuD 2016, 73, (76 f.).
[157] *Boehme-Neßler*, Privacy: a matter of democracy. Why democracy needs privacy and data protection, International Data Privacy Law 2016, Vol. 6 No. 3, p. 222 (227 f.).

2.1.2 INFORMATIONELLE SELBSTBESTIMMUNG

Das Bundesverfassungsgericht hat 1983 das Recht auf informationelle Selbstbestimmung aus den Grundrechten der freien Entfaltung der Persönlichkeit und der Unantastbarkeit der Menschenwürde abgeleitet. Es hat dieses Recht als weitere Konkretisierung des allgemeinen Persönlichkeitsrechts gekennzeichnet, das die Befugnis des Individuums gewährleistet, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[158] Damit wurde das Recht auf informationelle Selbstbestimmung zur maßgeblichen Grundlage des Datenschutzes in Deutschland.

Das Recht auf informationelle Selbstbestimmung stellt vor allem auf die Möglichkeit der Verknüpfung personenbezogener Daten durch moderne Informationstechnologien ab. Vor diesem Hintergrund gebe es, so das BVerfG, kein belangloses Datum mehr.[159] Der Bürger solle die Chance haben zu wissen, wer was wann über ihn weiß. Wer nicht mit hinreichender Sicherheit überschauen könne, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt seien, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermöge, könne in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.[160]

Schutz der Privatsphäre und Schutz der informationellen Selbstbestimmung sind neben ihrer Bedeutung als Individualrecht immer auch unter dem Gesichtspunkt diskutiert worden, dass demokratische Gemeinwesen in seiner Funktionstüchtigkeit zu schützen. Im Volkzählungsurteil des BVerfG, das die informationelle Selbstbestimmung 1983 als Verfassungsrecht ausformuliert hat, heißt es hierzu: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[161] Der Schutz vor Erfassung und Verwendung persönlicher Daten stellt daher ein eminent öffentliches Interesse dar.[162]

2.2 ZIELE DES BESCHÄFTIGTENDATENSCHUTZES

Vom Arbeitsverhältnis wird im Allgemeinen nicht erwartet, dass es einen besonders geschützten Rückzugsraum im Sinne der räumlichen Privatsphäre bietet. Rückzug in die Privatheit findet in der Freizeit, in der Familie, in der eigenen Wohnung oder im Ferienhaus statt. Arbeit hingegen findet traditionell in Betrieben oder Verwaltungen unter sozialen Kontakten statt. Eine Beobachtung des individuellen Sozial- und Leistungsverhaltens durch andere Betriebsangehörige und Betriebs-

[158] BVerfG v. 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, NJW 1984, 419 (422).
[159] Ebenda.
[160] Ebenda.
[161] BVerfG, Urt. v. 15.12.1983 - 1 BvR 209/83 u. a., NJW 1984, 419 (422), wieder aufgegriffen in BVerfG, Urt. v. 2. 3. 2006 - 2 BvR 2099/04, NJW 2006, 976 (979).
[162] *Winter*, Demokratietheoretische Implikationen des Rechts auf informationelle Selbstbestimmung, in: Friedewald/Lamla/Roßnagel (Hg.), 2017, S. 37 (46).

fremde ist dabei oft unvermeidlich und selbstverständlich. Dennoch hat Datenschutz im Arbeitsverhältnis zum Teil die gleichen Funktionen wie im gesellschaftlichen Leben insgesamt. Es können jedoch spezifische Ausformungen und zusätzliche Aspekte hinzukommen.[163]

2.2.1 PRIVATSPHÄRE IM BETRIEB

Gibt es im Betrieb ein „Right to be let alone"? Der Arbeitstag dauert immerhin bis zu 10 Stunden. Die menschliche Leistungskurve bleibt über einen solchen Zeitraum keineswegs konstant. Pausen sind für den Erhalt sowohl der physischen als auch der psychischen Gesundheit erforderlich, die je nach den Umständen des einzelnen Arbeitsplatzes auch gerade als Pausen frei von Beobachtungsdruck und informationeller Einbindung gestaltet sein müssen.

Aber auch private Gespräche am Arbeitsplatz sind legitim und wichtig, um soziale Beziehungen unterschiedlicher Intensität zu knüpfen und zu pflegen. Dabei geht es um eine Vielzahl von Belangen angefangen von der guten Arbeitsatmosphäre bis hin zum Wissen, wen man in einer kritischen Situation um Rat fragen kann.

2.2.2 SELBSTBESTIMMUNG STATT ANPASSUNGSDRUCK

Lange vor dem Volkszählungsurteil des BVerfG begann die Geschichte des Beschäftigtendatenschutzes in Deutschland mit einer Technik namens „Produktograph". Auch weil das BAG für dessen Einsatz ein Mitbestimmungsrecht des Betriebsrates 1960 abgelehnt hatte,[164] entschied der Gesetzgeber, im Betriebsverfassungsgesetz 1972 § 87 Abs. 1 Nr. 6 BetrVG aufzunehmen.[165] Den Druckern, die sich gegen den Produktographen gewehrt hatten, ging es nicht um Lohn. Eine Leistungslohnbemessung war anhand der Daten des Produktographen nicht vorgesehen. Ihnen ging es um Freiräume, ihren anerkannt hohen Sachverstand frei von Gängelung kompetent einzusetzen.

Die Überwachungstechnik hat sich seit 1972 dramatisch verändert. Gleichwohl sind bei vielen Tätigkeiten Eigeninitiative, Flexibilität und Kreativität mehr denn je gefordert, die sich jedoch unter ständiger Beobachtung und Ausforschung des Arbeitsverhaltens schwer entwickeln können.[166] Die erforderliche Motivation zum initiativen und kreativen Arbeiten hängt von einem weiten Spektrum von Faktoren ab. Freiräume in der Leistungserbringung gehören dazu. Datenschutz soll daher Anpassungsdruck mindern.[167]

2.2.3 GESUNDHEIT

Aus den bereits genannten Punkten ist schon deutlich geworden, dass es bei den Belangen Privatsphäre und Selbstbestimmung im Betrieb auch um die Gesundheit der Beschäftigten geht. Pausen in Gestalt unbeobachteter Entspannungsphasen oder privater Gespräche unter Kolleg*innen dienen der psychischen und physischen Gesundheit. Ihr Fehlen ist gesundheitsgefähr-

[163] Eine frühere Fassung dieser Thesen findet sich bereits in *Rose*, in: Festschrift für Taeger, 2020, S. 400 ff.
[164] BAG, 27.5.1960 – 1 ABR 11/59, BeckRS 1960, 103662.
[165] Zu den Einzelheiten *Schwarz*, Arbeitnehmerüberwachung und Mitbestimmung, 1982, S. 69 ff.
[166] Zum Anpassungsdruck durch kontinuierliche Videoüberwachung BAG, 29.6.2004 – 1 ABR 21/03, NZA 2004, 1278, 1281.
[167] Sehr anschaulich *Schröder,* Die digitale Treppe, Frankfurt am Main 2016, S. 134 f., der von Konformismusdruck spricht.

dend. Auch geringer Handlungsspielraum für eigenverantwortliches Arbeiten (z. B. durch elektronisch gelenktes Arbeitshandeln) gilt als psychischer Belastungsfaktor.[168]

Informationelle Selbstbestimmung richtet sich auch gegen den Beobachtungsdruck, der von zahlreichen Sensoren am Arbeitsplatz (z. B. von Videoüberwachung oder vernetzten Assistenzsystemen) ausgehen kann. Beobachtungsdruck könnte zu Stress und psychischer Belastung führen. Ob und unter welchen Umständen dies tatsächlich so ist, ist nicht befriedigend erforscht. Die großangelegte Meta-Studie von Backhaus[169] stellt für der Studien eine stresssteigernde Wirkung von Überwachungsmaßnahmen fest. Der Effekt ist insgesamt nicht sehr groß, aber signifikant. Stärker werden der Kontrollverlust und die gestiegene Beanspruchung unter Überwachung wahrgenommen. Weitere Forschung ist hier dringend erforderlich.

2.2.4 KONFLIKTFÄHIGKEIT UND MITBESTIMMUNG

Der Betrieb ist keine konfliktfreie Zone, sondern vielmehr durch charakteristische Interessengegensätze geprägt. Um einen gerechten Leistungsaustausch unter menschengerechten Bedingungen zu gewährleisten, ist die Konfliktfähigkeit der Beschäftigtenseite unverzichtbar. Ähnlich wie Privatsphäre und informationelle Selbstbestimmung die vielfältige öffentliche Meinungsbildung sichern (s. o.), bedarf auch im Arbeitsleben Kritik- und Konfliktfähigkeit der Beschäftigten des Schutzes entsprechender Daten. Das beginnt bei der Möglichkeit zum freien Meinungsaustausch der Beschäftigten z. B. über betriebliche Missstände. Kein System sollte – außerhalb begründeter Dokumentationspflichten – erfassen, wer mit wem über was spricht.

Das gilt verschärft, wenn ein Betriebsrat gegründet oder die Tarifbindung erkämpft werden soll. Derartige Kommunikation muss so weit wie möglich informationeller Selbstbestimmung unterliegen. Angesichts zunehmend effektiver Systeme der Persönlichkeitsbeurteilung besteht zudem die Gefahr, dass schon im Vorfeld Bewerber*innen im Hinblick auf ihren Widerspruchsgeist durchleuchtet werden. Die verbotene Frage nach der Gewerkschaftszugehörigkeit ist angesichts solcher Perspektiven fast schon Schnee von gestern. Auch das gezielte Kündigen potenzieller Aktivist*innen wird mit Big Data-Analysen und Legal Tech bedrohlich erleichtert.

2.2.5 LOHN UND LEISTUNG

Inwieweit auch das Austauschverhältnis zwischen Arbeitsleistung und Vergütung durch Datenschutz beeinflusst wird, ist bisher kaum erörtert. Dabei sind technische Einrichtungen zur Leistungsüberwachung nach § 87 Abs. 1 Nr. 6 BetrVG Hauptanknüpfungspunkt für die datenschutzrechtliche Mitbestimmung des Betriebsrats. Überwachung am Arbeitsplatz z. B. durch Kameras kann Freiräumen beschneiden und soll nicht selten Leistungsdruck erhöhen. Wer sich beobachtet fühlt, neigt zu spontanem Wohlverhalten, was auch in Überbeanspruchung der eigenen Kräfte münden kann. Bestimmte Formen des Antreibens zu möglichst hoher Arbeitsleistung können jedenfalls durch Daten- bzw. Persönlichkeitsschutz der Beschäftigten unterbunden werden. Das veranschaulicht eine BAG-Entscheidung aus dem Jahre 2017, wonach ein automatisiertes System

[168] *GDA*-Arbeitsprogramm Psyche, S. 17.
[169] *Backhaus*, Kontextsensitive Assistenzsysteme und Überwachung am Arbeitsplatz: Ein meta-analytisches Review zur Auswirkung elektronischer Überwachung auf Beschäftigte, ZArbWiss. 2019 73: 2 (9).

der lückenlosen, dauerhaften und detaillierten Erfassung des wesentlichen Arbeitsspektrums von Sachbearbeitern mit § 75 Abs. 2 BetrVG nicht zu vereinbaren sei.[170]

Jede digitalisierte individuelle Leistungsmessung oder Leistungsbeurteilung bedient sich personenbezogener Daten und ist daher auch nach datenschutzrechtlichen Kriterien zu beurteilen. Beschäftigtendatenschutz kann daher auch einen Beitrag zur betrieblichen Leistungsregulierung[171] sein. Im Zuge der Digitalisierung 4.0 ist damit zu rechnen, dass das Verhältnis von Lohn zu Leistung völlig neu vermessen wird, weil angesichts allgegenwärtiger Sensorik und Big Data-Analyse ganz neue Möglichkeiten der Arbeits- und Leistungsbewertung zur Verfügung stehen. Die Definitionshoheit, was eine angemessene Arbeitsleistung darstellt, hat dann derjenige, der über die Daten und deren Auswertung verfügt. Angesichts sinkender Tarifbindung wird dies häufig allein der Arbeitgeber sein. Beschäftigtendatenschutz könnte hier Grenzen setzen und jedenfalls für Transparenz sorgen.

Ein letzter Punkt in diesem Zusammenhang betrifft die Preisgabe von persönlichen Fertigkeiten, Spezialwissen oder Tricks, die die Arbeit erleichtern. Gibt es ein Recht auf informationelle Selbstbestimmung hinsichtlich solchen „privaten" Wissens? Oder hat der Arbeitgeber einen Anspruch darauf, das Know-how eines jeden Beschäftigten im Rationalisierungsinteresse auszuschöpfen. Allgegenwärtige Sensorik entscheidet diesen Konflikt zugunsten des Arbeitgebers. Angesichts ständig optimierungsbedürftiger KI-Anwendungen wird die Preisgabe personenbezogener Daten zunehmend selbst zum Leistungsinhalt. Wer den Roboter kollaborativ trainiert, investiert nicht nur Zeit und Arbeitskraft, sondern gibt auch das persönliche Know-how in Form personenbezogener Daten Preis.

[170] So erfolgt im Fall BAG, 25.4.2017 – 1 ABR 46/15, NZA 2017, 1205, 1210 f.
[171] Zu deren Krise *Haipeter*, WSI Mitteilungen 2020, 47.

3. POTENZIAL DES AKTUELLEN REGELUNGSSYSTEMS

Für Unternehmen und Beschäftigte ergeben sich die Pflichten und Rechte, die sich auf die vom Unternehmer verarbeiteten personenbezogenen Daten der Beschäftigten beziehen, aus dem – recht unübersichtlichen – Regelungssystem des Beschäftigtendatenschutzes. Betroffen sind in der Bundesrepublik Deutschland rund 40 Millionen Personen, deren Tun und Lassen sich Arbeitstag für Arbeitstag in vielen Fällen in großen Datenmengen niederschlägt. Zu welchen Anteilen diese Daten in den Machtbereich des Arbeitgebers gelangen und zu welchen Zwecken sie vom Arbeitgeber dann verarbeitet werden, unterliegt grundsätzlich dessen *Organisationsgewalt*. Die Organisationsmacht[172] des Arbeitgebers umfasst laut § 106 GewO ausdrücklich nicht nur Inhalt, Ort und Zeit der Arbeitsleistung, sondern auch Ordnung und Verhalten des Arbeitnehmers im Betrieb. Gegen die Freiheit des Arbeitgebers, die Leistungs- und Verhaltensdaten von Beschäftigten entsprechend seiner unternehmerischen Interessen und Präferenzen z. B. zu speichern, mit anderen Daten zusammenzuführen, zu analysieren oder weiterzugeben, steht das Datenschutzrecht. Es sind die Regelungen des Beschäftigtendatenschutzes, die der Freiheit des Arbeitgebers zur Verarbeitung von Beschäftigtendaten Grenzen setzen und den Arbeitnehmer*innen individuell bzw. deren Interessenvertretungen diesbezüglich Rechte einräumen.

Dieses Kapitel ist zweigeteilt. Es beginnt mit einer keineswegs trivialen Klärung der Frage, welche Regelungen eigentlich den Beschäftigtendatenschutz ausmachen (3.1). Es folgt eine Analyse des Wirkungspotenzials dieses Regelungssystems anhand seiner zentralen Stellschrauben (3.2). Der einleitende Überblick ist unverzichtbar, damit die anschließenden Untersuchungen zu maßgeblichen Details nicht nur für einen kleinen Kreis von Fachleuten verständlich sind. Die im zweiten Teil folgenden Analysen stellen sich der weiterführenden Frage, welches Potenzial das geltende Recht bei entschlossener Anwendung bietet, um den Herausforderungen der aktuellen umfassenden Digitalisierungsprozesse in den Unternehmen gerecht zu werden. Auf dieser Grundlage können dann in Kapitel 4 die Defizite erörtert werden.

3.1 ÜBERBLICK: WAS UMFASST DER BESCHÄFTIGTENDATENSCHUTZ?

Es wäre äußerst wünschenswert, dass sich die für so viele Menschen tagtäglich wichtigen Pflichten und Rechte des Beschäftigtendatenschutzes auf wenigen Seiten sinnvoll zusammenfassen lassen. Dafür wäre zunächst zu klären, wo denn die für das deutsche Recht maßgeblichen Regelungen zu finden sind, bevor die wichtigsten Bestimmungen benannt werden.

3.1.1 MAßGEBLICHE RECHTSQUELLEN

Fast umfassend wird der Schutz personenbezogener Daten von natürlichen Personen seit Mai 2018 durch die Datenschutz-Grundverordnung (DSGVO) auf EU-Ebene geregelt. Ein kurzer Aus-

[172] *Richter*, Begriff des Arbeitsgebers, in: Kiel/Lunk/Oetker (Hg.), Münchener Handbuch zum Arbeitsrecht, 4. Aufl., 2018, Band 1: Individualarbeitsrecht I, § 23 Rn. 2 f.

nahmekatalog nicht erfasster Bereiche findet sich in Art. 2 Abs. 2 DSGVO z. B. für persönliche und familiäre Tätigkeiten (lit c). Der Beschäftigtendatenschutz jedoch wird hier nicht genannt. Die Regelungen der DSGVO gelten auch für die Verarbeitung personenbezogener Daten der Beschäftigten durch deren Arbeitgeber.[173] Allerdings findet sich in Art. 88 DSGVO eine „Öffnungsklausel", die es den Mitgliedsstaaten in Abs. 1 erlaubt, durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorzusehen. Dies hat der deutsche Gesetzgeber mit § 26 BDSG ausdrücklich und wirksam[174] getan. Auch Regelungen im Betriebsverfassungsgesetz (§ 87 Abs. 1 Nr. 6 BetrVG) sowie in Personalvertretungsgesetzen, die eine Beteiligung der Interessenvertretungen bei der Datenverarbeitung vorschreiben, sollen weiter anzuwenden sein.

Damit jedoch ist noch nicht geklärt, welche Vorschriften für den Beschäftigtendatenschutz maßgeblich sind. Nach Art. 288 Abs. 2 AEUV haben europäische Verordnungen wie die DSGVO allgemeine Geltung, sind in allen ihren Teilen verbindlich und gelten in jedem Mitgliedstaat unmittelbar.[175] Grundsätzlich dürfen in ihrem Regelungsbereich keine nationalen Bestimmungen erlassen werden, schon gar nicht abweichende. Wie schon erwähnt, wird in Art. 88 DSGVO ausdrücklich zugelassen, dass für den Datenschutz der Beschäftigten auf nationaler Ebene „spezifischere Vorschriften" vorgesehen werden dürfen. Die Formulierung „spezifischere" wird allerdings so verstanden, dass konkrete nationale Regelungen des Beschäftigtendatenschutzes, wie sie in § 26 BDSG zu finden sind, die allgemeinen Vorschriften der DSGVO keinesfalls insgesamt verdrängen.[176] Verdrängt werden nur solche Regelungen der DSGVO, für die tatsächlich eine konkretere nationale Regelung in gleicher Sache als „lex specialis" getroffen worden ist,[177] z. B. wenn zur Einwilligung der Beschäftigten in die Datenverarbeitung national eine Regelung getroffen wird, die die allgemeinen Regelungen der DSGVO zur Einwilligung verdrängen könnte. Auch dann bleibt aber der Umstand, dass die nationale Regelung im Sinne entsprechender DSGVO-Vorschriften auszulegen ist.

Es ist also kaum ein Entrinnen aus der Situation, dass beim Beschäftigtendatenschutz ständig DSGVO und nationales Recht nebeneinander gelesen und dabei im Detail abgegrenzt oder aufeinander bezogen werden müssen. Der Rechtsklarheit und Anwendungsfreundlichkeit dient das nicht (siehe zu den Regelungsoptionen Kap. 5).

3.1.2 ZULÄSSIGE DATENVERARBEITUNG NACH § 26 ABS. 1-4 BDSG

Aus § 26 BDSG ist vor allem zu entnehmen, unter welchen Voraussetzungen Beschäftigtendaten verarbeitet werden dürfen. Gesetzestechnisch ist sowohl in der DSGVO als auch im BDSG der Grundgedanke, dass die Verarbeitung personenbezogener Daten verboten ist, es sei denn, sie ist jeweils nach Inhalt und Zweck gesetzlich oder in gesetzlich anerkannter Form zugelassen.

[173] BeckOK DatenschutzR/*Riesenhuber*, 33. Ed. 1.5.2020, DS-GVO Art. 88 Rn. 15; EuArbRK/*Franzen*, 3. Aufl., 2020, DSGVO Art. 88 Rn. 5.
[174] Jedenfalls vom BAG zweifach bestätigt in BAG v. 9.4.2019 – 1 ABR 51/17, NZA 2019, 1055, 1057 und BAG v. 7.5.2019 – 1 ABR 53/17, NZA 2019, 1218, 1223.
[175] BeckOK DatenschutzR/*Riesenhuber*, 33. Ed. 1.5.2020, DS-GVO Art. 88 Rn. 15; Taeger/Gabel/*Zöll*, 3. Aufl., 2019, DSGVO Art. 88 Rn. 7.
[176] Auernhammer/*Forst*, 7. Aufl., 2020, DSGVO Art. 88, Rn. 4; EuArbRK/*Franzen*, 3. Aufl., 2020, DS-GVO Art. 88 Rn. 6; Simitis/Hornung/Spiecker gen. Döhmann/*Seifert,* 1. Aufl., 2019, DSGVO Art. 88, Rn. 21.
[177] BeckOK DatenschutzR/*Riesenhuber*, 33. Ed. 1.5.2020, DS-GVO Art. 88 Rn. 16; ähnlich EuArbRK/*Franzen*, 3. Aufl., 2020, DSGVO Art. 88 Rn. 6; Schwartmann et al./*Thüsing/Traut*, 2. Aufl., 2020, DS-GVO Art. 88, Rn. 20.

Insgesamt werden in § 26 Abs. 1-4 BDSG drei Quellen unterschieden, auf denen die Zulässigkeit der Datenverarbeitung beruhen kann:

- auf einer gesetzlichen Erlaubnisnorm aus der Aufzählung in § 26 Abs. 1 und 3 BDSG,
- auf einer Einwilligung des betroffenen Beschäftigten gemäß § 26 Abs. 2 BDSG oder
- auf einer Kollektivvereinbarung gemäß § 26 Abs. 4 BDSG.

a) Gesetzliche Erlaubnisnormen

Zur Konkretisierung der gesetzlichen Erlaubnisnormen wird in § 26 Abs. 1 BDSG als allgemeiner Rahmen zunächst festgestellt, dass es um Zwecke des Beschäftigungsverhältnisses gehen muss, um dann abschließend fünf Erlaubnisgründe festzulegen. Die Datenverarbeitung muss demnach für einen der folgenden Zwecke erforderlich sein:

- Für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses,
- für die Durchführung des Beschäftigungsverhältnisses,
- für die Beendigung des Beschäftigungsverhältnisses,
- zur Ausübung oder Erfüllung der Rechte und Pflichten der Interessenvertretung der Beschäftigten
- oder zur Aufdeckung von Straftaten.

Für die Verarbeitung „besondere Kategorien personenbezogener Daten“ gilt allerdings § 26 Abs. 3 BDSG. Damit sind die „sensiblen Daten“ gemeint, die in Art. 9 Abs. 1 DSGVO aufgezählt werden, also Daten, aus denen

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen
- oder die Gewerkschaftszugehörigkeit

hervorgehen sowie

- genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten
- oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Auch solche „sensiblen Daten“ dürfen für Zwecke des Beschäftigungsverhältnisses auf gesetzlicher Grundlage verarbeitet werden, wenn die im Vergleich wohl etwas strengeren Voraussetzungen des § 26 Abs. 3 BDSG erfüllt werden.

b) Erlaubnis durch Einwilligung

Die Einwilligung der jeweils betroffenen Beschäftigten ist eine völlig andersgeartete Erlaubnisgrundlage für die Datenverarbeitung im Unternehmen. Sie ist zwar in DSGVO und BDSG gesetzlich

anerkannt. Sie ist aber inhaltlich nicht durch das Gesetz beschränkt. Denn nicht das Gesetz, sondern der freie Wille des Betroffenen ist hier die Legitimationsgrundlage. Während die genannten gesetzlichen Erlaubnisgründe mehr oder weniger streng auf das rational Sinnvolle und Interessengerechte begrenzt sind, verwirklicht die Einwilligung die informationelle Selbstbestimmung des Beschäftigten. Die einzige Voraussetzung ist, dass die Einwilligung tatsächlich freiwillig erfolgt. Genau auf diesen Aspekt beziehen sich die gesetzlichen Einschränkungen. Gerade im Beschäftigungsverhältnis, das der einseitigen Organisations- und Weisungsmacht des Arbeitgebers unterliegt, aber auch bei einer Bewerbung für ein Beschäftigungsverhältnis bestehen große Zweifel an der Freiwilligkeit einer Einwilligung der Beschäftigten bzw. Bewerber*innen. Denn unerfreuliche Konsequenzen einer Verweigerung der Einwilligung stehen jederzeit im Raum.

In Art. 4 Ziff. 11 DSGVO, der auch für das BDSG maßgeblich ist, wird unter „Einwilligung" jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung verstanden. Ohne Freiwilligkeit liegt also keine Einwilligung im Rechtssinne vor.

In § 26 Abs. 2 BDSG wird die Einwilligung für das Beschäftigungsverhältnis zweifach konkretisiert. Auf der formalen Ebene hat der Arbeitgeber die Einwilligung in der Regel schriftlich oder elektronisch einzuholen, nachdem die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht aufgeklärt worden ist. Auf der inhaltlichen Ebene muss die Freiwilligkeit der Einwilligung unter Berücksichtigung der im Beschäftigungsverhältnis bestehenden Abhängigkeit der beschäftigten Person sowie der Umstände, unter denen die Einwilligung erteilt worden ist, beurteilt werden. Um dies zu veranschaulichen, nennt der Gesetzgeber hier zwei Regelbeispiele. Freiwilligkeit kann demnach insbesondere dann vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

c) Erlaubnis durch Kollektivvertrag

Schließlich kann als Erlaubnisgrundlage auch eine Regelung in einem *Kollektivvertrag* dienen. Vereinbarungen zwischen dem Arbeitgeber auf der einen Seite und dem Betriebs- oder Personalrat auf der anderen Seite sowie gewerkschaftlich ausgehandelte Tarifverträge können die Verarbeitung personenbezogener Beschäftigtendaten ebenfalls erlauben. Auch hier gibt es im Gesetz keine ausdrücklichen inhaltlichen Einschränkungen. Allerdings sind die Kollektivvertragspartner an die inhaltlichen Vorgaben des Art. 88 Abs. 1 und Abs. 2 DSGVO sowie an grundrechtliche Wertungen gebunden. Im Ergebnis werden sie damit bei der Formulierung von spezifischen Erlaubnisnormen ähnliche Abwägungen vorzunehmen haben, wie sie auch der Gesetzgeber nach § 26 Abs. 1 und 3 BDSG fordert.

3.1.3 ERGÄNZENDE REGELUNGEN AUS DER DSGVO

Die DSGVO enthält sonst keine Vorschriften, die speziell im Arbeitsverhältnis gelten. Es gibt dort aber zahlreiche generell geltenden Rechte der Betroffenen und Pflichten der Verantwortlichen, die auch im Betrieb anzuwenden sind. Aus diesen Teilen der DSGVO, die durch § 26 BDSG keinesfalls verdrängt werden, ergeben sich für den Beschäftigtendatenschutz eine Fülle an weiteren Vorschriften, die vor allem der organisatorischen und technischen Durchsetzung des Datenschutzes im betrieblichen Alltag dienen können. In erster Linie geht es um die Rechte der betroffenen Personen (hier: der betroffenen Beschäftigten) gemäß Art. 12-23 DSGVO sowie um die Pflichten der für die Datenverarbeitung Verantwortlichen (hier: der Arbeitgeber) vor allem gemäß

Art. 24-39 DSGVO. Hinzu kommen zahlreiche Grundsätze einer rechtskonformen Datenverarbeitung vor allem nach Art. 5 DSGVO.

a) Rechte der Beschäftigten

Bei den Rechten der betroffenen Beschäftigten geht es – plakativ formuliert – um *Transparenz, Berichtigung und Löschung*. In der DSGVO wird gerade Transparenz immer wieder besonders betont, z. B. bei den Vorgaben für spezifische nationale Regelungen des Beschäftigtendatenschutzes in Art. 88 Abs. 2 DSGVO. Die Regelungen des Rechts auf Transparenz in den Art. 12-15 DSGVO erschließt sich nicht auf den ersten Blick. Denn in den Art. 12-14 DSGVO geht es erstmal um Informationspflichten des Verantwortlichen, also im Beschäftigungskontext des Arbeitgebers, bevor sich dann aus Art. 15 DSGVO endlich ein Recht auf Auskunft der betroffenen Beschäftigten entnehmen lässt. Die insofern komplizierte Regelung ist aber durchaus nachvollziehbar. Denn damit hängt die Transparenz nicht von der Initiative einzelner Beschäftigter ab, sondern der Arbeitgeber muss als derjenige, der die betriebliche Datenverarbeitung organisiert, in Vorleistung treten und ungefragt einzelne Betroffene jeweils detailliert über die Datenverarbeitung informieren. Einzelheiten ergeben sich aus den Informationskatalogen der Art. 13 bzw. 14 Abs. 1 und 2 DSGVO. Dazu gehört gemäß Art. 13 Abs. 2 lit. b-d und Art. 14 Abs. 2 lit. c-e DSGVO auch die Informationen, welche Rechte betroffene Beschäftigte beim Arbeitgeber oder auch bei der Aufsichtsbehörde geltend machen können. Das eigentliche „Recht" zur Herstellung von Transparenz ergibt sich dann aus Art. 15 DSGVO. Beschäftigte, die sich unzureichend informiert fühlen, können auf dieser Grundlage weitere Details bis hin zu einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, nach Art. 15 Abs. 3 DSGVO verlangen.

Vorrangig interessant sind für Beschäftigte folgende Rechte:

- Recht auf Auskunft (Art. 15 DSGVO)
- Recht auf Berichtigung bzw. Vervollständigung (Art. 16 DSGVO)
- Recht auf Löschung vor allem unrechtmäßig oder nicht mehr zulässig verarbeiteter Daten (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung vor allem für Schwebezustände noch ungeklärter Rechtmäßigkeit der Verarbeitung (Art. 18 DSGVO)
- Recht auf Widerspruch gegen eine Datenverarbeitung aus Gründen einer besonderen Situation eines betroffenen Beschäftigten (Art. 21 Abs. 1 DSGVO) – einschließlich[178] eines Widerspruchs gegen ein Profiling i. S. v. Art. 22 DSGVO.
- Recht auf Beschwerde bei der Aufsichtsbehörde (Art. 77 Abs. 1 DSGVO)

b) Pflichten des Arbeitgebers

Besonders umfassend quer durch die gesamte DSGVO ist das Thema der Pflichten der verantwortlichen Person (hier also des Arbeitgebers) geregelt. Der Arbeitgeber ist im Betrieb der für die Verarbeitung der Beschäftigtendaten Verantwortliche, dem damit grundlegend nach Art. 5 Abs. 2 DSGVO die Einhaltung der datenschutzrechtlichen Verpflichtungen der DSGVO auferlegt worden ist. Er hat für die Rechtmäßigkeit der personenbezogenen Datenverarbeitung zu sorgen und muss diese nachweisen können. Er hat sicherzustellen, dass nur im Rahmen der Erlaubnisnormen Art. 6 und 9 DSGVO, § 26 Abs. 1-4 BDSG für festgelegte legitime Zwecke

[178] So jedenfalls Taeger/Gabel/*Taeger*, 3. Aufl., 2019, DSGVO Art. 22 Rn. 76.

erforderliche Datenverarbeitungen stattfinden (Zweckbindung gem. Art. 5 Abs. 1 lit. b DSGVO) und dass dabei die *Prinzipien* der Datensparsamkeit, Datenminimierung, Datenrichtigkeit, zeitlichen Begrenzung der Datenspeicherung, Integrität und Vertraulichkeit der Daten (lit. c-f) durchgeführt werden. In § 26 Abs. 5 BDSG wird ausdrücklich betont, dass der verantwortliche Arbeitgeber geeignete Maßnahmen zu ergreifen hat, um sicherzustellen, dass diese Grundsätze – insbesondere aus Art. 5 DSGVO – eingehalten werden.

Darüber hinaus sind eine Reihe verpflichtender *Instrumente der DSGVO* zu nennen, die die tatsächliche Umsetzung des Datenschutzes unterstützen sollen und für die praktische Wirksamkeit von entscheidender Bedeutung sein können, insbesondere:

- Datenschutz durch Technikgestaltung nach Art. 25 DSGVO
- Verarbeitungsverzeichnis nach Art. 30 DSGVO
- Technische und organisatorische Maßnahmen nach Art. 32 DSGVO
- Meldung von Datenschutzverletzungen nach Art. 33 DSGVO
- Datenschutz-Folgenabschätzung nach Art. 35 DSGVO
- Datenschutzbeauftragte nach Art. 37 DSGVO

Eine zentrale Rolle für das vorliegende Thema der fortschreitenden Digitalisierung kommt dabei der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO zu, denn hier sollen die Risiken der Verwendung neuer Technologien *vorab* vom Arbeitgeber bewertet und Abhilfemaßnahmen getroffen werden.

3.1.4 MITBESTIMMUNG

Zum Beschäftigtendatenschutz zählen schließlich die Beteiligungsrechte der Betriebsräte u. a. nach § 87 Abs. 1 Nr. 6 BetrVG und der Personalräte nach den Bundes- und Landespersonalvertretungsgesetzen (siehe § 26 Abs. 6 BDSG).

3.2 KRITISCHE PUNKTE IM BESCHÄFTIGTENDATENSCHUTZ

Nach diesem Überblick sollen nun zentrale Aspekte näher untersucht werden, ob sie den in Kap. 1 beschriebenen Herausforderungen der Digitalisierung des Arbeitslebens gerecht werden. Gesucht sind insbesondere die *„Stellschrauben"* im geltenden Recht, die – neu justiert – helfen können, Beschäftigtendatenschutz auch künftig wirksam zu praktizieren.

Dazu sollen zunächst in vier Unterpunkten die Zulässigkeitsnormen in § 26 Abs. 1-4 BDSG untersucht werden, inwieweit sie ein wirkungsvolles Instrument zur Bewältigung der Herausforderungen darstellen können. Im zweiten Schritt geht es dann in zwei Unterpunkten um die ergänzend anzuwendenden Transparenz- und Umsetzungsnormen der DSGVO.

3.2.1 ZULÄSSIGKEIT FÜR DIE DURCHFÜHRUNG DES BESCHÄFTIGUNGSVERHÄLTNISSES

Nach § 26 Abs. 1 Satz 1 BDSG ist die Verarbeitung personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses zulässig, wenn dies u. a. für dessen Durchführung erforderlich ist.

Unter den fünf genannten Zwecken:

- Für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses,
- für die Durchführung des Beschäftigungsverhältnisses,
- für die Beendigung des Beschäftigungsverhältnisses,
- zur Ausübung oder Erfüllung der Rechte und Pflichten der Interessenvertretung der Beschäftigten,
- oder zur Aufdeckung von Straftaten,

ist der Zweck „Durchführung des Beschäftigungsverhältnisses“ der für die digitale Zukunft bei weitem bedeutungsvollste. Der weitaus größte Teil der bevorstehenden Digitalisierung fällt in diese Kategorie. Das gilt etwa für die angestrebte Vernetzung aller Arbeitsprozesse oder für die Digitalisierung des Arbeits- und Gesundheitsschutzes z. B. durch Assistenzsysteme, wobei Besonderheiten bei der Verarbeitung sensibler Daten zu beachten sind (siehe 3.2.1 c). Auch das Thema Überwachung des Arbeits- und Leistungsverhaltens der Beschäftigten gehört weitgehend zu diesem Zweck und fällt nur ausnahmsweise unter den Spezialtatbestand „Aufdeckung von Straftaten“. Lediglich das digitalisierte „Recruiting“ fällt nicht darunter, sondern unter den Spezialtatbestand „Entscheidung über die Begründung eines Beschäftigungsverhältnisses“ (siehe 3.2.2).

Das Gesetz verzichtet auf konkrete Kategorien oder Beispiele. Die einzelnen Zwecke einer Datenverarbeitung, die im digitalisierten Betrieb vorstellbar sind, werden nicht weiter ausdifferenziert. Erst recht gibt es für die Vielzahl einzelner Programme bzw. Instrumente der Datenverarbeitung, die im Beschäftigungsverhältnis zum Einsatz kommen können, keinerlei Spezialregelungen, die dem Anwender Rechtsicherheit gewähren könnten. Für alle gilt der sehr allgemeine Maßstab ihrer Erforderlichkeit für Zwecke des Beschäftigungsverhältnisses nach § 26 Abs. 1 Satz 1 BDSG, es sei denn, es werden sensible Daten verarbeitet, die unter § 26 Abs. 3 Satz 1 BDSG fallen. In dem Fall gilt der ebenfalls sehr weite und abstrakte Maßstab, dass die Datenverarbeitung zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich sein muss und außerdem kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Ob diese Dopplung höchst abstrakter Maßstäbe in der Praxis ernsthaft zu handhaben ist, sei hier schon mal bezweifelt.

Derart *hochabstrakte Maßstäbe* haben zur Folge, dass um die Interpretation im Einzelfall immer wieder neu gestritten werden kann, bis höchste Gerichte wie das BAG oder der EuGH für eine gewisse Klarheit sorgen. Das geschieht regelmäßig erst fünf bis zehn Jahre nach dem Aufkommen einer neuen Technologie. Immerhin aber haben Rechtsprechung und Rechtslehre eine recht einheitliche Meinung dazu entwickelt, wie die einzelnen Schritte der rechtlichen Prüfung der datenschutzrechtlichen Zulässigkeit im Einzelfall auszusehen haben. Bis zu einem gewissen Grad haben sich auch konkretere Maßstäbe der Prüfung entwickelt, die zweifellos eine wichtige Stellschraube

für die Wirksamkeit des Beschäftigtendatenschutzes darstellen. Nachfolgend werden die einzelnen Prüfschritte der Reihe nach beleuchtet.

a) Konkretisierung der Zwecke

Um die Zulässigkeit einer personenbezogenen Datenverarbeitung zu gewährleisten, muss der jeweilige Zweck genauer bestimmt werden. Nach dem Grundsatz der „Zweckbindung" muss vor der Erhebung[179] festgelegt werden, für welche i. S. v. Art. 5 Abs. 1 lit. b) DSGVO eindeutigen und legitimen Zwecke die Daten verarbeitet werden sollen. Es lohnt sich, schon bei diesem ersten Merkmal einen Moment zu verharren. Denn die Qualität der rechtlichen Prüfung einzelner Vorhaben der Datenverarbeitung hängt stark davon ab, wie streng die Zwecksetzung beurteilt wird. Das hat vier Aspekte.

Erstens ist niemals die jeweilige Datenverarbeitung selbst der Zweck, sondern es geht um die *Ziele oder Aufgaben*, die mit der Datenverarbeitung erreicht werden sollen.[180]

Zweitens muss der Zweck *konkretisiert* werden.[181] Allein die abstrakte gesetzliche Formulierung „Durchführung des Arbeitsverhältnisses" reicht als Zwecksetzung nicht.[182] Wie konkret allerdings die Zwecksetzung gefasst werden muss, ist unklar. Diese rechtliche Unsicherheit, so heißt es,[183] führe dazu, dass in der Praxis insbesondere bei Big Data-Anwendungen sehr weite Zwecke benannt würden, um die Grenzen des Erlaubten auszuloten. Zutreffend heißt es demgegenüber, dass ein Stöbern in Beschäftigtendaten ins Blaue hinein ohne konkreten Zweck mit dem Grundsatz der Zweckbindung unvereinbar sei.[184] Der Zweckbindungsgrundsatz stehe vor allem unkontrollierten Big-Data-Analysen im Personalbereich entgegen.[185] Aber ob dies angesichts diffuser gesetzlicher Anordnungen funktioniert, ist zweifelhaft.

Hier befindet sich jedenfalls eine *wichtige Stellschraube*. Das gilt umso mehr, als die formulierten Zwecke im Rahmen des Transparenzgebotes den betroffenen Beschäftigten gemäß Art. 13 Abs. 1 lit. c) bzw. Art. 14 Abs. 1 lit c) DSGVO mitzuteilen sind. Hier entscheidet sich also auch, wie genau der oder die Beschäftigte erfährt, was mit den erhobenen Daten eigentlich geschehen soll.

Drittens fragt sich, ob Zwecke, die der Arbeitgeber verfolgen will, inhaltlich begrenzt sind. Es sollen laut Art. 5 Abs. 1 lit. b) DSGVO *legitime Zwecke* sein. Das wäre wohl generell erreicht, wenn sie mit der Durchführung des Arbeitsverhältnisses in einem klaren Zusammenhang stehen. In der maßgeblichen Öffnungsklausel in Art. 88 DSGVO wird in Abs. 1 der Beschäftigungskontext durch Regelbeispiele erläutert. Insbesondere geht es danach um u. a. Zwecke der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden. In diesen und ähnlichen Feldern müssten die Zwecke verortet sein. Bei der Festlegung wird dem Arbeitgeber ein gewisser Entscheidungsspielraum zugebilligt.[186] In der Tat hat der Arbeitgeber das Unternehmen zu leiten. Er legt im Rahmen der Gesetze und ggf. unter Mitbestimmung eines Betriebsrates fest, nach welchen

[179] Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, BDSG § 26 Rn. 17; *Culik/Döpke*, ZD 2017, 226 (227).
[180] *Hornung/Hofmann*, in: Hirsch-Kreinsen/Ittermann/Niehaus (Hrsg.), Digitalisierung industrieller Arbeit, 2. Aufl., 2018, S. 233 (240).
[181] Mit Beispielen *Däubler*, Gläserne Belegschaften, 8. Aufl., 2019, Rn. 394 ff.; *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, Rn. 2290 ff.
[182] *Hornung/Hofmann*, in: Hirsch-Kreinsen/Ittermann/Niehaus (Hrsg.), Digitalisierung industrieller Arbeit, 2. Aufl., 2018, S. 233 (240).
[183] *Culik/Döpke*, ZD 2017, 226 (227).
[184] Auernhammer/*Forst*, 7. Aufl., 2020, BDSG § 26 Rn. 65.
[185] Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, BDSG § 26 Rn. 17.
[186] *Hornung/Hofmann*, in: Hirsch-Kreinsen/Ittermann/Niehaus (Hrsg.), Digitalisierung industrieller Arbeit, 2. Aufl., 2018, S. 233 (240).

Methoden Produkte hergestellt oder Dienstleistungen erbracht werden. Auch die Methoden der Unternehmensführung einschließlich des Personalmanagements unterliegen grundsätzlich seiner Entscheidungsgewalt. Im Arbeitsschutz ist es sogar die gesetzliche Pflicht des Arbeitgebers nach § 3 Abs. 1 ArbSchG, die erforderlichen Entscheidungen zu treffen. Ob eine und welche Strategie der Überwachung der Arbeitsleistung, um ein klassisches Beispiel zu nennen, etabliert werden soll, liegt zunächst – jedenfalls in der Phase der Zwecksetzung – bei ihm.

Das Zauberwort „Digitalisierung" wird bei der Frage der Legitimität der Zwecksetzung aktuell eine zentrale Rolle spielen. Denn angesichts der unter dem Stichwort Industrie 4.0 klar gesetzten Paradigmen der Betriebswirtschaftslehre wird es kaum jemand für abwegig halten, dass umfassende betriebliche Digitalisierungsstrategien einen legitimen Zweck verfolgen.

Viertens ist es dem Verantwortlichen unter bestimmten Bedingungen erlaubt, Daten unter geänderten Zwecken weiterzuverarbeiten.[187] Es wird beobachtet bzw. befürchtet, dass in der Praxis der Digitalisierung, eine Vermischung von Daten, die zu unterschiedlichen Zwecken erhoben worden sind, stattfindet, ausforschende Big-Data-Analysen ohne konkreten Zweck durchgeführt und Daten als Trainingsmaterial für KI-Anwendungen zweckentfremdet werden.[188] Zu der schon erwähnten Problematik, dass gesetzlich an die Konkretisierung der Zwecksetzung keine klaren Anforderungen formuliert werden, kommt die gesetzlich ausdrücklich vorgesehene Möglichkeit der nachträglichen *Zweckänderung* durch den Verantwortlichen (= Arbeitgeber) hinzu.[189] Für jede weitere Big-Data-Analyse könnte unter Ausnutzung dieser Möglichkeit ein jeweils neuer Zweck zur erneuten Verarbeitung der Daten definiert werden. Keine andere Thematik ist in DSGVO und BDSG umständlicher und undurchschaubarer geregelt als gerade das Recht der Zweckänderung.

Diese „Stellschraube" wird daher auch durch die Rechtsprechung nicht absehbar so zu justieren sein, dass ausreichende Rechtsklarheit für die Praxis eintritt.

b) Erforderlichkeit

Erst auf der Grundlage der erfolgten Zwecksetzung kann eine Prüfung der Erforderlichkeit der jeweiligen Datenverarbeitung stattfinden. Der Begriff „erforderlich" durchzieht DSGVO und BDSG, ohne dass es eine klare Definition gäbe. Umstritten[190] ist erstens, wie zwingend und unverzichtbar für den gesetzten Zweck eine erforderliche Datenverarbeitung sein muss. Zweitens geht es um die Frage, ob schon allein der Begriff „erforderlich" eine Interessenabwägung impliziert.

Der zweite Punkt scheint immerhin für den Beschäftigtendatenschutz geklärt zu sein. Alles spricht dafür, dass v. a. die Formulierung in § 26 Abs. 1 Satz 1 BDSG „dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies … erforderlich ist" eine Interessenabwägung einschließt, obwohl dies im Unterschied zu Abs. 3 nicht ausdrücklich angeordnet wird. Gleich drei starke Argumente sprechen dafür. In der maßgeblichen Öffnungsklausel Art. 88 DSGVO werden in Abs. 2 die berechtigten Interessen und die Grundrechte der betroffenen Person besonders hervorgehoben.[191] Eine spezifischere Vorschrift des nationalen Rechts, in der diese berechtigten

[187] *Däubler*, Gläserne Belegschaften, 8. Aufl., 2019, Rn. 391c ff.
[188] *Culik/Döpke*, ZD 2017, 226 (230); *Joos*, NZA 2020, 1216 (1219), *Weichert/Schuler*, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2020_beschdsg_final.pdf, S. 8 f.
[189] *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, Rn. 2298 ff.
[190] Taeger/Gabel/*Taeger*, 3. Aufl., 2019, DSGVO Art. 6 Rn. 49.
[191] Darauf stellt auch Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, BDSG § 26 Rn. 18 ab.

Interessen völlig ausgeblendet bleiben, kann dem nicht gerecht werden. Der nationale Gesetzgeber des § 26 BDSG stellt sich das ausweislich der Begründung des Gesetzentwurfs in BT-Drs. 18/11325, S. 97 so vor, dass im Rahmen der Erforderlichkeitsprüfung die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwägen seien. Die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten seien zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt. Nun sind Begründungen von Gesetzentwürfen kein verbindlicher Normtext. Aber in Zusammenhang mit den verbindlichen Vorgaben in Art. 88 Abs. 2 DSGVO ist die Sache eindeutig. Eine Interessenabwägung ist in den Gesetzestext hineinzulesen. Dem hat sich auch das BAG am 7.5.2019 bei Auslegung des § 26 Abs. 1 Satz 2 BDSG ausdrücklich angeschlossen, um dann im zu entscheidenden Fall eine Interessenabwägung durchzuführen.[192] Dies ist gefestigte Rechtsprechung, da sie an die Interpretation des Begriffs Erforderlichkeit in der Vorgängervorschrift § 32 Abs. 1 Satz 1 BDSG a.F. direkt anknüpft.[193] Auch die Fachliteratur folgt dem.[194]

Kritisiert wird zu Recht, dass der Gesetzgeber des neuen BDSG gut daran getan hätte, das unpräzise Erforderlichkeitskriterium nicht erneut zu verwenden, sondern das, was eigentlich gemeint ist (Verhältnismäßigkeitsprinzip; Interessenabwägung), auch im Gesetzestext zum Ausdruck zu bringen.[195]

Demnach wird die Prüfung der Erforderlichkeit in insgesamt drei Schritten durchgeführt. Die Datenverarbeitung muss geeignet, im Sinne eines mildesten Mittels erforderlich und schließlich nach Abwägung der Interessen der Beteiligten angemessen sein. Soweit ist dies mittlerweile klar herrschende Lehre und Meinung. Allerdings tritt bei jedem einzelnen Punkt erneut die Frage auf, wie streng die Prüfung durchzuführen ist.

Geeignetheit

Bei der Frage der Eignung des jeweiligen Mittels der Datenverarbeitung für den gesetzten Zweck zeigen sich Literatur und Rechtsprechung meist großzügig. Der Punkt wird kurz abgehakt, übersprungen oder es werden Zweifel geäußert, die dann im Hinblick auf ein Scheitern der Datenverarbeitung an den folgenden Prüfpunkten offen gelassen werden. Letzteres geschah etwa in der Entscheidung des BAG vom 25.4.2017, in der es um eine technisch detailliert erfasste Belastungsstatistik ging. Es heißt dort, dass angesichts der erfassten Daten schon Vieles dafür spräche, dass die eingesetzten Mittel als solche untauglich seien, den vorgegebenen Zweck, eine unterschiedliche Belastungssituation der Arbeitnehmer und deren Ursachen in Erfahrung zu bringen, zu fördern.[196] Erst beim Prüfpunkt der Angemessenheit aber machte das BAG Nägel mit Köpfen und erklärte die betreffende Datenverarbeitung für rechtswidrig.

Die Lehrmeinungen zum Prüfungsmaßstab klingen oft ebenfalls zögerlich. Geeignet sei eine Verarbeitung, wenn sie beitrage, das legitime Ziel zu erreichen.[197] Es sei zu prüfen, ob der mit der Maßnahme angestrebte Zweck gefördert werden könne.[198] In der Tat ist die Frage der Eignung

[192] BAG v. 7.5.2019 – 1 ABR 53/17, NZA 2019, 1218 Rn. 42 f.
[193] Siehe z. B. BAG v. 20.6.2013 – 2 AZR 546/12, NZA 2014, 143 Rn. 26; BAG v. 17.11.2016. – 2 AZR 730/15, NZA 2017, 394 Rn. 30; BAG v. 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327 Rn. 30.
[194] Auernhammer/*Forst*, 7. Aufl., 2020, BDSG § 26 Rn. 63 ff.; ErfK/*Franzen*, 20. Aufl., 2020, BDSG § 26 Rn. 9-11; Gola/Heckmann/*Gola*, 13. Aufl., 2019, BDSG § 26 Rn. 16; Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, BDSG § 26 Rn. 18 f.; Taeger/Gabel/*Zöll*, 3. Aufl., 2019, BDSG § 26 Rn. 25; *Wybitul*: Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DSGVO, NZA 2017, 413 (415).
[195] *Kort*, ZD 2017, 319 (320).
[196] BAG v. 25.4.2017 – 1 ABR 46/15, NZA 2017, 1205 Rn. 25 f.
[197] Auernhammer/*Forst*, 7. Aufl., 2020, BDSG § 26 Rn. 64.
[198] ErfK/*Franzen*, 20. Aufl., 2020, BDSG § 26 Rn. 10.

eines bestimmten Instrumentariums der Datenerfassung, um damit bestimmte unternehmerische Zwecke zu erreichen, keine juristische, sondern eine technische, betriebsökonomische oder arbeitswissenschaftliche Frage. Unternehmerische Entscheidungsfreiheit bei der Wahl der Mittel beansprucht hier ebenso wie Experimentierfreude bei der technischen Optimierung der Arbeitsabläufe ausreichende Spielräume.

Unterschieden werden müsste aber schon zwischen einem zwar kleinen, aber verlässlichen, und einem zweifelhaften Beitrag zur Zweckerreichung. Der umfassende Digitalisierungsanspruch der gegenwärtigen Rationalisierungswelle darf jedenfalls nicht zu der Annahme führen, jedes Digitalisierungsprojekt sei hilfreich und gut. Technische Innovationen können sich als Fehlschläge erweisen oder werden nur betrieben bzw. fortgesetzt, weil die Fördermittel fließen oder ein Scheitern nicht eingestanden werden kann. Die Förderung des Zwecks muss durch Fakten belegbar sein.

Selbstverständlich muss neue Technik, deren Wirksamkeit noch unklar ist, praktisch erprobt werden, gerade wenn damit personenbezogene Daten erfasst werden. Der *Erprobungszweck* ist ein eigener Zweck, der personenbezogene Datenverarbeitung in spezifischer Weise rechtfertigen kann. Die Erprobung darf aber nicht auf Dauer gestellt werden. Können nach einem angemessenen Zeitraum keine positiven Erprobungsergebnisse festgestellt werden, so ist der Erprobungszweck verbraucht und eine Eignung für den Einsatzzweck hat sich nicht ergeben.

Erforderlichkeit als Gebot des mildesten Mittels

In der Fachliteratur wird gelegentlich betont, dass mit dem Begriff der Erforderlichkeit in § 26 Abs. 1 Satz 1 BDSG keine absolute Erforderlichkeit gemeint sein kann.[199] Selbstverständlich kann es an dieser Stelle nicht darum gehen, ob die Datenverarbeitung unverzichtbar für die Durchführung des Arbeitsverhältnisses generell ist.[200] Auch ein konkret benannter Zweck (s. o.) soll hier nicht erneut unter dem Gesichtspunkt seiner Erforderlichkeit in Frage gestellt werden. Die Frage ist nur noch, ob die vorgesehene oder bereits betriebene Maßnahme der Datenverarbeitung in der gewählten Ausgestaltung erforderlich ist oder durch eine weniger in die Rechte der Beschäftigten auf Privatsphäre bzw. informationelle Selbstbestimmung eingreifende Maßnahme ersetzt werden könnte.

Die Maßnahme der Datenverarbeitung muss dabei das *mildeste aller gleich effektiven* zur Verfügung stehenden Mittel darstellen.[201] Soweit reicht die herrschende Meinung, die kaum weiter differenziert.

Zur Verdeutlichung: Die Datenverarbeitung ist demnach erforderlich, auch wenn durch Einsatz einer anderen zweckdienlichen, aber *weniger effektiven* Technologie wesentlich weniger personenbezogene Daten erfasst werden müssten. Die Datenverarbeitung ist dagegen nicht erforderlich, wenn eine Datenminimierung möglich ist, ohne die Zweckerreichung zu beeinträchtigen.

[199] *Kort*, RdA 2018, 242 (246).
[200] *Hornung/Hofmann*, in: Hirsch-Kreinsen/Ittermann/Niehaus (Hrsg.), Digitalisierung industrieller Arbeit, 2. Aufl., 2018, S. 233 (240); ähnlich *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, Rn. 150.
[201] Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, BDSG § 26 Rn. 19; ähnlich Auernhammer/*Forst*, 7. Aufl., 2020, BDSG § 26 Rn. 64; ErfK/*Franzen*, 20. Aufl., 2020, BDSG § 26 Rn. 10; *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, Rn. 147; Taeger/Gabel/*Zöll*, 3. Aufl., 2019, BDSG § 26 Rn. 25.

Zur eingehenderen Erörterung besteht aber durchaus Anlass. Denn diese eigentümliche Logik könnte durchaus mit dem Datenminimierungsgrundsatz aus Art. 5 Abs. 1 lit c) DSGVO in Widerspruch stehen, auf den u. a. auch § 26 Abs. 5 BDSG eindeutig verweist. Denn das Datenminimierungskonzept der DSGVO kennt keinen Vorbehalt, dass die Effektivität der Systeme nicht angetastet werden darf.

Ein *zumutbarer Zusatzaufwand* oder zumutbare Zusatzkosten werden jedenfalls hinzunehmen sein, um eine deutlich schonendere Datenverarbeitung als milderes Mittel anzuerkennen. Denn Zusatzaufwand oder Zusatzkosten als solche beeinträchtigen die Zweckerreichung in vielen Fällen nicht, solange sie nicht vernünftige Grenzen sprengen. Ist etwa die Steigerung des Gesundheitsschutzes Zweck einer Maßnahme, ist die Zweckerreichung allein durch die höheren Kosten eines nach Privacy-by-Design-Gesichtspunkten konstruierten datenschonenderen Systems nicht beeinträchtigt. Ist hingegen die Kostensenkung durch Digitalisierung selbst der Zweck, könnte eingewendet werden, kann das kostspieligere System in der Regel nicht die gleiche Kostenersparnis realisieren. Kostensenkung ist ein legitimer Zweck und digitale Technik ist hierzu vielfach durchaus geeignet. Allerdings hat jede Technik ihren technischen Zweck neben dem möglichen Ziel der Kostensenkung. Auf diesen technischen Zweck ist bei der Klärung der Frage abzustellen, ob das mildere Mittel in gleicher Weise für die Zweckerreichung geeignet ist. Sonst könnten datenschutzfreundliche Verfahren und Technologien, die mit einem Zusatzaufwand verbunden sind, schlicht mit dem Hinweis auf den Zweck der Kostensenkung als milderes Mittel abgelehnt werden. Allerdings wird nicht jeder beliebige Finanzaufwand gefordert werden können. Es geht um realistische und praktikable mildere Mittel. Insofern wäre die Grenze der „Zumutbarkeit“ [202] das passende Instrument, Maßnahmen zu völlig unverhältnismäßigen Kosten auszugrenzen.

Hier jedenfalls liegen noch Unschärfen in der Interpretation, deren weitere Klärung von Belang für die Wirksamkeit des Rechts sein wird.

Interessenabwägung

Im dritten Schritt hat dann eine Interessenabwägung stattzufinden. Ein wenig Orientierung bietet der Gesetzentwurf zum BDSG in BT-Drs. 18/11325, S. 97, wonach im Rahmen der Prüfung der Erforderlichkeit die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwägen seien. Die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten seien zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt. Offensichtlich knüpft dies an Art. 88 Abs. 2 DSGVO an, wonach die nationalen Vorschriften geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person zu umfassen haben.

Angeknüpft wird auch an die Rechtsprechung des BAG zur Vorgängerregelung in § 32 BDSG a. F. Dort hieß es zuletzt, dass die Verhältnismäßigkeit im engeren Sinne (Angemessenheit) gewahrt sei, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehe. Die Datenverarbeitung und -nutzung dürfe keine übermäßige Belastung für die Betroffenen darstellen und muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen.[203]

[202] Zur Zumutbarkeit Taeger/Gabel/*Taeger*, 3. Aufl., 2019, DSGVO Art. 6 Rn. 112; Zumutbarkeit des milderen Mittels verlangt auch Gola/Heckmann/*Gola*, 13. Aufl., 2019, BDSG § 26 Rn. 16.
[203] Fast gleichlautend BAG v. 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327 Rn. 30; BAG v. 23.8.2018 – 2 AZR 133/18, NZA 2018, 1329 Rn. 24.

Grundsätzlich können hier *alle Umstände des Einzelfalls* erneut auf den Tisch kommen. Sogar die Zwecksetzung des Arbeitgebers kann u. U. unter dem Gesichtspunkt relativ geringer Relevanz des jeweiligen Zwecks für die Durchführung des Arbeitsverhältnisses in Frage gestellt werden.

Entscheidender Ausgangspunkt ist allerdings, dass eine gewisse „Schwere des Eingriffs" in die Persönlichkeitsrechte der Beschäftigten festgestellt wird.[204] Fehlt es daran, überwiegen in aller Regel die Belange auf Arbeitgeberseite. Darauf, was die Schwere eines solchen Eingriffs ausmacht, finden sich unterschiedliche Hinweise in Literatur und Rechtsprechung.

Zunächst gilt, dass die Menge der erfassten personenbezogenen Daten sowie die Dauer und Intensität der Datenverarbeitung eine Rolle spielen.[205] Kurze Speicherfristen, schnelle Anonymisierung oder wenigstens Pseudonymisierung sprechen für einen weniger schweren Eingriff bzw. ihr Fehlen indiziert die erhebliche Eingriffsschwere. Dann ist die Art der Daten von Bedeutung. Daten aus der Privatsphäre dürfen nur ausnahmsweise und solche aus der Intimsphäre der Arbeitnehmer in aller Regel nicht genutzt werden.[206] Das Zusammenführen von Daten zur selben Person kann ebenso die Schwere des Eingriffs belegen wie der Tiefgang der Datenanalyse, insbesondere wenn das Ergebnis der Analyse weitere personenbezogene Daten sind. So sieht das BAG die Gefahr besonders intensiver Persönlichkeitsverletzungen bei digitaler Überwachungstechnik, die weitergehende Auswertungen bis hin zur Profilerstellung erlaubt.[207]

Für Videoüberwachungsmaßnahmen im Betrieb äußerte das BAG[208] schon 2004 grundlegend, dass bedeutsam sei, wie viele Personen wie intensiven Beeinträchtigungen ausgesetzt seien und ob diese Personen hierfür einen Anlass gegeben hätten. Das Gewicht der Beeinträchtigung hänge auch davon ab, ob die Betroffenen als Personen anonym blieben, welche Umstände und Inhalte der Kommunikation erfasst werden könnten und welche Nachteile den Grundrechtsträgern aus der Überwachungsmaßnahme drohten oder von ihnen nicht ohne Grund befürchtet würden.

Insbesondere bei Überwachungsmaßnahmen ist auch das Maß an Transparenz bedeutsam. Mangelnde Transparenz verstärkt den Eingriff.[209] Heimliche Maßnahmen sind zur Leistungsbeurteilung nicht, zur Aufdeckung von Fehlverhalten nur bei konkretem Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zulasten des Arbeitgebers zulässig.[210] Verschiedentlich dient der Begriff der *„Totalüberwachung"*[211] oder „Komplettüberwachung"[212] dazu, um eine besondere Schwere des Eingriffs zu kennzeichnen, die demnach generell unzulässig sei.

Besonders bemerkenswert ist hier erneut die Entscheidung des BAG vom 25.4.2017.[213] Es stelle, so der dritte Leitsatz, einen schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht der betroffenen Arbeitnehmer dar, wenn ohne zeitliche Begrenzung sämtliche Arbeitsschritte ihrer wesentlichen Arbeitsleistung durch eine technische Überwachungseinrichtung erfasst, gespeichert und einer Auswertung nach quantitativen Kennzahlen zugeführt würden. Der Entscheidung

[204] Gola/Heckmann/*Gola*, 13. Aufl., 2019, BDSG § 26 Rn. 70; Schaub/*Link*, 18. Aufl., 2019, § 153 Rn. 8; Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, DS-GVO Art. 88 Rn. 67
[205] Taeger/Gabel/*Zöll*, 3. Aufl., 2019, BDSG § 26 Rn. 25.
[206] Taeger/Gabel/*Zöll*, 3. Aufl., 2019, BDSG § 26 Rn. 25; auch *Chandna-Hoppe*, NZA 2018, 614 (617).
[207] BAG v. 29.6.2004 – 1 ABR 21/03, NZA 2004, 1278 (1284).
[208] BAG v. 29.6.2004 – 1 ABR 21/03, NZA 2004, 1278 (1281).
[209] BAG v. 25.4.2017 – 1 ABR 46/15, NZA 2017, 1205 Rn. 33 f.; BAG v. 29.6.2004 – 1 ABR 21/03, NZA 2004, 1278 (1281) unter II.1.
[210] BAG v. 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327 Rn. 27.
[211] *Kor*t, NZA 2018, 1097 (1100); *Kort*, RdA 2018, 24 (25); Taeger/Gabel/*Zöll*, 3. Aufl., 2019, BDSG § 26 Rn. 25.
[212] *Chandna-Hoppe*, NZA 2018, 614 (618) mit Blick auf die Keylogger-Entscheidung des BAG v. 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327 Rn. 33.
[213] BAG v. 25.4.2017 – 1 ABR 46/15, NZA 2017, 1205.

lag ein Fall zugrunde, bei dem das Arbeitsverhalten und die Arbeitsleistung des einzelnen Sachbearbeiters durch die Kennzahlen einer digitalen Belastungsstatistik einer detaillierten quantitativen Beobachtung unterliegt, die am Ende jeder Arbeitswoche anhand der zu erstellenden 1-Wochen-, 4-Wochen- und 26-Wochen-Sichten stets eine erneute – mit den Ergebnissen der Gruppe vergleichende – Auswertung erfährt.[214] Dadurch, so das BAG, stehe der Sachbearbeiter unter ständiger Beobachtung. Dies erzeuge einen schwerwiegenden und zudem dauerhaften Anpassungsdruck, möglichst in allen maßgebenden Arbeitsbereichen in Bezug auf die Kennzahlen unauffällig zu arbeiten, um nicht aufgrund „erheblicher Abweichungen" später Personalgesprächen oder gar personellen Maßnahmen ausgesetzt zu sein.

Auch schon unterhalb der Schwelle der Totalüberwachung sieht es das BAG als unzulässig an, durch Überwachungsmaßnahmen einen solchen psychischen Anpassungsdruck zu erzeugen, dass die Betroffenen bei objektiver Betrachtung in ihrer Freiheit, ihr Handeln aus eigener Selbstbestimmung zu planen und zu gestalten, wesentlich gehemmt seien.[215] So betrachtet das BAG[216] auch eine nur zeitweise aktive Videoüberwachung als unzulässig, die dazu führt, dass sich die Beschäftigten bei jeder ihrer Bewegungen kontrolliert fühlen müssten. Ihre Gestik und Mimik, bewusste oder unbewusste Gebärden, der Gesichtsausdruck bei der Arbeit oder bei der Kommunikation mit Vorgesetzten und Kollegen unterlägen stets der Möglichkeit dokumentierender Beobachtung. Damit entstehe, so das BAG, ein Druck, sich möglichst unauffällig zu benehmen, setzten sich doch die Arbeitnehmer andernfalls der Gefahr aus, später wegen etwa abweichender Verhaltensweisen Gegenstand von Kritik, Spott oder gar Sanktionen zu werden.

Der psychische Druck, der durch eine Überwachungsmaßnahme ausgeübt wird, ist jedenfalls ein wichtiges Kriterium des Datenschutzes, das zudem auch den Arbeits- und Gesundheitsschutz sehr interessieren dürfte.

Bei der Abwägung ist schließlich die Gesamtsituation der unterschiedlichen Systeme, die im Betrieb zusammenwirken, im Blick zu behalten. Die „Schwere des Eingriffs" kann auch dadurch erreicht werden, dass verschiedene Systeme, die einzeln tolerabel wären, zusammen ein problematisches Ausmaß an Überwachungsdruck erzeugen. Dies dürfte gerade unter den Bedingungen von Arbeit 4.0 eine große Rolle spielen, wenn dem Paradigma gefolgt wird, alle betrieblichen Systeme und Funktionen zu digitalisieren.

Auch bei einem schweren Eingriff in die Persönlichkeitsrechte der Beschäftigte ist allerdings ein Überwiegen der Belange des Arbeitgebers nicht ausgeschlossen. Dabei wird künftig eine große Rolle spielen, dass es gerade Kern der aktuellen Rationalisierungswelle von Industrie 4.0 bis KI sei, die Funktionsdaten aller Systeme und Funktionen im Unternehmen durch intelligente Auswertung ständig zu optimieren. Schwere Eingriffe werden unter diesen Bedingungen nicht mehr die Ausnahme sein, sondern übliche Begleiterscheinung der allseits angestrebten und gebilligten zukunftsträchtigen Prozesse.

Ein in diesem Zusammenhang wohl zunehmend wichtiges Kriterium wird durch die Erwägungsgründe der DSGVO in die Debatte gebracht. Zu berücksichtigen sind demnach bei der Interessenabwägung insbesondere die vernünftige Erwartungshaltung der betroffenen Person (reasonable expectations) bzw. die Absehbarkeit (Branchenüblichkeit) der Verarbeitung[217] (vgl. ErwG 47). Es besteht die Möglichkeit, dass damit die Üblichkeit der datenintensiven Digitalisierungsprozesse

[214] BAG v. 25.4.2017 – 1 ABR 46/15, NZA 2017, 1205 Rn. 32.
[215] BAG v. 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327 Rn. 31.
[216] BAG v. 29.6.2004 – 1 ABR 21/03, NZA 2004, 1278 (1281).
[217] BeckOK DatenschutzR/*Albers/Veit*, 33. Ed. 1.5.2020, DS-GVO Art. 6 Rn. 53; Gola/*Schulz*, 2. Aufl., 2018, DS-GVO Art. 6 Rn. 61.

zum Argument wird. Was an allen Arbeitsplätzen geschieht, kann demnach nicht mehr überraschen und entspricht damit vernünftigen Erwartungen.

Für die künftige Entwicklung ist die Interessenabwägung sicherlich eine zentrale Stellschraube. Die damit verbundene Ungewissheit kann zweifellos mit starken Gründen kritisiert werden (siehe Kap. 4). Das BAG handhabt sie bisher allerdings souverän im Sinne eines durchaus wirksamen Schutzes. Eine reichhaltige gefestigte Judikatur ist gesetzgeberischen Eingriffen, die zwangsläufig neue Unsicherheit erzeugen, wohl vorzuziehen. Außerdem kann Ungewissheit rechtlicher Beurteilung auch für hilfreiche Kompromissbereitschaft auf Betriebsebene sorgen.

c) Zulässigkeit der Verarbeitung sensibler Daten

Unter den erfassten personenbezogenen Daten sind häufig auch solche, die als besonders sensibel gelten. Insbesondere sind im Arbeitsverhältnis *Gesundheitsdaten* vielfach relevant. Der gesamte Bereich Arbeitsschutz befasst sich damit. Aber auch in vielen anderen Zusammenhängen geben erfasste Daten Aufschluss über den physischen oder psychischen Gesundheitszustand der Beschäftigten. In der DSGVO ist für diese „besonderen Kategorien personenbezogener Daten" in Art. 9 eine besondere Erlaubnisgrundlage mit eigenen Öffnungsklauseln für nationale Regelungen geschaffen worden. Die für das Arbeitsrecht einschlägige Öffnungsklausel in Art. 9 Abs. 2 lit. b DSGVO hat der deutsche Gesetzgeber in § 26 Abs. 3 BDSG genutzt. Damit hat er der Praxis allerdings mehr Rätsel als Lösungen an die Hand gegeben.

Klar ist zunächst, dass auch für die Verarbeitung sensibler Daten *Zwecke* des Beschäftigungsverhältnisses festzulegen sind (s.o. 3.2.1 a). Für die Zulässigkeit soll es dann aber darauf ankommen, dass die Verarbeitung zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist. Diese dem deutschen Beschäftigtendatenschutz fremde Formulierung ist der gleichlautenden Formulierung in der Öffnungsklausel der DSGVO geschuldet.

Auch hier handelt es sich um eine bedeutsame Stellschraube, denn „Verarbeitung zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht" lässt sich sehr weit und relativ eng auslegen. Die weite Auslegung würde alle Digitalisierungsmaßnahmen, die auf dem Weisungsrecht des Arbeitgebers beruhen, als „Verarbeitung zur Ausübung von Rechten" aus dem Arbeitsvertrag interpretieren. Der Wortlaut steht dem aber wohl entgegen. Denn es heißt nicht Verarbeitung infolge der Ausübung von Rechten, sondern „zur" Ausübung. Die Verarbeitung ist hier also nicht Konsequenz, sondern Bedingung der Ausübung. Damit liegt die engere Interpretation näher, dass Rechte oder Pflichten im (gesetzlichen oder tariflichen) Arbeitsrecht bestehen müssen,[218] die ohne eine bestimmte Datenverarbeitung nicht ausgeübt bzw. erfüllt werden können.

Für einen eindeutigen Fall der Erfüllung von Pflichten ist der Beschluss des BAG vom 9.4.2019 beispielhaft, in dem es um die Informationspflicht des Arbeitgebers gegenüber dem Betriebsrat nach § 80 Abs. 2 Satz 1 BetrVG geht. Hat der Betriebsrat, so das BAG[219], nach § 80 Abs. 2 Satz 1 BetrVG einen Anspruch darauf, dass ihm die Arbeitgeberin nach einer Anzeige i. S. d. § 15 Abs. 1 MuSchG den Namen der schwangeren Arbeitnehmerin mitteilt, ist die damit

[218] So auch Däubler et al./*Däubler/Wedde*, 2. Aufl., 2020, BDSG § 26 Rn. 240.
[219] BAG v. 9.4.2019 – 1 ABR 51/17, NZA 2019, 1055 (1059) Rn. 38.

verbundene Datenverarbeitung i. S. v. § 26 Abs. 3 Satz 1 BDSG zur Erfüllung einer rechtlichen Pflicht aus dem Arbeitsrecht erforderlich.

In der Fachliteratur werden *gegensätzliche Interpretationen* favorisiert. Im DSK-Kurzpapier Nr. 17 heißt es, dass solche Verarbeitungen jedoch nur dann stattfinden dürfen, wenn sie nach einer Rechtsvorschrift erforderlich sind. Davon umfasst seien auch Kollektivvereinbarungen wie Betriebsvereinbarungen.[220] Eine Verpflichtung aus dem Arbeitsvertrag reiche nicht.[221] Vielmehr soll der verschärften Schutz bei der Verarbeitung sensibler Daten gerade in der Bindung an spezifische arbeitsrechtliche Regelungen bestehen.[222] Andere Stimmen lassen rechtliche Pflichten aus dem Arbeitsvertrag als Erlaubnisgrundlage ausreichen.[223] Nach dieser Ansicht würde es reichen, eine bestimmte Pflicht in den Arbeitsvertrag zu schreiben, die eine Verarbeitung sensibler Daten erfordert, oder gar die allgemeine arbeitsvertragliche Arbeitspflicht durch Weisung entsprechend zu konkretisieren, um eine Verarbeitung sensibler Daten zuzulassen. Mit dem Grundgedanken, dass sensible Daten im Vergleich verschärft zu schützen sind, wäre dies jedoch nicht mehr zu vereinbaren.

Neben der Verhältnismäßigkeitsprüfung im Rahmen der Erforderlichkeit darf wie bisher nach § 28 Absatz 6 BDSG a. F. kein Grund zu der Annahme bestehen, dass die schutzwürdigen Interessen der Betroffenen die Interessen der Verantwortlichen an der Verarbeitung überwiegen, heißt es im Gesetzentwurf.[224] Teilweise wird dies für eine überflüssige Dopplung,[225] teilweise für eine Verschärfung des Erforderlichkeitsmaßstabs gehalten.[226] Letztlich kann dieser Streit dahinstehen, solange bei der Interessenabwägung die Verarbeitung sensibler Daten bei der Beurteilung der „Schwere des Eingriffs“ besonderes Gewicht bekommt.

Ohnehin ist bei klaren gesetzlichen Pflichten, bestimmte personenbezogene Informationen zu erheben und zu verarbeiten, für eine Interessenabwägung kein Raum. Allerdings gibt es fast überall kleine oder große Spielräume, in denen die Pflicht nach Abwägung auf die eine oder die andere Art zu erfüllen ist.

Schließlich ist der Verweis auf § 22 Abs. 2 BDSG von Bedeutung. Damit wird der Gesetzgeber Art. 9 Abs. 2 lit. b DSGVO gerecht, wonach die nationale Regelung geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen muss. Bei der Verarbeitung sensibler Daten sind zusätzlich vielfältige technische und organisatorische Schutzmaßnahmen aus dem in § 22 Abs. 2 BDSG genannten Katalog zu ergreifen.

Für den Arbeitsschutz und für das Personalmanagement ist gerade der letzte Punkt von größter Bedeutung. Da hier sensible Daten ständig bzw. oft verarbeitet werden, sind die Maßnahmen nach § 22 Abs. 2 BDSG hier unverzichtbarer Standard.

Zusammenfassend betrachtet bedarf § 26 Abs. 3 BDSG dringend einer Klärung. Das könnte auch die Rechtsprechung leisten. Doch im Interesse eines Mindestmaßes an Verständlichkeit des geschriebenen Rechts scheint hier doch der *Gesetzgeber zum Handeln aufgerufen*.

[220] Datenschutzkonferenz, DSK-Kurzpapier Nr. 17, Besondere Kategorien personenbezogener Daten, S. 1 f.
[221] Gola/*Pötters*, 2. Aufl., 2018, DS-GVO Art. 88 Rn. 94.
[222] Gola/*Pötters*, 2. Aufl., 2018, DS-GVO Art. 88 Rn. 95.
[223] *Piltz*, BDSG, § 26 Rn. 84; Gola/Heckmann/*Gola*, 13. Aufl., 2019, BDSG § 26 Rn. 147.
[224] BT-Drs. 18/11325, 98.
[225] Gola/*Pötters*, 2. Aufl., 2018, DS-GVO Art. 88 Rn. 93; in der Tendenz auch Auernhammer/*Forst*, 7. Aufl., 2020, BDSG § 26 Rn. 84.
[226] Taeger/Gabel/*Zöll*, 3. Aufl., 2019, BDSG § 26 Rn. 84; BeckOK DatenschutzR/*Riesenhuber*, 33. Ed. 1.8.2020, BDSG § 26 Rn. 65.

3.2.2 ZULÄSSIGKEIT ZUR ENTSCHEIDUNG ÜBER DIE BEGRÜNDUNG DES BESCHÄFTIGUNGSVERHÄLTNISSES

Bewerber*innen für ein Beschäftigungsverhältnis gelten als Beschäftigte. Das wird in § 26 Abs. 8 Satz 2 BDSG ausdrücklich für den Beschäftigtendatenschutz angeordnet. Dennoch unterscheidet sich das Thema Datenschutz im Bewerbungsverfahren deutlich vom sonstigen Beschäftigtendatenschutz. Das hat vor allem damit zu tun, dass der einstellende Arbeitgeber ein enormes personenbezogenes Informationsbedürfnis hat. Das gilt unter Bedingungen des Fachkräftemangels nicht weniger als bei hohem Bewerber*innenandrang. Es ist im Übrigen ein sehr altes Thema, das im Arbeitsrecht bereits bestand, als von Beschäftigtendatenschutz noch keine Rede war.[227] Denn die Auskunft über das Bestehen einer Schwangerschaft oder die Auskunft über die Mitgliedschaft in einer Gewerkschaft im Bewerbungsverfahren war schon immer von potenziell hoher Brisanz. Es stoßen hier also sehr alte arbeitsrechtliche Grundsätze auf modernen Datenschutz, um sich aktuell mit den Anforderungen des E-Recruiting auseinanderzusetzen.

Laut § 26 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Bewerbers nur dann erhoben und ausgewertet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Es soll nicht darum gehen, dass die Daten für den Arbeitgeber unverzichtbar sind.[228] Das traditionelle Szenario eines Bewerbungsgesprächs vor Augen, in dem Bewerber*innen mit diversen Fragen des personalsuchenden Arbeitgebers konfrontiert werden, heißt es in der Fachliteratur, dass das Fragerecht des Arbeitsgebers auf Fragen beschränkt sei, an deren Beantwortung der Arbeitgeber ein berechtigtes, billigenswertes und schutzwürdiges Interesse hat,[229] das so stark ist, dass das Interesse des Arbeitnehmers dahinter zurücktritt.[230] Überschreite der Arbeitgeber die Grenzen des Fragerechts, habe der Arbeitnehmer nicht nur ein „Recht zu lügen“; die so gewonnenen Daten dürften auch nicht weiter verwertet werden.[231]

Mit diesen traditionellen Maßstäben wird auch versucht, die Zulässigkeit aktueller Techniken des E-Recruiting zu überprüfen. Auch Background-Checks oder Pre-Employment-Screenings werden, grundsätzlich an den Maßstäben des Fragerechts gemessen.[232] Psychologische Testverfahren (z. B. in Form der Analyse von Bewerber*innenvideos) sind demnach nur zulässig, wenn es tatsächlich um eine Stelle geht, die hohe psychische Zuverlässigkeit verlangt (Beispiel Pilot*in).[233] Dagegen wären psychologische Sprachanalysen, die darauf gerichtet sind, die kontaktfreudigste Person für Verkaufstätigkeiten zu ermitteln, wohl unzulässig. Auf jeden Fall hängt die Zulässigkeit davon ab, dass die Kandidat*innen zuvor über die Art der Analyse informiert wird. Das hat das BAG schon für graphologische Gutachten 1982 entschieden.[234] Für die aktuelle datenschutzrechtliche Bewertung gilt nichts anderes, denn nach § 26 Abs. 1 BDSG würde eine heimliche Analyse spätestens an der Voraussetzung der Erforderlichkeit scheitern.

Umstritten ist, welche Rolle eine informierte Einwilligung für die Zulässigkeit der verschiedenen psychologischen Analyseverfahren spielen kann.[235] Laut ErwG 42 DSGVO kommt es darauf an, ob

[227] *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, Rn. 559.
[228] *Piltz*, BDSG, § 26 Rn. 37.
[229] Anknüpfend an die st. Rspr. des BAG, z. B. schon v. 20.02.1986 - 2 AZR 244/85, NZA 1986, 739.
[230] Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, BDSG § 26, Rn. 29; ähnlich Auernhammer/*Forst*, 7. Aufl., 2020, BDSG § 26 Rn. 129; *Piltz*, BDSG, § 26 Rn. 38; Taeger/Gabel/*Zöll*, 3. Aufl., 2019, BDSG § 26 Rn. 30.
[231] ErfK/*Franzen*, 20. Aufl., 2020, BDSG § 26 Rn. 12.
[232] Taeger/Gabel/*Zöll*, 3. Aufl., 2019, BDSG § 26 Rn. 31; *Gola*, Das Internet als Quelle von Bewerberdaten, NZA 2019, 654 (655).
[233] *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, Rn. 697.
[234] BAG v. 16.9.1982 – 2 AZR 228/80, NJW 1984, 446
[235] Pro Zulässigkeit per Einwilligung *Stück*, ArbRAktuell 2020, 153 (154); contra *Joos*, NZA 2020, 1216 (1217).

Bewerber*innen eine echte oder freie Wahl haben und somit in der Lage sind, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Der Nachteil ist hier sehr offensichtlich, dass bei Ablehnung der Analyse die Aussichten der Bewerbung regelmäßig dramatisch sinken. Überwiegend wird daher vertreten, dass die Zulässigkeit ansonsten unzulässiger Analyseverfahren nicht per Einwilligung herbeigeführt werden könne.[236]

Scheidet die Einwilligung als Erlaubnisgrundlage aus, kommt es auf die Erforderlichkeit des jeweiligen Analyseverfahrens für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses gemäß § 26 Abs. Satz 1 BDSG an. In der Fachliteratur wird auf der Suche nach einem milderen Mittel z. B. darüber gestritten, ob automatisierte Sprachanalysen tiefer in Persönlichkeitsrechte eingreifen als etwa ein klassisches Assessment-Center.[237] Bei einem hohen Bewerbungsaufkommen könnte die Erforderlichkeit einer automatisierten Vorauswahl per KI daraus gezogen werden, dass sonst der Ansturm nicht zu bewältigen ist.[238]

Die Diskussion ist eindeutig noch nicht abgeschlossen. Ein klärendes Wort der Rechtsprechung ist absehbar nicht zu erwarten. Das Personalmanagement bräuchte aber angesichts der Vielzahl an technischen Errungenschaften der Bewerber*innenauswahl (siehe Kap. 1.2) dringend Orientierungspunkte. Auch Bewerber*innen haben angesichts der unübersichtlichen Rechtslage kaum die Chance ihre Rechte zu beurteilen.

3.2.3 ZULÄSSIGKEIT NACH EINWILLIGUNG

Zu den wenigen substanziellen Neuerungen, die der Gesetzgeber 2018 in § 26 BDSG verankert hat, gehören die Regelungen zur Zulässigkeit der Datenverarbeitung wegen einer Einwilligung des betroffenen Beschäftigten in § 26 Abs. 2 und 3 Satz 2 BDSG. Entscheidende Merkmal für eine wirksame Einwilligung in die Datenverarbeitung sind nach der Begriffsdefinition in Art. 4 Ziff. 11 DSGVO die Freiwilligkeit, die Bestimmtheit und die Informiertheit der Erklärung bzw. des Erklärenden. Was unter Freiwilligkeit zu verstehen ist, wird in ErwG 42 DSGVO erläutert. Danach sollte nur dann davon ausgegangen werden, dass die betroffene Person ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Ob Arbeitnehmer*innen im Arbeitsverhältnis angesichts der regelmäßig vorliegenden Abhängigkeit vom Arbeitgeber tatsächlich in freier Entscheidung ihre Einwilligung zu dessen Datenverarbeitung erteilen können, war lange heftig umstritten.[239] In einem auf Dauer angelegten Vertragsverhältnis, in dem eine Seite u. a. Weisungsbefugnisse hat, ist die Verweigerung einer Einwilligung in die Pläne der weisungsbefugten Seite, immer problematisch. Andererseits ist die völlige Bevormundung der Beschäftigtenseite durch das Recht, insbesondere wenn es um informationelle *Selbstbestimmung* geht, auch ein Problem.

Mit § 26 Abs. 2 BDSG ist nunmehr seitens des Gesetzgebers geklärt worden, dass auch im Arbeitsverhältnis Freiwilligkeit vorliegen kann. In Satz 2 wird festgelegt, dass eine freiwillige Einwilligung insbesondere vorliegen kann, wenn durch die Datenverarbeitung für die beschäftigte Person ein

[236] *Gola*, Handbuch Beschäftigtendatenschutz, 8. Aufl., 2019, Rn. 554; *Joos*, NZA 2020, 1216 (1217); *Kort*, NZA-Beilage 2016, 62 (67).
[237] *Betz*, ZD 2019, 148 (149); *Joos*, NZA 2020, 1216 (1220).
[238] Bei „zehntausenden Bewerbungen" laut Art. 29 Datenschutzgruppe 17/DE WP251rev 01 „Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679", 26.
[239] Einzelheiten bei *Däubler*, Gläserne Belegschaften, 8. Aufl., 2019, Rn. 150 ff.; Taeger/Gabel/*Taeger*, 3. Aufl., 2019, DSGVO Art. 7 Rn. 96 ff.; *Taeger/Rose*, BB 2016, 819, 822 f.

rechtlicher oder wirtschaftlicher Vorteil erlangt wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

Auch dies ist eine nicht unbedeutende Stellschraube für die Wirksamkeit des Datenschutzrechts in der Arbeit 4.0. Denn die Gefahr, dass alle gesetzlichen Grenzen der personenbezogenen Datenverarbeitung im Betrieb durch exzessive Einwilligungsstrategien unterlaufen werden, steht durchaus im Raum.

Das neu geschaffene Recht macht solche Strategien für die Unternehmen jedoch wenig attraktiv. Eine pauschale Einwilligung, z. B. gleich zu Beginn im Arbeitsvertrag, kann nicht eingeholt werden. Der Bestimmtheitsgrundsatz erfordert, dass jede Erweiterung der Erhebung oder Veränderung der Verarbeitung der Daten einer neuen Einwilligung bedarf. Einwilligungen können ganz oder teilweise erfolgen, sie können ganz oder teilweise widerrufen werden. Es droht dadurch ein sehr uneinheitlicher Rechtszustand im Betrieb. Schließlich sind auch die inhaltlichen Grenzen der Wirksamkeit in § 26 Abs. 2 BDSG recht eng.

Die Datenschutzkonferenz geht in ihrem Kurzpapier Nr. 14 davon aus,[240] dass die Einwilligung in der Praxis überwiegend in Konstellationen möglich sein wird, die nicht das Arbeitsverhältnis als solches, sondern Zusatzleistungen des Arbeitgebers betreffen (wie z. B. bei der Gestattung privater Nutzung dienstlicher Fahrzeuge, Telefone und EDV-Geräte; Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung; Aufnahme in Geburtstagslisten).

Bei der Datenverarbeitung für Zwecke des Arbeitsschutzes liegt es nicht fern, gleichgelagerte Interessen anzunehmen.[241] Sicherheit und Gesundheitsschutz sind in der Tat grundsätzlich gemeinsame Interessen der Arbeitsvertragspartner. Das gilt aber nicht für jede einzelne Arbeitsschutzmaßnahme, die mit der Verarbeitung von Beschäftigtendaten verbunden ist. Wird etwa unternehmensweit eine neue Technologie eingeführt, die bestimmte datenintensive Arbeitsschutzmaßnahmen erforderlich macht, so steht der einzelne Beschäftigte in der Regel so stark unter Druck einzuwilligen, dass von Freiwilligkeit keine Rede mehr sein kann. Etwas anderes mag es sein, wenn Freiwillige gesucht werden, um ein neues Assistenzsystem auszuprobieren.

Wo Betriebs- bzw. Personalräte installiert sind, kann die Einwilligung ohnehin kaum eine Rolle spielen, da sowohl im Arbeitsschutz als auch im Datenschutz Mitbestimmungsrechte zu beachten sind, die nicht durch individuelle Einwilligungen unterlaufen werden dürfen. Denkbar ist aber, dass in Betriebs- oder Dienstvereinbarungen geregelt wird, dass zusätzlich zur kollektivrechtlichen Erlaubnis für bestimmte Verarbeitungen eine individuelle Einwilligung einzuholen ist, um die persönliche Entscheidungsfreiheit zu wahren.

Alles in allem gehört damit das Recht der Einwilligung im Beschäftigungsverhältnis, das in § 26 Abs. 2 BDSG bereits neu geregelt ist, nicht zu den ungeklärten Problembereichen des Beschäftigtendatenschutzes.

[240] Datenschutzkonferenz, DSK-Kurzpapier Nr. 14, Beschäftigtendatenschutz, S. 2.
[241] *Martini/Botta*, NZA 2018, 625, 629.

3.2.4 ZULÄSSIGKEIT AUF GRUNDLAGE EINES KOLLEKTIVVERTRAGS

Gemäß § 26 Abs. 4 Satz 1 BDSG ist die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, auf der Grundlage von Kollektivvereinbarungen zulässig. Die Vorschrift hat lediglich klarstellende Funktion,[242] da die Möglichkeit bereits durch Art. 88 Abs. 1 Satz 1 DSGVO eingeräumt worden ist.

Die in diesem Zusammenhang zentrale Stellschraube betrifft die Frage, ob Kollektivvereinbarungen dazu eingesetzt werden können, das Datenschutzrecht zu entschärfen, um die aktuell angestrebte umfassende Datenverarbeitung im Betrieb zu erleichtern.

In der Literatur gibt es ein sehr uneinheitliches Meinungsspektrum. Teilweise wird ein „weiter Regelungsspielraum"[243] konstatiert, der es erlaubt, in der Kollektivvereinbarung von den Vorgaben der DSGVO nicht nur „nach oben", sondern auch „nach unten" abzuweichen.[244] Teilweise wird das glatte Gegenteil vertreten[245] (heißt: weder „nach oben" noch „nach unten") oder jedenfalls eine „Reduzierung des gesetzlichen Datenschutzstandards" als unzulässig[246] angesehen. Teilweise werden die Vorgaben der Verordnung als Mindestbedingungen für den Beschäftigtendatenschutz auch in Betriebsvereinbarungen angesehen.[247]

Der Streit ist recht alt und verhärtet und möglicherweise wenig relevant. Denn der Spielraum „nach unten" ist bei den Erlaubnistatbeständen auch für die Tarif- oder Betriebsparteien begrenzt. Die Tarifvertragsparteien sind an die informationelle Selbstbestimmung aus Art. 1 Abs. 1 und 2 Abs. 1 GG und die Betriebsvereinbarungsparteien an das Gebot, die Persönlichkeit der Beschäftigten zu schützen und zu fördern gemäß § 75 Abs. 2 BetrVG gebunden. Einzuhalten sind außerdem die Vorgaben des Art 88 Abs. 1 BDSG, wozu v. a. die in Abs. 2 genannten Anforderungen gehören. Festzulegen sind demnach geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe und die Überwachungssysteme am Arbeitsplatz. Hinzu kommt noch die Bindung an die Grundsätze in Art. 5 DSGVO gemäß § 26 Abs. 5 BDSG.

Größer ist der Spielraum „nach oben", denn auch hier gibt es Grenzen, die aber nicht so eng gezogen sind. Angesichts der unternehmerischen Freiheit des Arbeitgebers muss die Regelung allerdings zumutbar sein.

Um zur Ausgangsfrage zurückzukommen, ist festzustellen, dass die Gefahr, dass durch Kollektivvereinbarungen Schutzstandards unterlaufen werden, *theoretisch* unter juristischen Gesichtspunkten wenig brisant ist. Ein Absenken einzelner Schutzstandards der DSGVO wäre wohl denkbar, müsste aber durch andere Schutzmaßnahmen – eben spezifischere Maßnahmen – kompensiert werden. Ganz anders könnte sich das jedoch aus *empirisch-praktischer* Blickrichtung darstellen. Denn dort, wo sich Arbeitgeber und Interessenvertretung einig sind, ist kaum damit zu rech-

[242] BT-Drs. 18/11325, S. 98.
[243] Taeger/Gabel/*Zöll*, 3. Aufl., 2019, BDSG § 26 Rn. 88.
[244] Auernhammer/*Forst*, 7. Aufl., 2020, DSGVO Art. 88 Rn. 18 f.; ähnlich BeckOK DatenschutzR/*Riesenhuber*, 33. Ed. 1.5.2020, DS-GVO Art. 88 Rn. 66 ff.
[245] Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, DS-GVO Art. 88 Rn. 40; tendenziell auch EuArbRK/*Franzen*, 3. Aufl., 2020, DS-GVO Art. 88 Rn. 10.
[246] Gola/*Pötters*, 2. Aufl., 2018, DS-GVO Art. 88 Rn. 26.
[247] *Körner*, NZA 2019, 1389 (1390).

nen, dass eine juristische Überprüfung überhaupt stattfindet. Dennoch, der gewährte Experimentierspielraum für die Tarif- und Betriebsparteien ist funktional, bedarf aber der kritischen Beobachtung.

3.2.5 TRANSPARENZREGELN DER DSGVO

In Art. 88 Abs. 2 DSGVO betont der europäische Gesetzgeber, dass spezifische nationale Vorschriften, die auf Grundlage der Öffnungsklausel für die Regelung des Beschäftigtendatenschutzes auf nationaler Ebene erlassen werden, angemessene und besondere Maßnahmen insbesondere im Hinblick auf u. a. die Transparenz der Verarbeitung zu umfassen haben. Dies ist in § 26 BDSG nicht geschehen. Es gibt nicht einmal einen Verweis auf die Transparenzregeln in Art. 12-15 DSGVO. Die wird letztlich schlicht so zu verstehen sein, dass die Art. 12-15 DSGVO „eins zu eins" auch im nationalen Beschäftigtendatenschutz gelten sollen.[248] Es bleibt insoweit bei der unmittelbaren und zwingenden Wirkung der Normen der DSGVO.[249]

Die Transparenzregeln sind ein entscheidender Punkt des Beschäftigtendatenschutzes. Denn sie sollen die Datenverarbeitung hinter dem Rücken der Betroffenen ausschließen und diesen damit überhaupt erst konkrete Handlungsmöglichkeiten zum Schutz ihrer Daten in die Hand geben.

Beschäftigte müssen klar erkennen und nachvollziehen können, ob, von wem und zu welchem Zweck ihre personenbezogenen Daten erhoben werden.[250] Zum Zeitpunkt der Erhebung muss der Arbeitgeber daher jeweils betroffene Beschäftigte mit einer Reihe von Informationen nach Art. 13 Abs. 1 und 2 DSGVO ausstatten. Werden die Daten nicht bei der betroffenen Personen selbst erhoben, kann nach Art. 14 Abs. 3 DSGVO die Information nachträglich erfolgen. Eine angemessene Frist ist einzuhalten, die bis zu einem Monat dauern kann. Bei Weiterverarbeitung zu einem anderen Zweck als ursprünglich bei der Erhebung beabsichtigt, hat die Information darüber allerdings immer vor dieser Weiterverarbeitung zu erfolgen.

Inhaltlich umfasst die Information 12 Einzelpunkte, in deren Mittelpunkt wohl vielfach Art. 13 Abs. 1 lit. c) bzw. Art. 14 Abs. 1 lit. c) DSGVO stehen dürfte, wonach über die Zwecke der Datenverarbeitung zu informieren ist. An dieser Stelle müssen die Zwecke so konkret und eindeutig genannt werden, wie sie nach Art. 5 Abs. 1 lit. b) DSGVO vom Verantwortlichen festzulegen sind. Der Arbeitgeber ist an diese benannten Zwecke gebunden. Über eine mögliche Zweckänderung ist zuvor erneut zu informieren.[251]

Wichtig könnte schließlich noch im Hinblick auf digitalisierte Beurteilungs- und Auswahlverfahren die Information gemäß Art. 13 Abs. 2 lit. f), Art. 14 Abs. 2 lit. h DSGVO sein, die über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zu erteilen ist.

[248] Auernhammer/*Forst*, 7. Aufl., 2020, DSGVO Art. 88 Rn. 31.
[249] Vorbehaltlich begrenzter zulässiger Einschränkungen gemäß §§ 32 ff. BDSG.
[250] Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, BDSG § 26 Rn. 21.
[251] Auernhammer/*Forst*, 7. Aufl., 2020, DSGVO Art. 13 Rn. 26.

Das Problem ist allerdings, dass gerade bei schneller Weiterentwicklung der Datenverarbeitung im Betrieb, wie sie in der absehbaren Phase der Digitalisierung zu erwarten ist, sehr häufig solche Informationen erforderlich werden können. Der oder die Beschäftigte wird dann möglicherweise von solchen Informationen überschüttet, ohne dass eine realistische Chance besteht, sich damit sinnvoll auseinanderzusetzen.

Immerhin können Beschäftigte unabhängig von einzelnen Mitteilungen nach den Art. 13 bzw. 14 DSGVO Auskunft vom Arbeitgeber beantragen, ob und – wenn ja – welche Datenkategorien zu welchen Zwecken auf welche Dauer zur jeweiligen Person verarbeitet werden. Hinzu kommen Auskünfte über mögliche Empfänger der Daten, u. U. ihre Herkunft und diverse Rechte, die der oder die Beschäftigte weiter geltend machen kann. Schließlich haben Beschäftigte das Recht nach Art. 15 Abs. 3 DSGVO, eine Kopie der personenbezogenen Daten zu verlangen, die Gegenstand der Verarbeitung sind.

Das sind zusammen mächtige Rechte, mit denen sich der oder die Beschäftigte einen vollständigen Überblick verschaffen kann, vorausgesetzt die erforderlichen Daten liegen vor oder sind jedenfalls ermittelbar. Dies wird durch die aktuelle Phase der Digitalisierung zunehmend in Frage gestellt. Die „Black Box" der Big Data-Analyse wird auch vom Arbeitgeber oft nicht durchschaut. Selbst der Datenanalyst wisse oft nicht, so *Holthausen*, auf welche Daten der Algorithmus gerade zugreife; selbst wenn er es wüsste, wäre die Datenmenge zu groß um alle Betroffenen zu informieren.[252]

Bei großen Datenmengen und KI-gestützter Datenverarbeitung braucht also Transparenz technische Unterstützung. Das hat zwei Seiten. Der Arbeitgeber muss selbst in der Lage sein, die Auswirkungen seiner Datenverarbeitung so zu durchschauen, dass er seine Pflichten erfüllen und Transparenz herstellen kann. Dazu braucht er die zielgerichtete Unterstützung der Entwickler bzw. Hersteller der datenverarbeitenden Technik.[253] Die Beschäftigten wiederum müssen technische Instrumente in die Hand bekommen, die eigene Betroffenheit eigenständig zu beurteilen, damit sie nicht in der Informationsflut ertrinken.

3.2.6 TECHNISCHE- UND ORGANISATORISCHE MAßNAHMEN

Ein enormer Gewinn an Datenschutz kann sich aus dem Instrumentenkasten der DSGVO an technischen und organisatorischen Verpflichtungen des Verantwortlichen ergeben, die sich in den Art. 25-39 DSGVO finden und durchweg auch im Beschäftigtendatenschutz anzuwenden sind.

Ausgangspunkt ist Art. 24 Abs. 1 DSGVO, wonach der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen *geeignete technische und organisatorische Maßnahmen* umsetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der Verordnung erfolgt.

Nach Art. 30 Abs. 1 DSGVO führt jeder Verantwortliche – hier also i. d. R. der Arbeitgeber – ein *Verzeichnis aller Verarbeitungstätigkeiten*, die seiner Zuständigkeit unterliegen. Der Inhalt wird in der Vorschrift genau aufgelistet. Ausgenommen sind nach Abs. 5 Unternehmen oder Einrichtun-

[252] *Holthausen*, RdA 2021, 19 (25).
[253] *Käde/von Maltzan*, CR 2020, 66 (69), weisen darauf hin, dass es stets der Entwickler*in überlassen sei, technische Ansätze, die den Blick in die Black Box erlaubten, zu implementieren.

gen, die weniger als 250 Mitarbeiter beschäftigen. Allerdings folgt dort sofort die Rückausnahme für u. a. die Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO. Vor diesem Hintergrund dürften Unternehmen, die tatsächlich der Ausnahme entsprechen, praktisch kaum zu finden sein. Das ist auch sinnvoll, denn das Verarbeitungsverzeichnis ist Dreh- und Angelpunkt für alles Weitere. Es informiert zunächst einmal den Arbeitgeber selbst, was eigentlich in seinem Unternehmer im Bereich der Verarbeitung personenbezogener Daten geschieht, so dass weitere Konsequenzen gezogen werden können.

Zu den weiteren Konsequenzen könnte zunächst die Bestellung eines *Datenschutzbeauftragten* gehören. Hier ist das deutsche Recht gemäß § 38 Abs. 1 BDSG im nichtöffentlichen Bereich wesentlich strenger als Art. 37 DSGVO. Eine Datenschutzbeauftragte oder ein Datenschutzbeauftragten ist bereits zu bestellen, soweit in der Regel mindesten 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Hier sind nicht nur Beschäftigtendaten gemeint, sondern z. B. auch Kundendaten. Schon in mittleren Unternehmen wird diese Grenze angesichts der zahlreichen Digitalisierungsphänomene meistens erreicht sein. Selbstverständlich aber verbleiben viele kleine und auch mittlere Unternehmen, die unterhalb der Grenze liegen. Auch hier gibt es jedoch Rückausnahmen, insbesondere für Fälle, in denen eine Datenschutz-Folgenabschätzung erforderlich ist (s. u.).

Zu den weiteren Konsequenzen könnte weiter die Pflicht zur Durchführung einer *Datenschutz-Folgenabschätzung* (DSFA) nach Art. 35 DSGVO gehören. Diese Vorschrift, die oft als wichtige Neuerung der DSGVO gefeiert wird,[254] ist für den aktuellen Digitalisierungsschub der Wirtschaft gezielt gemacht. Denn es heißt dort, dass insbesondere *bei Verwendung neuer Technologien* diese Pflicht zum Tragen kommen soll, sobald die Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Der Verantwortliche hat in diesen Fällen vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Was genau ein hohes Risiko ist, beschäftigt seither die Fachdiskussion.[255] Die Regelbeispiele in Art. 35 Abs. 3 DSGVO machen deutlich, dass – im Unterschied zum Verarbeitungsverzeichnis nach Art. 30 DSGVO – bei weitem nicht jedes Unternehmen betroffen ist und wiederholt Datenschutz-Folgenabschätzung durchzuführen hat. So muss hier als Voraussetzung z. B. eine *umfangreiche* Verarbeitung besonderer Kategorien von personenbezogenen Daten durch die jeweilige Anwendung vorliegen. Allerdings führen systematische Videoüberwachung oder nicht nur vereinzelte KI-Anwendungen im Personal- oder Arbeitsschutzbereich vielfach in die Pflicht zur Datenschutz-Folgenabschätzung.[256] Dennoch sind die Einschränkungen in Abs. 3 ein Problem, weil sie den Eindruck erwecken, die Datenschutz-Folgenabschätzung sei ein Instrument für besondere Ausnahmen und für die übliche Innovation des Betriebsalltags nicht gemacht. Die Datenschutzkonferenz hat gemäß Art. 35 Abs. 4 DSGVO eine nicht abschließende Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, veröffentlicht.[257] Die näheren Inhalte der DSFA sind in Art. 35 Abs. 7 DSGVO aufgeführt und betreffen v. a. die Bewertung der Gefahren und erforderliche Abhilfemaßnahmen. Zur Unterstützung existieren Handbücher und Software-Tools.

[254] Kritisch hierzu Auernhammer/*Raum*, 7. Aufl., 2020, DSGVO Art. 35 Rn. 3.
[255] Für Handlungsempfehlungen siehe *Ritter/Reibach/Lee*, ZD 2019, 531 (535).
[256] Näher *Holthausen*, RdA 2021, 19 (31 f.).
[257] www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf

Welche *technischen und organisatorischen Maßnahmen* der Arbeitgeber ggf. zu ergreifen hat, ergibt sich generell aus Art. 32 Abs. 1 DSGVO. Die Konkretisierung durch Verhaltensregeln der Verbände (siehe Art. 40 Abs. 2 lit. h DSGVO) wird in § 32 Abs. 3 DSGVO nahegelegt. § 26 Abs. 3 Satz 3 DSGVO verweist zudem für den Fall der Verarbeitung sensibler Daten im Beschäftigungsverhältnis auf den detaillierteren Maßnahmenkatalog nach Art. 22 Abs. 2 Satz 2 BDSG.

Art. 25 DSGVO ist schließlich besonders vielversprechend überschrieben mit „*Datenschutz durch Technikgestaltung* und durch datenschutzfreundliche Voreinstellungen", weil damit an die langjährig unter dem Stichwort „Privacy by Design" diskutierte Hoffnung angeknüpft wird, die Technik könnte von vornherein durch ihre Ausgestaltung den Datenschutz garantieren. Der Inhalt des Art. 25 Abs. 1 DSGVO fällt gegenüber der Überschrift doch recht blass aus. Denn wie schon zuvor generell in Art. 24 Abs. 1 DSGVO werden schlicht „geeignete technische und organisatorische Maßnahmen" gefordert. Der springende Punkt findet sich in der Formulierung „sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung". Hier geht es also nicht darum, eine technisch bestehende Verarbeitung durch Begleitmaßnahmen irgendwie einzuhegen. Vielmehr ist von vornherein die Technik der Verarbeitung so auszuwählen, dass Datenschutzgrundsätze wirksam umgesetzt werden. Hinzu kommt die Pflicht zu entsprechend wirksamen Voreinstellungen der gewählten Technik aus Art. 25 Abs. 2 DSGVO.

Das sind Gebote, die z. B. auf jegliche Auswahl von Überwachungstools oder KI-Tools in Personalmanagement oder Arbeitsschutz schon nach geltendem Recht anzuwenden sind. Allerdings kann sich der Arbeitgeber darauf berufen, dass entsprechende Technik nicht verfügbar ist. Dazu heißt es in ErwG 78 der Verordnung: „In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen." Mehr als eine solche „Ermutigung" der Hersteller hat der Verordnungsgeber nicht gewagt.[258]

Alles in allem bietet der Instrumentenkasten der DSGVO damit zahlreiche Werkzeuge, die einen wirksamen Beschäftigtendatenschutz gewährleisten können. Fraglich ist allerdings, ob die Datenflut der zunehmenden Digitalisierung die Instrumente überfordern könnte. Denn umfangreiche Datenmengen, die zudem in vielfältiger Hinsicht u. U. in der Black Box der KI verarbeitet werden, sind durch die genannten Instrumente nur dann zu beherrschen, wenn diese ihrerseits in digitaler Ausführung vorliegen und weitgehend automatisiert funktionieren. Der Verantwortliche muss sich dann auf die Aussagen des Software- oder Geräteherstellers verlassen, dass ein elektronische Verarbeitungsverzeichnis, eine elektronisch durchgeführte Datenschutz-Folgenabschätzung oder eine elektronisch durchgeführte Auswahl geeigneter Mittel oder Maßnahmen tatsächlich im Sinne des Datenschutzes wirken. Ohne gesetzgeberischen Zugriff auf die Produkte selbst ist das nicht realisierbar.

[258] Effekte am Markt erwarten *Klingbeil/Kohm*, MMR 2021, 3 (4).

3.2.7 KOLLEKTIVE INTERESSENVERTRETUNGEN

Betriebsräten steht das Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG zur Verfügung, wonach die Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, der zwingenden Mitbestimmung unterliegt. In ständiger Rechtsprechung legt das BAG die Vorschrift so aus, dass das Merkmal „dazu bestimmt" auf den objektiven Charakter der Technik und nicht auf die subjektiven Absichten des Arbeitgebers abstellt.[259] Die Technik muss objektiv geeignet sein, Verhalten und Leistung der Arbeitnehmer zu überwachen. Zuletzt hat das BAG auch festgestellt, dass das Mitbestimmungsrecht bei Einsatz softwarebasierter Personalverwaltungssysteme nicht vom Überschreiten einer „Erheblichkeits- oder Üblichkeitsschwelle" abhänge, denn es sei offenkundig, dass im Zusammenhang mit digitaler Personalverwaltung erfasste Daten – unabhängig von der konkret genutzten Software – für Verarbeitungsvorgänge zur Verfügung stünden, die für eine Überwachung genutzt werden könnten.[260]

Diese Rechtsprechung hat bedingt Zustimmung in der Fachwelt gefunden,[261] stößt aber aktuell wieder auf verschärfte Kritik. So heißt es, dass das Abstellen auf die bloße Überwachungseignung der Technik letztlich zu einer fast uferlosen Ausweitung der Mitbestimmung führe und ein nicht zustimmender Betriebsrat – egal aus welchen Gründen – in Zeiten von Digitalisierung/Arbeit 4.0 technische Innovation verhindern, zumindest aber verzögern bzw. hohe Aufwände für Einigungsstellenverfahren und ggf. Sachverständige generieren könne.[262]

In der Tat hat die Rechtsprechung dazu geführt, dass der Betriebsrat weitreichende Mitbestimmungsrechte in tendenziell allen Fragen des Beschäftigtendatenschutzes ausüben kann, ohne sich im Einzelfall mit unüberprüfbaren subjektiven Bekundungen der Arbeitgeberseiten zu jeweiligen Absichten auseinandersetzen zu müssen. Unter Bedingungen fortgeschrittener Digitalisierung besteht allerdings eine enorme Gefahr der Überforderung, wenn das gesamte Digitalisierungsgeschehen kontinuierlich sachverständig von der Interessenvertretung nachvollzogen werden muss. Das lässt sich jedoch nicht dadurch lösen, dass Mitwirkungsrechte gesetzlich beschränkt werden.[263] Der Konflikt würde allenfalls verlagert und der Betriebsrat müsste statt in die Einigungsstelle zur Aufsichtsbehörde oder vor Gericht ziehen, um den Belangen des Beschäftigtendatenschutzes im Streitfall Geltung zu verschaffen.

Ein kleiner Schritt in die richtige Richtung ist im Gesetzentwurf der Bundesregierung eines Betriebsrätemodernisierungsgesetzes vom 21.4.2021 enthalten.[264] „Künstliche Intelligenz" wird hier ausdrücklich adressiert. Schon im Planungsstadium muss der Betriebsrat nach beabsichtigter Ergänzung von § 90 Abs. 1 Ziff. 3 BetrVG über den Einsatz von Künstlicher Intelligenz bei Arbeitsverfahren und Arbeitsabläufen unterrichtet werden. Es handelt sich ausdrücklich[265] lediglich um eine Klarstellung des ohnehin gelten Rechts. Wenn allerdings der Betriebsrat zur Durchführung seiner Aufgaben die Einführung und Anwendung von KI beurteilen muss, soll künftig nach dem neuen Satz 2 in § 80 Abs. 3 BetrVG in diesen Angelegenheiten die Prüfung der Erforderlichkeit für

[259] Zuletzt z. B. BAG v. 13.12.2016 – 1 ABR 7/15, NZA 2017, 657 (659), Rn. 22; BAG v. 11.12.2018 – 1 ABR 13/17, NZA 2019, 1009 (1011 f.), Rn. 24.
[260] BAG v. 23.10.2018 – 1 ABN 36/18, ZD 2019, 131 (132) Rn. 5 mit Anmerkung *Stück*.
[261] Uneingeschränkt *Däubler*, Gläserne Belegschaften, 8. Aufl., 2019, Rn. 756 m. w. N.; mit Einschränkung, dass die bloße Möglichkeit der Überwachung nicht ausreiche z. B. Richardi/*Maschmann,* Betriebsverfassungsgesetz, 16. Aufl., 2018, § 87 Rn. 513.
[262] *Stück*, Anmerkung zu BAG v. 23.10.2018 – 1 ABN 36/18, ZD 2019, 131 (132); ähnlich *Haußmann/Thieme*, NZA 2019, 1612 (1617) m. w. N.
[263] Siehe einen entsprechenden Formulierungsvorschlag bei *Haußmann/Thieme*, NZA 2019, 1612 (1618).
[264] BT-Drs. 19/28899.
[265] BT-Drs. 19/28899, S. 22.

die Hinzuziehung eines Sachverständigen entfallen. Da Sachverständigenkosten nicht selten zwischen Arbeitgeber und Betriebsrat umstritten sind, kann diese Neuregelung tatsächlich die Informationsgrundlage der Betriebsratsarbeit ein wenig verbessern.

3.3 ERGEBNIS

Das Potenzial des geltenden Beschäftigtendatenschutzes aus § 26 BDSG ist unter Berücksichtigung der ergänzenden Transparenz- und Durchsetzungsvorschriften der DSGVO durchaus beachtlich. Die Zulässigkeitsmaßstäbe sind in der Auslegung des Bundesarbeitsgerichts ausreichend streng und die begleitenden Rechte der Beschäftigten sowie organisatorischen Pflichten aus der DSGVO sind vielversprechend, wenn sie systematisch als Teil des Beschäftigtendatenschutzes angewendet werden. Das liegt vor allem daran, dass in den vorgeschriebenen Verfahren, die technologieneutral ausgestaltet sind, neue Entwicklungen vorab vorausschauend berücksichtigt werden müssen. Umsetzungsdefizite bestehen zweifellos, die aber wohl durch die dazu berufenen Institutionen Rechtsprechung, Behörden, betriebliche Akteure sowie Formate der Selbstregulierung aussichtsreich bearbeitet werden könnten, solange sich die Anforderungen kontinuierlich entwickeln.

Die Frage in dieser Studie ist allerdings, ob dieses Instrumentarium auch der Wucht einer allseitig fortschreitenden Digitalisierung aller betrieblichen Funktionen gewachsen ist, wie sie im Zuge der 4.0-Prozesse beabsichtigt ist.

Unklares und schwer verständliches Recht ist ein bedeutender Faktor, der die Durchsetzungskraft des Beschäftigtendatenschutzes schwächt. Daher soll zunächst auf die bisher aufgefundenen Unklarheiten und Schwachstellen des geltenden Rechts hingewiesen werden:

- Wenig konkrete gesetzliche Anforderungen an die *Zwecksetzung* der Verarbeitung von Beschäftigtendaten und schwer durchschaubare Möglichkeiten der nachträglichen *Zweckänderung* durch den Arbeitgeber erleichtern es, dass umfangreiches personenbezogenes Datenmaterial recht frei von ursprünglichen Absichten und schwer kontrollierbar neuen Auswertungen zuzuführen ist.
- Große *Rechtsunsicherheit* besteht insbesondere auf zentralen Feldern wie dem Datenschutz im Bewerbungsverfahren oder der Verarbeitung sensibler Daten nach § 26 Abs. 3 BDSG.
- Strukturelle Nachteile der Beschäftigtenseite in der Interessenabwägung drohen, wenn den betriebswirtschaftlich anerkannten und staatlich geförderten unternehmerischen Belangen einer umfassenden Digitalisierung, die im Mainstream der technischen Entwicklung liegt, im *isolierten Einzelfall* nur sehr schwer ähnlich starke Belange des Persönlichkeitsschutzes entgegengehalten werden können. Eine Gesamtschau wäre erforderlich.

Aber auch nach klärender Überarbeitung des geltenden Rechts würden die zentralen Probleme fortbestehen:

- Ohne systematische technische Unterstützung ist eine Überforderung der Arbeitgeber, Transparenzpflichten über ein hoch komplexes und KI-durchzogenes Datenverarbeitungsgeschehen herzustellen, unvermeidlich.

- Eine Überforderung der individuellen Reaktionsmöglichkeiten der Beschäftigten ist bei hoher technologischer Dynamik ohnehin zu erwarten. Insbesondere bei Abwesenheit kollektiver Interessenvertretungen liegt die Kontrolle weitgehend beim Individuum, das aber schon die einzelnen Auswirkungen der Datenverarbeitung, geschweige denn deren Rechtmäßigkeit regelmäßig nicht beurteilen kann.
- Bei beschleunigter Digitalisierungsentwicklung besteht auch die Gefahr der Überforderung der betrieblichen und behördlichen Interessenvertretungen, die auf einem technisch schwer zu durchschauenden Feld tragfähige Lösungen für komplexe Interessenlagen finden müssen.
- Zu schwach sind die Verpflichtungen des Technischen Datenschutzes nach Art. 25, 35 DSGVO. Die systematische Folgenabschätzung der Technik nach Art. 35 DSGVO scheint zu sehr auf Ausnahmen beschränkt zu sein. „Privacy by Design“ nach § 25 DSGVO beschränkt sich auf die Möglichkeiten der Anwender. Der rechtliche Durchgriff auf die Anbieter und Entwickler fehlt. Datenschutz gehört aber ins Technikrecht, denn nur in der Technik kann er implementiert werden.

Das vorrangige Problem ist also, dass alle Systeme des rechtlichen Datenschutzes auf quantitativ und hinsichtlich ihrer Verarbeitungslogik überschaubare Formen der personenbezogenen Datenverarbeitung ausgerichtet sind. Der einzelne Beschäftigte hat dafür alle nötigen Rechte, auch die Interessenvertretungen sind rechtlich machtvoll ausgestattet. Aber gegenüber der Wucht ständig fortentwickelter Technologie auf zahlreichen „Baustellen“ gleichzeitig ist das Individuum am Ende der Entscheidungskette nahezu hilflos. Besser sieht es für die Interessenvertretungen aus, die vorab zu beteiligen sind und von deren Zustimmung technische Innovationen abhängig sind. Voraussetzung ist allerdings, dass Interessenvertretungen vorhanden sind, die über das anspruchsvolle technische Wissen verfügen, die Kapazitäten haben, sich mit der Technologieentwicklung ständig dezidiert auseinanderzusetzen, und über Kreativität für sinnvolle Regelungen verfügen, die den unterschiedlichen Interessen auch innerhalb der Belegschaften gerecht werden.

Die mögliche Lösung, direkt die Entwickler der Technik in die Pflicht zu nehmen, ist demgegenüber angesichts des gegenwärtigen Standes des technischen Datenschutzes (Art. 25 DSGVO) völlig unterentwickelt. Hier liegt der zentrale Ansatzpunkt.

4. REGELUNGSDEFIZITE UND REGELUNGSIDEEN

Seit mindestens 20 Jahren wird von der Bundesregierung bzw. vom Deutschen Bundestag ein Beschäftigtendatenschutzgesetz in Aussicht gestellt, das 2010 sogar schon einmal konkrete Gestalt angenommen hat, um letztlich aber doch wegen unüberbrückbarer Interessengegensätze nicht verabschiedet zu werden.[266] Die kleine Lösung in Form eines Paragraphen § 32 BDSG 2009 galt als Übergangslösung, wurde dann aber mit kleinen, nicht ganz unerheblichen Ergänzungen auch in § 26 BDSG 2017 in die Zeit nach Geltung der DSGVO übernommen. Auszufüllen ist damit die Öffnungsklausel in Art. 88 DSGVO durch „spezifischere Vorschriften" zum Beschäftigtendatenschutz. In welcher Weise dies durch § 26 BDSG geschehen ist und welche Vorschriften der DSGVO ergänzend eine Rolle spielen, ist in Kap. 3 eingehend dargestellt und bereits auf möglich Schwachstellen abgeklopft worden. Im Folgenden geht es darum, die Defizite der aktuellen Regulierung im Hinblick auf die laufenden Digitalisierungsprozesse vertiefend zu erörtern und dabei auch Regelungsideen für die künftige Rechtsentwicklung zu bestimmen.

In einer *Literaturauswertung* sollen zunächst vorhandene Studien und Diskussionsbeiträge zum Reformbedarf des Beschäftigtendatenschutzes zusammengetragen werden (4.1), um die dort festgestellten Defizite zur Kenntnis zu nehmen. Die Papiere liefern zudem zahlreiche Vorschläge, was der Gesetzgeber künftig im Beschäftigtendatenschutz regeln sollte. Die inhaltlichen Schwerpunkte, die sich aus diesen Analysen und Ideen ergeben, werden im Anschluss (4.2.) vor dem Hintergrund der eigenen Erkenntnisse aus Kap. 1-3 diskutiert.

4.1 BEITRÄGE DER WISSENSCHAFTLICHEN DISKUSSION

Die ausführlichste Studie ist 2017 von *Krause* als Forschungsbericht 482 des BMAS unter dem Titel „Digitalisierung und Beschäftigtendatenschutz" vorgelegt worden.[267] In diesem Bericht sind die Defizite als Fortentwicklungsbedarf beschrieben. Laut *Krause*[268] sollte sich ein gesetzgeberisches Handeln davon leiten lassen, der arbeitsrechtlichen Praxis ein möglichst klares und übersichtliches Regelungswerk an die Hand zu geben. Hiervon sei die gegenwärtige Ausgestaltung des BDSG im Hinblick auf den Arbeitnehmerdatenschutz weit entfernt. Dem Ziel einer praxisnahen und handhabbaren Regelung käme ein eigenständiges Beschäftigtendatenschutzgesetz am nächsten. Krause empfiehlt keine zu stark an einzelnen technologischen Entwicklungen orientierte Regelungstechnik zu wählen, die durch Innovationen rasch überholt würde. Stattdessen hält er die Festschreibung bestimmter Grundsätze für erforderlich: der grundsätzliche Ausschluss heimlicher Kontrollen, die Begrenzung der Lokalisierung von Mitarbeitern sowie der Ausschluss von umfassenden Bewegungsprofilen, der grundsätzliche Ausschluss von Dauerüberwachungen des Arbeitsverhaltens, die regelmäßige Einschränkung von biometrischen Systemen auf Authentifizierung und Autorisierungszwecke, klare Einschränkungen von psychologischen Untersuchungsmethoden (strenge Wissenschaftlichkeit, keine Durchleuchtung der gesamten Persönlich-

[266] Zur Geschichte der Bemühungen um ein Beschäftigtendatenschutzgesetz *Däubler*, Gläserne Belegschaften, 8. Aufl., 2019, S. 606 ff.; *Lurtz/Ruhmann*, Der lange Weg zu einem Beschäftigtendatenschutzgesetz?, ZD-Aktuell 2020, 07281.
[267] *Krause*, Forschungsbericht 482, 2017.
[268] Ebenda, S. 49.

keit).[269] Für die Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG empfiehlt er eine Ausdehnung generell auf den Umgang mit personenbezogenen bzw. personenbeziehbaren Daten von Beschäftigten.[270]

Zahlreiche weitere wissenschaftliche Diskussionsbeiträge zu Defiziten oder Änderungsbedarfen des Beschäftigtendatenschutzes sind in den arbeits- und datenschutzrechtlichen Fachmedien seit 2016 publiziert worden. Die folgende Auswertung konzentriert sich auf jene Beiträge, die die Herausforderungen der fortschreitenden Digitalisierung erkennbar adressieren.

Hofmann[271] geht 2016 davon aus, dass sich die Herausforderungen der Industrie 4.0 für den Arbeitnehmerdatenschutz mit den bekannten Prinzipien angemessen bewältigen ließen. Im Betrieb werde die Hauptaufgabe darin bestehen, die Zwecke der eingesetzten Systeme genau zu bestimmen und basierend hierauf den erforderlichen Datenumgang präzise abzugrenzen. Würden die hierbei gewonnenen Erkenntnisse von Anfang an bei der *Technikauswahl und -gestaltung* berücksichtigt, könnten die meisten Probleme bereits im Ausgangspunkt vermieden werden. In Bereichen, in denen ein intensiver Datenumgang dennoch erforderlich bleibe, sei dem daraus resultierenden Risiko *mit der Implementierung rechtlicher Verwendungsschranken* zu begegnen.

Körner[272] betont ebenfalls bereits 2016, dass sich angesichts rasant entwickelnden Informationstechnologie, der Speicherkapazitäten und damit der Auswertungsmöglichkeiten großer Datenmengen rein normative Vorgaben den Schutz der informationellen Selbstbestimmung des Einzelnen nicht mehr ausreichend sicherten. Die vagen Verpflichtungen aus Art. 25 DSGVO zum Datenschutz durch Technik könne der nationale Gesetzgeber im Beschäftigtendatenschutz viel genauer in zu treffenden Maßnahmen bzw. zuständigen Instanzen bestimmen.

Nebel[273] stellt 2018 fest, dass die herkömmlichen Konzepte des Beschäftigtendatenschutzes bei Big Data-Anwendungen nicht tauglich seien. Bei Big Data-Analysen verarbeiteten viele Beteiligte viele – oftmals anonyme – Daten aus vielen Quellen. Der Personenbezug und die Zweckbestimmung sei oft unklar, oftmals würden private und geschäftliche Zwecke vermengt. Zweckbindung, Erlaubnistatbestände und Transparenz seien praktisch nicht durchführbar. Eine wichtige Rolle hätten Betriebsvereinbarungen zur Schaffung adäquater Regelungen. Darüber hinaus sei der Gesetzgeber langfristig in der Verpflichtung, adäquate, moderne Lösungen zu finden, insbesondere die Entwickler der entsprechenden Technologien in die Pflicht zu nehmen, eine möglichst *datenschutzfreundliche, die Persönlichkeitsrechte der Arbeitnehmer wahrende Technik* zu entwickeln.

Kort[274] untersucht 2018 zahlreiche Phänomene der Digitalisierung am Arbeitsplatz und kommt zu dem Ergebnis, dass zwar angesichts von „Industrie 4.0“ eine „Rundumüberwachung“ des Arbeitnehmers technisch immer einfacher werde, der Gefahr einer solchen „Rundumüberwachung“ aber mit den Mitteln des neuen Datenschutzrechts und der arbeitsgerichtlichen Rechtsprechung, die auch unter Geltung der DSGVO und des neuen BDSG weiter Bedeutung hat, erfolgreich begegnet werden könne. In seiner Detailanalyse werden aber z. B. beim Phänomen Big Data-Anwendungen oder bei der Frage nach der Rechtsgrundlage der Videoüberwachung klärungsbedürftige Probleme deutlich.[275]

[269] Ebenda.
[270] Ebenda, S. 51.
[271] *Hofmann*, ZD 2016, 12 (17).
[272] *Körner*, NZA 2016, 1383 (1386).
[273] *Nebel*, ZD 2018, 520 (524).
[274] *Kort*, RdA 2018, 24 (33).
[275] Ebenda, 27 f.

Maschmann[276] hält 2018 ein eigenständiges Beschäftigtendatenschutzrecht für wünschenswert. Das Fehlen werde sich vor allem bei den praktisch besonders relevanten Fragen der Mitarbeiterkontrolle rächen, deren Voraussetzungen derzeit kaum verlässlich zu beschreiben seien. Er verweist u. a. auf die EGMR Rechtsprechung, die heimliche Videoüberwachung ausschließe,[277] wie sie das BAG auf Grundlage von § 32 Abs. 1 Satz 2 BDSG a.F. zugelassen habe.[278] Zwischenzeitlich hat sich zwar die Rechtsprechung durch die Große Kammer des EGMR geändert.[279] Dennoch dürfte die Kritik großer Rechtsunsicherheit bei (heimlichen) Mitarbeiterkontrollen fortbestehen.

Haußmann und Thieme[280] befürworten 2019 den Erlass eines Beschäftigtendatenschutzgesetzes, das u. a. technische und organisatorische Maßnahmen sowie Anforderungen an ein System, das Datenschutz durch Technikgestaltung umsetzen soll, konkretisiert. Standardisierung und Zertifizierung entsprechender Produkte sollten geregelt werden. Ein Vorschlag für die Reduzierung des Mitbestimmungsrechts des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG wird zwecks Verfahrensbeschleunigung und Konzentration auf die wesentlichen Fragen formuliert.[281]

Giesen[282] stellt 2020 ähnlich fest, dass es dort, wo Digitalisierung zur Diskussion stehe, die betriebsverfassungsrechtlichen Mitbestimmungsrechte auf einem so soliden Fundament stünden, dass es für den Betriebsrat ein Leichtes sei, einen Renovierungsstau auszulösen. Die Betriebsverfassung werde unnötig diskreditiert. Diese Entwicklung ließe sich mit einer Reform des Betriebsverfassungsrechts verhindern, welche die Verfahren beschleunige und die materiellen Mitbestimmungsrechte auf die Erfordernisse der Digitalisierung ausrichte.

Lurtz und Ruhmann[283] sprechen sich 2020 für ein Beschäftigtendatenschutzgesetz aus, denn im Beschäftigungsverhältnis bestünden einige Regelungsbereiche, die einer Konkretisierung bedürften. Dazu zählen sie die ständig umfassender werdende Videoüberwachung; Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent und vergleichbar werden lassen; die zunehmende Vermischung des beruflichen und des privaten Bereichs; der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten z. B. aus sozialen Netzwerken. Darüber hinaus erscheine es u. a. sinnvoll, Grenzen zu zulässigen Kontrollen von Beschäftigten zu ziehen sowie die Begrenzungen von Lokalisierungen oder biometrischer Authentifizierungssysteme zu regeln. Ferner verdiene die Verarbeitung von sensiblen Daten auf Grund ihrer zunehmenden Häufigkeit im Beschäftigungsverhältnis und der unklaren Regelung des § 26 Abs. 3 BDSG eine genauere Betrachtung.

Die *Datenschutzkonferenz*[284] aus den unabhängigen Datenschutzbehörden des Bundes und der Länder hat 2020 in der Aktualisierung des Kurzpapiers Nr. 14 Beschäftigtendatenschutz abschließend Wünsche an ein Beschäftigtendatenschutzgesetz geäußert. Ein solches Gesetz könnte demnach unter anderem das Fragerecht bei der Einstellung von Bewerberinnen und Bewerbern, die Problematik eines Pre-Employment-Screenings, die Grenzen zulässiger Kontrollen von Beschäftigten, die Begrenzung von Lokalisierungen (GPS) und die Verwendung biometrischer Authentifi-

[276] *Maschmann*, NZA-Beilage 2018, 115 (124).
[277] Ebenda, 121.
[278] Vgl. BAG v. 27.03.2003, NZA 2003, 1193); BAG, NZA 2017; BAG NZA 2017, 112 (114).
[279] EGMR (GK), Urt. v. 17.10.2019 – 187413 1874/13, 8567/13, NZA 2019, 1697 in der Besprechung von Körner, EGMR relativiert Verbot der Videoüberwachung, NZA 2020, 25 (27).
[280] *Haußmann/Thieme*, NZA 2019, 1612 (1618).
[281] Ebenda, S. 1618, 1620.
[282] *Giesen*, NZA 2020, 73 (76).
[283] *Lurtz/Ruhmann*, Der lange Weg zu einem Beschäftigtendatenschutzgesetz?, ZD-Aktuell 2020, 07281.
[284] *DSK*, Kurzpapier Nr. 14, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf.

zierungs-und Autorisierungssysteme oder die Nutzung künstlicher Intelligenz zum Gegenstand haben.

Weichert und Schuler[285] setzen im Rahmen ihrer Empfehlungen für ein Beschäftigtendatenschutzgesetz vom 18.12.2020 vorrangig auf eine verbesserte Beherrschbarkeit der Technik. Die Datenschutz-Folgenabschätzung soll u. a. durch eine ausdrückliche Pflicht, den Betriebsrat zu beteiligen, aufgewertet werden, die bereits in Art. 35 Abs. 9 DSGVO angelegt ist.[286] Vorgeschlagen wird weiter, die Zertifizierung von IT-Systemen gemäß Art. 42 Abs. 1 DSGVO für den Beschäftigtendatenschutz zu spezifizieren. Der Nachweis der Datenschutzkonformität könnte durch Zertifizierung erbracht werden.[287] Aus den zahlreichen weiteren Vorschlägen von Weichert und Schuler sticht die geforderte Klarstellung zu den Grenzen der Zweckänderung bei Beschäftigtendaten heraus. Klarzustellen ist insbesondere, dass die zahlreichen erfassten Daten für unterschiedlichste Zwecke nicht beliebig insbesondere zur Leistungskontrolle zusammengeführt werden dürfen.[288] Eine wesentliche Innovation ergäbe sich aus der vorgeschlagenen Einrichtung eines Kompetenzzentrums Beschäftigtendatenschutz beim Bundesarbeitsministerium, das Empfehlungen erarbeitet.[289] Die Möglichkeiten, Verhaltensregeln nach Art. 40 DSGVO zu vereinbaren und Verbandsklagen nach Art. 80 Abs. 2 DSGVO zuzulassen, sollen nach Weichert und Schuler die Durchsetzung des Beschäftigtendatenschutzes weiter verbessern.[290]

In der Diskussion um die Neuregelung des BDSG 2017, haben sich auch Verbände zu Wort gemeldet. Die Auswertung beschränkt sich hier auf zwei Stellungnahmen, soweit sie die Entwurfsfassung von § 26 BDSG betreffen und auch nach Inkrafttreten noch von Belang sind.

Der *BDA* vertritt,[291] dass vor dem Hintergrund der Debatte zu „Arbeiten 4.0" die grundlegende Frage zu stellen sei, wie der Beschäftigtendatenschutz an die technischen Entwicklungen angepasst werden müsse, damit er die sich hieraus ergebenen Chancen flankieren kann, ohne dabei zum Hemmschuh für den Einsatz neuer technischer Entwicklungen zu werden. Weitere Verschärfungen gesetzlicher Vorgaben, seien der falsche Weg. Der BDA vermisst z. B. eine Klarstellung, dass Arbeitgeber auch dann einem konkreten Verdacht auf eine schwere Vertragspflichtverletzung zielgerichtet nachgehen könnten, wenn diese unterhalb der Schwelle zur Strafbarkeit läge.[292] Das gelte auch für präventive Ermittlungen.[293] Konkrete Vorgaben im Gesetzestext, wann eine freiwillige Einwilligung vorliegen könne, lehnt der BDA ab. Ein klares Ungleichgewicht im Arbeitsverhältnis sei grundsätzlich nicht gegeben. Mit der Erteilung einer Einwilligung übe der betroffene Grundrechtsträger sein Grundrecht auf informationelle Selbstbestimmung aus. Nur bei begründeten Zweifeln sollte geprüft werden, ob eine besondere Situation vorliege, die der freiwilligen Erteilung einer Einwilligung entgegenstehen könnte.[294] Auch die Vorgabe, dass § 26 BDSG auch dann anzuwenden sei, wenn Daten verarbeitet werden, die nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen, wird abgelehnt.[295] Gleiches gilt für die in § 26 Abs. 8 BDSG vorgenommene Ausweitung des Beschäftigtenbegriffs auf Leiharbeitneh-

[285] *Weichert/Schuler*, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2020_beschdsg_final.pdf; ähnlich *Weichert*, NZA 2020, 1597.
[286] *Weichert/Schuler*, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, S. 20.
[287] Ebenda, S. 21.
[288] Ebenda, S. 22.
[289] Ebenda, S. 24.
[290] Ebenda, S. 26.
[291] BDA, Beschäftigtendatenschutz vernünftig anpassen, 2. März 2017, Deutscher Bundestag – Innenausschuss, Drs. 18/(4)813, S. 9.
[292] Ebenda, S. 3.
[293] Ebenda, S.9.
[294] Ebenda, S. 3 f.
[295] Ebenda, S. 6.

mer*innen.[296] Darüber hinaus sei es wesentlich, dass klargestellt werde, dass beiden Parteien einer Kollektivvereinbarung ein weiter Verhandlungsspielraum zugestanden werde. Eine solche Klarstellung sei insbesondere vor dem Hintergrund der veränderten Sanktionsfolgen und dem Auslegungsbedarf vieler Vorschriften der Datenschutz-Grundverordnung erforderlich. Die Verhandlungspartner benötigten Rechtssicherheit.[297] Im Beschäftigtendatenschutz sollte ein Anreiz dafür gesetzt werden, personenbezogene Daten zu anonymisieren oder zu pseudonymisieren. Das könnte dadurch geschehen, das eine solche Anonymisierung oder Pseudonymisierung ohne Einwilligung der betroffenen Person erfolgen könne. Im Bereich der Privatnutzung von E-Mail und Internet bedürfe es zudem einer gesetzlichen Klarstellung, dass Arbeitgeber in diesem Fall nicht Diensteanbieter im Sinne des TKG und TMG werden.[298]

Der *DGB*[299] vertritt 2017 die Auffassung, dass die vom Gesetzgeber vorliegend gewollte Ausgestaltung des Beschäftigtendatenschutzes nach Maßgabe des Art. 88 DSGVO durch die Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes vorgenommen werden sollte. Als Übergangsregelung akzeptiert der DGB § 26 BDSG (in der Entwurfsfassung 2017) sowie die dort bereits vorhandenen Konkretisierungen. Es fehlten jedoch andere erforderliche Konkretisierungen für eine personenbezogene Verarbeitung von Beschäftigtendaten im Beschäftigungskontext wie die notwendige Erweiterung des Mitbestimmungsrechts für Betriebsräte bei der personenbezogenen Datenverarbeitung; die Konkretisierung und Einschränkung der Videoüberwachung im Beschäftigungsverhältnis; die Regelung über die Voraussetzungen einer Nutzung personenbezogener Speicher- und Verarbeitungsmedien zu Zwecken des Beschäftigungsverhältnisses sowie die Ausformung der spezifischen Zweckbindung und Zweckänderung im Beschäftigungskontext.[300] In einem künftigen Beschäftigtendatenschutzgesetz sind laut DGB[301] insbesondere folgende weitere Themenbereiche regelungsbedürftig. Zugriff auf personenbezogene oder beziehbare Daten bei der Verwendung moderner Kommunikationsmittel; Umfang des Fragerechts des Arbeitgebers sowie Regeln zur Zulässigkeit ärztlicher Untersuchungen und Eignungstests; Verwertung und Aufbewahrung von Daten vor, während und nach der Beendigung des Beschäftigungsverhältnissen; Umgang mit Daten aus sozialen Medien; Datenschutz bei Bring Your Own Device; Beweisverwertungsverbot von unrechtmäßig erhobenen Daten. Zu Durchsetzungszwecken plädiert der DGB zudem für ein Verbandsklagerecht.

Zusammengefasst lassen sich – um den Preis viele auch wichtige Details beiseitezulassen – vier Schwerpunkte der bisherigen Diskussion erkennen:

1. Rechtsklarheit/einheitliches Gesetz
2. Überwachung/psychologische Analysen
3. Big Data/KI/Datenschutz durch Technik
4. Mitbestimmung/Partizipation

[296] Ebenda, S. 6.
[297] Ebenda, S. 5.
[298] Ebenda, S. 9.
[299] DGB Bundesvorstand, Stellungnahme des Deutschen Gewerkschaftsbundes zum Gesetzentwurf der Bundesregierung: Gesetz zur Anpassung des Datenschutzrechts – DSAnpUG-EU, 27. Februar 2017, S. 2.
[300] Ebenda, S. 3.
[301] Ebenda, S. 27.

4.2 EINZELNE DEFIZITE UND LÖSUNGSVORSCHLÄGE

Die vier am Schluss von 4.1 genannten Schwerpunkte der Fachdebatte decken sich weitgehend mit den Ergebnissen der hier in Kap. 1 und 3 durchgeführten Analyse. Einige Aspekte wären zu ergänzen – vor allem im Hinblick auf die Frage, welche Rechtsfragen besonders dringend einer gesetzlichen Klarstellung bedürfen. Ein Unterpunkt zum „Datenschutz im Arbeitsschutz“ sei als fünfter Punkt ergänzt.

4.2.1 RECHTSKLARHEIT/EINHEITLICHES GESETZ

Der Wunsch nach einem einheitlichen Beschäftigtendatenschutzgesetz steht erneut im Raum, seitdem das Bundesarbeitsministerium (BMAS) einen Beirat aus unterschiedlichen Fachrichtungen berufen hat, der Empfehlungen für ein solches Gesetz entwickeln soll.

So solide der Beschäftigtendatenschutz in Deutschland als Gesamtsystem wirkt, so baufällig sind seine gesetzlichen Grundlagen. Wer nur die Rechtsquellen in DSGVO und BDSG zur Verfügung hat, tappt im Dunkeln. *Krause* plädiert völlig zurecht dafür, ein „benutzerfreundliches“ klares und übersichtliches Regelwerk zu schaffen.[302] In den Betrieben müssen viele Menschen mit diesem Recht arbeiten, die nicht juristisch ausgebildet sind. Es sollte wenigstens – notfalls mit Verweisen in andere Rechtsquellen – aus dem Gesetzestext klar werden, welche Vorschriften den Beschäftigtendatenschutz ausmachen.

Das Problem ist dreifacher Natur. Der gesetzliche Beschäftigtendatenschutz ist

- zersplittert,
- teils irreführend,
- teils zu abstrakt

geregelt.

Zersplittert bedeutet, dass die maßgeblichen Regelungen aus DSGVO und BDSG zusammenzusuchen sind. Viele wichtige Aussagen existieren überhaupt nur in der Rechtsprechung.

Irreführend heißt, dass in zentralen Vorschrift schlicht nicht das drinsteht, was sie aussagen sollen. Das gilt vor allem für den Maßstab der Erforderlichkeit in § 26 Abs. 1 BDSG. Weitgehend rätselhaft ist zudem § 26 Abs. 3 BDSG.

Abstrakt muss nicht schlecht sein bei einem Gesetz. Aber in manchen Fragen könnte mehr Orientierung durch den Gesetzgeber helfen. Genannt wird besonders häufig das Recht

- der Datenverarbeitung im Bewerbungsverfahren und
- der Videoüberwachung und anderer Überwachungstechniken,

bei denen versucht werden könnte, immerhin die geltende Rechtsprechung in Worte zu fassen.

[302] *Krause*, Forschungsbericht 482, 2017, S. 49.

Zwei Aspekte sollen hier auf Grundlage der eigenen Untersuchungen (Kap. 1 und 3) ergänzt werden, die zwar auch bei einzelnen Autor*innen genannt werden, aber bisher weniger im Blickpunkt der Debatte stehen:

- Die *Zweckbindung* der Datenverarbeitung muss für das Beschäftigungsverhältnis präzisiert werden. Der Betrieb ist nun mal ein einzigartiger Ort, an dem – oft über viele Jahre – so viele unterschiedliche Daten über eine Personen zu unterschiedlichsten Zwecken gehandhabt werden, dass Datenschutz dringend darauf angewiesen ist, dass die Trennung der Datenbestände nicht untergraben wird.[303] Gerade wenn die Chancen von Big Data und KI genutzt werden sollen, ist ein präzises Management der Datenvielfalt unerlässlich. Das Recht kann diese Trennung nicht zuverlässig erzwingen. Aber es kann klare und verständliche Regelungen für Zweckbindung und Zweckänderung im Beschäftigungsverhältnis formulieren. Helfen muss in der Umsetzung dessen die Technik, die wenigstens eine unkontrollierte Vermischung und unbefugte Verwendungen (weitgehend) ausschließen kann.
- *Sensible Daten*, insbesondere zum physischen und psychischen Befinden der Beschäftigten, werden eine zunehmend große Rolle spielen. Das folgt aus der Digitalisierung des Personalmanagements und des Arbeitsschutzes. Gerade hierfür ist die genannte Trennung von fundamentaler Bedeutung. Zugleich muss die Zulässigkeit ihrer Erhebung viel klarer als bisher in § 26 Abs. 3 BDSG geschehen formuliert werden.

4.2.2 ÜBERWACHUNG/PSYCHOLOGISCHE ANALYSEN

Den Themen Überwachung und psychologische Analysen ist gemeinsam, dass die Würde des Menschen hier besonders gefährdet sein kann. Klare Grenzen gesetzlicher Regelungen wären hier daher besonders wünschenswert.

a) Videoüberwachung

Videoüberwachung ist der wichtigste Sonderfall der Überwachung bei der Arbeit. Die technischen Möglichkeiten wachsen kontinuierlich. KI kann für eine automatisierte Bildauswertung sorgen. Auch Fahr- und Fluggeräte in Arbeitsstätten oder auf Baustellen nutzen Kameras, um sich zu orientieren. Schließlich benötigen auch Roboter „Augen“, wenn sie mit Menschen Hand in Hand arbeiten sollen. Oft sind von Videoüberwachung unterschiedliche Personenkreise betroffen, so etwa Kunden*innen im Einzelhandel und zugleich Beschäftigte. Hinsichtlich der Beschäftigten geht es einerseits – wie bei den Kunden*innen – um möglichen Diebstahl, aber auch das Arbeits- und Leistungsverhalten gerät ins Blickfeld. Es ist unklar, inwieweit sensible Daten miterfasst werden, z. B. Gesundheitsdaten, die sich etwa aus dem Gangbild ergeben können.

Für die Beschäftigten kann eine Dauerbelastung eintreten, da u. U. die gesamte Arbeitszeit im Aufnahmefeld von Kameras abgeleistet wird. Hinzu kommt die hohe Eingriffstiefe von Bilddaten. Videoüberwachung kann zudem technisch problemlos auch heimlich stattfinden. Auf Seiten der Arbeitgeber ist Videoüberwachung recht beliebt, um z. B. vor Diebstahl abzuschrecken. Gerade

[303] Siehe auch *Weichert/Schuler*, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, S. 22.

zur Täterermittlung werden heimliche Überwachungsverfahren eingesetzt. Entsprechend gegensätzlich sind die Wünsche an ein Beschäftigtendatenschutzgesetz.

Für alle betrieblich anfallenden *personenbezogenen Bild- und Videodaten* wären klare gesetzliche Regelungen sehr wünschenswert. Denn die Rechtslage ist unübersichtlich. Im gegenwärtigen Recht findet sich in § 4 BDSG eine gesetzliche Regelung zur Videoüberwachung, die das ältere Recht in § 6b BDSG a.F. fortschreibt, die aber auf öffentlich zugängliche Räume beschränkt ist. Das BAG hat ohnehin die Regelung in § 32 BDSG a.F. (jetzt § 26 BDSG), obgleich dort Videoüberwachung nicht konkret angesprochen wird, einer Anwendung von § 6b BDSG a.F. vorgezogen.[304] Zugleich gibt es eine aktuelle Rechtsprechung des Großen Senats des EGMR v. 17.10.2019, die ausnahmsweise auch verdeckte Videoüberwachung für vereinbar mit Art. 8 EMRK hält, jedenfalls soweit es um den berechtigten Verdacht schwerwiegender Straftaten geht.[305] Genauer gesagt heißt es beim EGMR, dass zwar nicht der geringste Verdacht von Unterschlagungen oder anderen Straftaten seitens des Personals den Arbeitgeber dazu berechtigen würde, eine geheime Videoüberwachung einzurichten. Ein berechtigter Verdacht aber, dass schwerwiegende Straftaten begangen würden, und der Umfang der festgestellten Verluste könnten eine erhebliche Rechtfertigung sein. Das gelte umso mehr in einer Situation, in der ein reibungsloser Betrieb eines Unternehmens durch den Verdacht von Straftaten gefährdet sei, die nicht nur von einem Arbeitnehmer, sondern durch gemeinsames Handeln mehrerer begangen würden, weil das ein allgemeines Klima des Misstrauens im Unternehmen erzeugen könnte.

Mit dieser Rechtsprechung mag sich eine Klärung der Grenzen heimlicher Videoüberwachung abzeichnen, die auch in ein Gesetz übernommen werden kann. Für die Frage der Erfassung sensibler Daten i. S. v. Art. 9 Abs. 1 DSGVO ist die Rechtslage jedoch noch völlig offen. Jede Kamera, die Menschen erfasst, erfasst auch sensible Daten über diese. Jedenfalls eine entsprechende Auswertung des Bildmaterials kann – mit denkbaren Ausnahmen für Arbeitsschutzzwecke – untersagt werden.

b) Ortungssysteme/sonstige Überwachung des Arbeitsverhaltens

Neben der in Branchen mit Kundenverkehr dominanten Videoüberwachung, die oftmals vorrangig Kund*innen überwacht und nur als Nebeneffekt auch die Beschäftigten, gibt es viele weitere Technologien, die geeignet sind, das Arbeitsverhalten von Beschäftigten zu erfassen. Es geht um ein weites Feld teils alter, teils hochmoderner und ständig verbesserter Technologie von Lokalisierungstechnik, Abhörtechnik im Telefon, Trackingtools in Arbeitsgeräten oder am Körper zu tragen, Bewertungstools (z. B. durch Kund*innen) u. V. m.

Die *permanente Ortung* von Beschäftigten, die innerhalb oder außerhalb des Betriebs unterwegs sind, durch GPS-Tracker oder RFID-Tags ähnelt der Videoüberwachung und wäre daher entsprechend zu regeln. Das heißt, dass die heimliche Durchführung nur in Extremfällen erlaubt werden könnte, wenn erhebliche kriminelle Energie nachweislich im Spiel ist. Umfassende Bewegungsprofile dürfen durch Ortungssysteme nicht routinemäßig erstellt werden, was schon nach gegenwärtigem Recht vielfach vertreten wird.[306] Die Rechtsprechung ist erst in Ansätzen[307] tätig gewor-

[304] Siehe zuletzt BAG v. 28.3.2019 NZA 2019, 1212 (1217) Rn. 49.
[305] EGMR (GK), Urt. v. 17.10.2019 – 187413 1874/13, 8567/13, NZA 2019, 1697
[306] *Däubler*, Gläserne Belegschaften, 8. Aufl., 2019, Rn. 322; *Kort*, RdA 2018, 24 (28); *Krause*, Forschungsbericht 482, 2017, 56: *Tiedemann*, in: Kramer, IT-Arbeitsrecht, 2. Aufl., 2019, B. Individualarbeitsrecht, Rn. 575; a. A. *Byers*, in: Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl., 2019, Teil B. VII b) Rn. 27.
[307] ArbG Heilbronn v. 30.1.2019 – 2 Ca 360/18, Telematik-Box, ArbRAktuell 2020, 22.

den. Zuletzt hat das VG Ansbach allerdings ausgeführt, dass GPS-Überwachung durch legitime Zwecke des Flottenmanagements gedeckt sein könne.[308] Widersprüchliche Ansichten in Lehre und Rechtsprechung legen den Wunsch nach einem klärenden Wort des Gesetzgebers nahe.[309]

Fragt sich also, ob es ein Defizit des geltenden Rechts darstellt, diese Abwägung vollständig den Gerichten zu überlassen, und ob eine gesetzliche Konkretisierung hilfreich wäre. Das Gesetz muss offen für künftige technische Entwicklungen bleiben. Auch muss es weiterhin die Möglichkeit einräumen, wechselnde betriebliche Umstände zu berücksichtigen. Von daher kann völlige Eindeutigkeit nicht erwartet werden. In der Keylogger-Entscheidung des BAG[310] etwa wurden die mangelnde Transparenz und die hohe Kontrolldichte als ausschlaggebend angesehen, die Anwendung der Technik als rechtwidrig einzustufen. Die vom Keylogger gewonnenen Daten ermöglichten es, so das BAG, ein nahezu umfassendes und lückenloses Profil sowohl von der privaten als auch dienstlichen Nutzung durch den Betroffenen zu erstellen.[311]

Um einprägsame Formulierungen zu präsentieren, wird in der Literatur zunehmend mit Begriffen operiert wie „Verbot der Totalüberwachung“ oder „Verbot der Erstellung umfassender Persönlichkeitsprofile“. Solche Begriffe sind für eine gesetzliche Regelung jedoch eher ungeeignet, da sie ihrerseits stark interpretationsbedürftig und tendenziell irreführend sind. Denn sowohl der Begriff „Totalüberwachung“[312] als auch der des „umfassenden Persönlichkeitsprofils“ legt Extremfälle nahe, die in der Praxis meist nicht erreicht werden. Selbstverständlich ist beides unzulässig. Aber die entscheidende Frage ist, inwieweit schon im Vorfeld des „Totalen“ oder des „Umfassenden“ Überwachung rechtswidrig sein soll. Diese Abwägung wird der Gesetzgeber nicht übernehmen können, sondern weiter den Gerichten überlassen.

Denkbar wäre aber eine Kombination aus Katalogen einerseits des eindeutig Unzulässigen ähnlich der „Blacklist“ im Anhang des UWG im Recht des unlauteren Wettbewerbs und andererseits von Vorgaben für die Gewichtung im Abwägungsprozess. Zwei *vorläufige Beispiele* sollen die Idee illustrieren:

Verboten ist

1. die verborgene und die intransparente Überwachung, es sei denn, dass wichtige Rechtsgüter akut und in erheblichem Umfang bedroht und mit milderen Mitteln nicht zu schützen sind.

Als besonders schwerwiegende Beeinträchtigung gilt insbesondere

1. das Zusammenführen von Ortungs- oder Handlungsdaten zu persönlichen Profilen

[308] VG Ansbach v. 16.3.2020 – AN 14 K 19.00464, ZD 2020, 607 (608).
[309] Ähnlich sieht es bei Systemen aus, die biometrische Merkmale des Personals nutzen, vgl. LAG Berlin-Brandenburg v. 4.6.2020 – 10 Sa 2130/19, NZA-RR 2020, 457: Ein biometrisches Zeiterfassungsystem ist in aller Regel nicht erforderlich im Sinne von Art. 9 Abs. 2 lit. b DSGVO, § 26 Abs. 3 BDSG.
[310] BAG v. 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327.
[311] BAG v. 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327 (1331) Rn. 33.
[312] *Körner*, NZA 2016, 1383 (1386); *Kort*, RdA 2018, 24 (25).

c) Psychologische Analysen

Der Hype um die Digitalisierung des Personalmanagements wird vorwiegend mit Blick auf neue Formen und Methoden des Recruiting unter Anwendung von KI und Big Data-Analysen diskutiert.[313] Der Unterschied etwa zum Thema „Smart Factory" ist hier, dass die Datenverarbeitung direkt auf die Person zielt und eine Anonymisierung oder ein Verbot der Zusammenführung von personenbezogenen Daten in der Regel widersinnig wäre. Hinzu kommt, dass der wissenschaftliche Anspruch, der hinter „People Analytics" steht,[314] Datenschutzbelangen diametral entgegensteht. Je präziser das Individuum durchleuchtet wird, desto besser die Chance, dass das perfekte Arbeitsverhältnis entsteht. Das ist jedenfalls die Botschaft des Hypes, keineswegs die herrschende Lehre im Personalmanagement. Klare Verbote invasiver Verfahren würden dort wohl nicht selten begrüßt.

Gesetzliche Verbote, bestimmte Daten zu ermitteln oder bestimmte Analysemethoden durchzuführen, wären hier vergleichsweise sinnvoll. Denn es bräuchte Standards, die allgemeine Bekanntheit genießen. Regelungen in Betriebsvereinbarungen oder Tarifverträgen nützen wenig, denn Bewerber*innen müssen wissen, welche Rechtsgrundlage in dem ihnen noch fremden Unternehmen gilt. Eine gesetzliche Neuregelung, die im Bereich Datenschutz im Bewerbungsverfahren stumm bleibt, wäre also eine herbe Enttäuschung.

Auch hier wäre eine „Blacklist" unzulässiger Fragen bzw. Verfahren eine sehr realistische Regelungsmöglichkeit. Eine solche müsste nicht zwingend direkt im Gesetz enthalten sein, sondern könnte auch Instanzen unterhalb der Gesetzgebung unter Beteiligung u. a. von Fachkreisen der Personalwissenschaften überantwortet werden.

4.2.3 BIG DATA/KI/DATENSCHUTZ DURCH TECHNIK

a) Big Data- und KI-Anwendungen

Big Data- und KI-Anwendungen werden wegen ihres hohen Datenbedarfs und der Undurchsichtigkeit ihrer Analyse kritisiert. In digitalisierten Betrieben ist die vollständige Vernetzung aller „Entitäten" – egal ob sachlichen Bestandteile oder menschliche Akteure – gerade die zentrale Strategie, um Effizienzgewinne zu erzielen.[315] Alle Aktivitäten der Beschäftigten sind in das planmäßige Geschehen informationstechnologisch fest eingebunden. Jede Abweichung fällt zwangsläufig auf. Die Überwachung des Menschen ist dabei nicht Ziel als solches – jedenfalls nicht im traditionellen Sinne. Es geht um die möglichst reibungslose Integration aller Systeme. Soweit dem Mensch dabei eine kreative Rolle zukommt, soll sein informationeller Beitrag wiederum vollständig in das Gesamtsystem eingespeist werden. Informationelle Selbstbestimmung erscheint hier als völliger Fremdkörper.

Auch auf die Beschäftigten in einer solchen Arbeitsstätte ist die Rechtsprechung des BAG anzuwenden, die eine umfassende Überwachung ausschließt. Mit den dort erfassten Daten wäre es in der Tat problemlos möglich, ein „nahezu umfassendes und lückenloses Profil"[316] von der Tätigkeit der Beschäftigten zu erstellen. Auch sensible Daten etwa zur körperlichen oder mentalen

[313] Vgl. etwa *Betz*, ZD 2019, 148; *Dzida*, NZA 2017, 541; *Kort*, NZA-Beilage 2016, 62.
[314] *Huff/Götz*, NZA-Beilage 2019, 73.
[315] Anschaulich bei *Hofmann*, ZD 2016, 12.
[316] BAG v. 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327 (1331) Rn. 33.

Leistungsfähigkeit werden dabei selbstverständlich erfasst. Angestrebte Wirklichkeit und rechtliche Grenzen stehen offensichtlich in klarem Widerspruch.

Wie unter diesen Bedingungen eine Beurteilung der Erforderlichkeit nach § 26 Abs. 1 Satz 1 und § 26 Abs. 3 BDSG ausgehen wird, steht noch in den Sternen. Klar ist, dass das Modernisierungs- und Rationalisierungsinteresse des Arbeitgebers großes Gewicht haben wird.[317] Aber häufig wird bei der erforderlichen Abwägung über mildere Mittel wie schnellstmögliche Löschung oder Anonymisierung der Daten, Begrenzung des Zugriffs oder der personenbezogenen Zusammenführung zu reden sein. Dass darüber geredet wird, sieht das Recht schon gegenwärtig mehrfach vor. Technische und organisatorische Maßnahmen sind nach Art. 24 und 32 DSGVO ohnehin zu ergreifen – spätestens im Rahmen der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, die bei fortgeschrittener Digitalisierung der Arbeitsprozesse unweigerlich zu erfolgen hat. Auch ein vorhandener Betriebsrat ist Punkt für Punkt zu beteiligen, um Regelungen zu treffen, die dem Persönlichkeitsrecht der Beschäftigten nach § 75 Abs. 2 BetrVG gerecht werden.

Die rechtlichen Instrumente liegen also bereit. Ein Rechtsdefizit ist insoweit nicht ersichtlich. Das Problem ist jedoch die ungeheure Menge an immer wieder anderen und neuen Datenverknüpfungen, die teils auch noch in der Black Box der KI verborgen sind, die eine bewusste und gezielte Anwendung der Schutzinstrumente stark erschwert.

b) Datenschutz durch Technik

Der Gegenentwurf heißt Datenschutz durch Technik. Die enorme Bedeutung der Technikgestaltung für einen wirksamen Beschäftigtendatenschutz unter den Bedingungen umfassender Digitalisierung ist jetzt mehrfach sehr deutlich geworden und wird quer durch die Literatur betont.[318] Es liegt auf der Hand, dass Technik in vielfacher Hinsicht die Ziele des Beschäftigtendatenschutzes unterstützen könnte. Das beginnt dabei, dass Technik so konfiguriert ist, dass sie bestimmte personenbezogene Daten nicht erhebt, die sie erheben könnte, oder mindestens nicht weitergibt oder verknüpft. Ein simples Beispiel wäre ein Assistenzsystem, das erforderliche Daten nur intern speichert und nicht im Netz ablegt. Weiter könnte ein Ziel technischer Entwicklung sein, dass erwünschte Resultate mit weniger personenbezogenen Daten erreicht werden können, z. B. auch indem eine frühzeitige Anonymisierung durchgeführt werden kann. Das „Vergessen" der Daten könnte ebenso eingebaut wie Transparenz für die Nutzer*innen, die durch Technik zu informationeller Selbstbestimmung ertüchtigt werden. Big Data und KI werden als selbsterklärende Systeme konzipiert.

Zu den zentralen Defiziten des geltenden Beschäftigungsdatenschutzes gehört, dass das Erfordernis einer datenschutzfreundlichen Technikgestaltung an keiner Stelle konkretisiert wird. Selbstverständlich gilt Art. 25 Abs. 1 DSGVO neben § 26 BDSG im Beschäftigtendatenschutz. Die Vorschrift ist aber sehr blass und abstrakt formuliert. Schon eine kleine Konkretisierung für die besonderen Bedürfnisse des Beschäftigungsdatenschutzes im nationalen Recht könnte durchaus eine neue Dynamik technischer Entwicklung lostreten.

[317] *Krause*, Forschungsbericht 482, 2017, 33 f.
[318] *Haußmann/Thieme*, NZA 2019, 1612 (1618); *Hofmann*, ZD 2016, 12 (17); *Hornung/Hofmann*, in: Hirsch-Kreinsen/Ittermann/Niehaus (Hrsg.), Digitalisierung industrieller Arbeit, 2. Aufl., 2018, S. 233 (248); *Nebel*, ZD 2018, 520 (524); *Weichert/Schuler*, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, S. 20 f.

Es fehlen aber nicht nur deutliche gesetzliche Gebote oder Anreize. Es fehlt auch die wissenschaftliche und administrative Infrastruktur, um entsprechende technische Entwicklung anzustoßen und zu bewerten. Im Betrieb könnte die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO in die Rolle einer Bewertungsinstanz für datenschutzfreundliche Technik hineinwachsen. Auch hier wären Anpassungen an den Beschäftigtendatenschutz vorzunehmen. Aber auch überbetrieblich sind Forschungs- und Entwicklungsanstöße notwendig und Institutionen, die die schnelle technische Entwicklung im Blick haben und zudem Technik prüfen und ggf. empfehlen können.[319]

4.2.4 MITBESTIMMUNG/PARTIZIPATION

Die Arbeitsrechtswissenschaften sind polarisiert und das zeigt sich aktuell besonders bei der Frage, ob die Mitbestimmungsrechte des Betriebsrats beim Beschäftigtendatenschutz einzuschränken oder auszudehnen seien (s. o. Kap. 3.2.7). Das tatsächliche Defizit liegt jedoch nicht bei der Formulierung des gesetzlichen Mitbestimmungstatbestandes in § 87 Abs. 1 Nr. 6 BetrVG. Der alte Streit, ob schon die „Eignung zur Überwachung" das Mitbestimmungsrecht auslöst, ist im Grunde obsolet. Denn im Zuge umfassender Digitalisierung dient tendenziell jedes personenbezogene Datum, das im Betrieb erfasst wird, zugleich einer spezifischen Funktion und zugleich der Überwachung. Der digitalisierte Betrieb ist eine sich selbst in allen dazugehörigen Entitäten überwachende Maschinerie, in der jedes beliebige erhobene Datum jederzeit Bedeutung bekommen kann. Aber selbst unterhalb dieser vielleicht noch futuristischen Vorstellung bringt es keiner Seite irgendeinen Gewinn, wenn vor der Ausübung der Mitbestimmung angesichts hochkomplexer technischer Strukturen aufwändig und unter erheblicher Unsicherheit zu klären ist, welche Datenverarbeitung in welchen Teilen überwachende Funktion hat und welche nicht.

Das Rechtsdefizit liegt auf einer anderen Ebene. Angesichts der Wucht zunehmender Datenverarbeitung muss *die Technik* als solche nicht nur datenschutzfreundlich, sondern auch *mitbestimmungsfreundlich* ausgestaltet werden. Bereits bei der Konstruktion der datenerfassenden Technik müssen die Belange des Datenschutzes, aber auch die Bedürfnisse, die Technik durch Mitbestimmung zu beherrschen, berücksichtigt werden. Das bedeutet vor allem, dass in die Technik Transparenz und zuverlässige Stellschrauben einer datenschutzgerechten Anpassung eingebaut werden.

Technik muss dann auch als datenschutzfreundlich erkennbar sein. Durch Zertifizierung könnte nachgewiesen werden, dass dort, wo „Privacy by Design" draufsteht, auch die erwartete Technik drin ist.[320]

Mitbestimmung endet, wo Betriebs- oder Personalräte nicht installiert sind. Dann gilt es besonders, einzelne Beschäftigte durch tatsächliche Transparenz zu unterstützen. Erneut ist Technik gefragt, die Transparenz gleich mitliefert oder den Beschäftigten einen zuverlässigen Überblick über die maßgebliche Datenlage erlaubt. So wird vorgeschlagen, dass „Privacy Dashboards" für jeden Beschäftigten jederzeitige Transparenz über die zur eigenen Person verarbeiteten Daten und – soweit gewünscht – auch Lösch- und Einflussmöglichkeiten herstellen.[321] Voraussetzung ist allerdings, dass die gesamte betriebliche Infrastruktur damit harmoniert.

[319] *Weichert/Schuler*, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, S. 24 empfehlen ein Kompetenzzentrum beim BMAS.
[320] *Weichert/Schuler*, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, S. 21.
[321] *Tolsdorf/Bosse/Dietrich/Feth/Schmitt*, DuD 2020, 176.

Bei den Fragen sowohl einer wirksamen Mitbestimmung als auch einer zumutbaren individuellen Partizipation sind also vorrangig technische Ressourcen gefragt. Das Recht muss diese ermöglichen und fördern.

4.2.5 DIGITALISIERUNG DES ARBEITSSCHUTZES

Weitere Defizite, die in der bisherigen Diskussion zum Regelungsbedarf (siehe 4.1) nur ganz am Rande zur Sprache gekommen sind, betreffen den Datenschutz im Arbeitsschutz. Dieser Punkt ist hier daher zu ergänzen.

Im Gegensatz zum Personalmanagement interessiert sich das Arbeitsschutzmanagement traditionell weniger für das Individuum, sondern vielmehr für den Arbeitsplatz und die dort auftretenden Gefährdungen. Wer auf dem jeweiligen Arbeitsplatz sitzt, ist meist nebensächlich, so dass die Daten vielfach anonym erhoben werden können. Eine Digitalisierung des Arbeitsschutzes muss daher keineswegs zwangsläufig mit einem sprunghaften Ansteigen der Verarbeitung personenbezogener Daten einhergehen.

Allerdings ist gerade der Arbeitsschutz auf ein hohes Maß an betrieblicher Kommunikation angewiesen, um im Verhalten aller Beteiligten permanent auf aktuellem Erfahrungsstand Beachtung zu finden. Es gibt zudem aktuelle Entwicklungen, die diese Einschätzung deutlich in Frage stellen. Erstens lässt die verschärfte Einbeziehung psychischer Gefährdungen die persönlichen Belange der Beschäftigten stärker in den Vordergrund treten. Zwar wird versucht, auch bei der Beurteilung psychischer Gefährdungen den Arbeitsplatz und nicht die Person in den Mittelpunkt zu stellen. Bei der Ermittlung ist jedoch die Beobachtung individueller psychischer Reaktionen (z. B. per Fragebogen) kaum verzichtbar. Zweitens stattet der digitale Arbeitsschutz die Beschäftigten zunehmend mit individualisierten Assistenzgeräten aus, die die Arbeit erleichtern und sicherer machen, dabei aber entweder sensible individuelle Daten produzieren oder auch benötigen, um optimal assistieren zu können (zu allem Kap. 1). Da den Entwicklern solcher Systeme auch der Mensch als Störfaktor gilt,[322] ist durchaus naheliegend, dass auch aus Sicherheitsgründen das menschliche Verhalten eng kontrolliert wird. Hier liegen auch Risiken, das Gesundheitsdaten und Leistungsdaten nicht mehr sauber getrennt werden.

Im Unterschied zur digitalen Optimierung der Mensch-Maschine-Interaktion oder zum digitalen Personalmanagement steht der Arbeitsschutz dem Datenschutz keineswegs konträr gegenüber. Alle Seiten haben hier ein gemeinsames Interesse, die Belange zu harmonisieren. So könnten die meisten Daten im Bereich psychischer Belastungen vielfach umgehend anonymisiert werden, ohne ihren Wert zu verlieren. Verbleibende Dokumentationspflichten könnten datenschutzrechtlich modifiziert werden. Assistenzsysteme können in aller Regel auch unvernetzt funktionieren. Das Exoskelett muss zwar Daten über den Benutzer erfassen, diese aber nicht unbedingt anderen zur Verfügung stellen. Sicherlich gibt es Konflikte, z. B. beim Einsatz von Kameratechnik,[323] die sich aber wohl technisch beherrschen ließen. Auch gilt es Datenbestände sorgfältig zu trennen. Die sensiblen Daten des Arbeitsschutzes sollten nicht in die Personalbeurteilung geraten. Technisch-organisatorische Lösungen hierzu wären zu verfeinern.

[322] *Evers/Krzywdzinski/Pfeiffer*, Arbeit 2019, 3 (23).
[323] *Rose*, Festschrift für Jürgen Taeger, 394 (406 ff.).

Ein großes Problem ist aber das *geringe Problembewusstsein* im Arbeitsschutz. Da hier die besonders hochrangigen Belange Leben und Gesundheit vertreten werden, erscheinen entgegenstehende Belange des Datenschutzes als vernachlässigbar. Dies muss und kann auch geändert werden, indem der Datenschutz in die Regelungen des Arbeitsschutzes explizit und durchgehend aufgenommen wird. Das wird sich vor allem auch dann aufdrängen, wenn sich bestätigt, dass Datenschutz gleichzeitig Gesundheitsschutz fördert. Denn Überwachung hat zweifellos psychische Auswirkungen, die im Einzelfall sicher auch problematisch sind.

Insoweit kann hier das Fehlen von spezifischen Datenschutzregelungen in Gesetzen, Verordnungen und Regelwerk als weiteres Defizit der Rechtslage verbucht werden. Insbesondere könnte es helfen, den Arbeitsschutzausschüssen aufzugeben, im Technischen Regelwerk Datenschutzbelange systematisch zu berücksichtigen.

4.3 ERGEBNIS

In der Diskussion um Regelungsdefizite des geltenden Beschäftigtendatenschutzes und Regelungsvorschläge für die Zukunft steht der Wunsch nach einem effektiveren *Datenschutz durch Technik* deutlich im Vordergrund. Daneben spielt der Wunsch nach klareren Vorschriften bis hin zu einem eigenständigen Beschäftigtendatenschutzgesetz angesichts der äußerst komplexen und oft unklaren Rechtslage auch eine erhebliche Rolle. Klare Regelungen, was vor allem auf dem Gebiet der Überwachung von Beschäftigten oder der psychologischen Analyse von Daten im Bewerbungsverfahren erlaubt ist bzw. nicht erlaubt ist, werden vielfach angemahnt. Lösungen für die Überforderung kollektiver und individueller Partizipation durch die Breite und Geschwindigkeit der Digitalisierung werden gesucht.

Vier Schwerpunkte der Fachdebatte konnten identifiziert werden:

1. Rechtsklarheit/einheitliches Gesetz
2. Überwachung/psychologische Analysen
3. Big Data/KI/Datenschutz durch Technik
4. Mitbestimmung/Partizipation

Ein fünfter Schwerpunkt sollte hinzutreten: Digitalisierung des Arbeitsschutzes mit erheblichem Regelungsbedarf auf dem Feld des Datenschutzes.

Der gesetzliche Beschäftigtendatenschutz ist derzeit zersplittert, teils irreführend und teils zu abstrakt geregelt. Die wenigen speziellen Vorschriften bedürfen zumindest einer zutreffenden und allgemeinverständlichen Neuformulierung. Auch die Transparenz- und Organisationsgebote der DSGVO wären für den Beschäftigtendatenschutz zu spezifizieren. Die Einheit aus materialen und prozeduralen Regelungen, die gemeinsam den Beschäftigtendatenschutz bilden, muss deutlich werden.

Die Möglichkeit der zuverlässigen Datentrennung nach verschiedenen Zwecken wäre eine wichtige Voraussetzung, die Digitalisierung der Produktion bzw. Dienstleistungstätigkeit sowie des Personal- und des Arbeitsschutzmanagements datenschutzfreundlich zu ermöglichen. Klarere Regelungen der Zweckbindung und der Zweckänderung als jene der DSGVO bzw. des BDSG könnten dabei sehr hilfreich sein.

Bestimmte Anwendungen technischer Errungenschaften stehen so deutlich im Widerspruch zu den Zielen des Datenschutzes, dass ein Verbot ausgesprochen werden kann. Das z. B. trifft für

bestimmte Überwachungspraktiken oder Bewerberanalysen zu. Eine Verbotsliste („Blacklist“), die die Abwägung im Einzelfall für bestimmte technische Verfahren durch eine Untersagung des Gesetzgebers ersetzt, ist möglich. Andere Praktiken der Datenverarbeitung könnten jedenfalls als „schwerwiegende Beeinträchtigung“ gelistet werden, was bei Abwägungsprozessen ins Gewicht fiele. Anstelle des Gesetzgebers könnten mit der Aktualisierung solcher Listen auch gesetzlich gebildete Fachgremien beauftragt werden.

Es fehlt an datenschutzfreundlicher Technik, an Maßstäben, was von einer solchen Technik erwartet wird, und an Institutionen, die diese Technik bewerten und ggf. empfehlen. Die Schaffung dieser Voraussetzungen würde die betriebliche Praxis erheblich erleichtern und nicht zuletzt die Mitbestimmungsverfahren deutlich verbessern und beschleunigen können. Dazu bedarf es Forschung, Entwicklung, Zertifizierung und vom Gesetzgeber unterstützende Regelungen.

5. REGELUNGSPERSPEKTIVEN

Im Hinblick auf ein künftiges Beschäftigtendatenschutzgesetz ist unter Expert*innen fast alles streitig. Nicht nur viele Detailfragen werden unterschiedlich beurteilt. Auch die Frage, ob überhaupt ein eigenständiges Beschäftigtendatenschutzgesetz sinnvoll ist und – mehr noch – ob ein solches mit Blick auf die europaweit unmittelbar geltende DSGVO überhaupt rechtlich zulässig ist, ist Gegenstand des Meinungsstreits.

Einigkeit besteht wohl noch hinsichtlich des Wunsches, dass eine für die Praxis klare und übersichtliche Gesetzeslage angestrebt wird. Klare Gesetze mit niedrigem Interpretationsbedarf sind leichter zu befolgen. Unglücklich sind Doppel- oder gar Dreifachregelungen. So wäre ein Beschäftigtendatenschutzgesetz sehr problematisch, das in zahlreichen Fragen dazu zwingt, zusätzlich die DSGVO und womöglich auch noch das BDSG zur Hand zu nehmen, insbesondere wenn dann Widersprüche zwischen den verschiedenen Regelwerken zu Tage träten.

Denkbar wäre, dass der Gesetzgeber

- sich darauf beschränkt, § 26 BDSG und wenige andere arbeitsrechtliche Vorschriften inhaltlich durch einige Klarstellungen zu überarbeiten und gezielt um vordringliche Punkte zu erweitern; parallel hätte dann Anwender*innen die Grundsätze nach Art. 5 DSGVO, die Rechte der betroffenen Person (Art. 12 ff. DSGVO) und die Pflichten der Verantwortlichen (Art. 24 ff. DSGVO) aus der DSGVO mitzulesen;
- ein knappes eigenständiges Regelwerk innerhalb oder außerhalb des BDSG schafft, das viele eigene Regelungen, aber ohne Anspruch auf Vollständigkeit trifft und ansonsten daher in die DSGVO verweist;
- ein eigenes Regelwerk mit Anspruch auf Vollständigkeit schafft, auch wenn bei verbliebenen Lücken immer ergänzend die DSGVO anzuwenden ist.

Die letzte Lösung wäre sicherlich die eleganteste und für die Praxis übersichtlichste, wenn sie denn europarechtlich Anerkennung fände und nicht jede enthaltenen Abweichung von der DSGVO ständig als europarechtswidrig angezweifelt würde.

Bevor also Regelungsperspektiven abschließend eingeschätzt werden (5.2), soll es um den Regelungsspielraum für ein nationales Beschäftigtendatenschutzgesetz gehen (5.1).

5.1 REGELUNGSSPIELRAUM

EU-rechtliche betrachtet ist die Antwort auf die Frage nach dem Regelungsspielraum durch Auslegung der Öffnungsklausel in Art. 88 DSGVO zu finden. Es geht um die Formulierung, dass die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen *spezifischere Vorschriften* zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen können.

5.1.1 RECHTSPRECHUNG

Letztlich ist es Aufgabe des EuGH, die Vorschriften der DSGVO verbindlich auszulegen. Im allgemeinen dauert es Jahre, bis das dann irgendwann geschieht. Aber zur Auslegung des Art. 88 DSGVO liegt seit dem 21.12.2020 bereits ein Vorlagebeschluss des VG Wiesbaden an den EuGH vor, so dass es überraschend schnell gehen könnte, dass dieser wichtige Fragen verbindlich klärt.[324]

Dem Gerichtshof der Europäischen Union werden vom VG Wiesbaden nach Art. 267 AEUV folgende Fragen zur Vorabentscheidung vorgelegt:

- Ist Art. 88 Abs. 1 der Verordnung (EU) 2016/679 dahin auszulegen, dass eine Rechtsvorschrift, um eine spezifischere Vorschrift zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext im Sinne des Art. 88 Abs. 1 der Verordnung (EU) 2016/679 zu sein, die an solche Vorschriften nach Art. 88 Abs. 2 der Verordnung (EU) 2016/679 gestellten Anforderungen erfüllen muss?
- Kann eine nationale Norm, wenn diese die Anforderungen nach Art. 88 Abs. 2 der Verordnung (EU) 2016/679 … offensichtlich nicht erfüllt, trotzdem noch anwendbar bleiben?

Es geht also hauptsächlich um die Berücksichtigung von Art. 88 Abs. 2 DSGVO. Doch mit Aussagen des EuGH zum gesamten Regelungsspielraum, den Art. 88 DSGVO bietet, kann dennoch gerechnet werden.

Dem VG Wiesbaden geht es um zwei Vorschriften des Hessischen Landesdatenschutzes, deren Anwendbarkeit das Gericht vor dem Hintergrund von Art. 88 DSGVO bezweifelt. Besonders brisant ist die Vorlage dadurch, dass eine diese Vorschriften (§ 23 Abs. 1 Satz 1 HDSIG) wortgleich mit § 26 Abs. 1 Satz 1 BDSG, also mit der Grundnorm des Beschäftigtendatenschutzes auf Bundesebene und für die Privatwirtschaft, formuliert ist. Der EuGH wird also mittelbar über das Herzstück des gegenwärtigen Beschäftigtendatenschutzrechts zu entscheiden haben.

Die Begründung des VG Wiesbaden liest sich wie eine scharfe Kritik an § 23 Abs. 1 Satz 1 HDSIG = § 26 Abs. 1 Satz 1 BDSG. Das Gericht erklärt ausdrücklich, dem BAG nicht folgen zu wollen, das davon ausgegangen ist, dass es bei § 26 Abs. 1 Satz 1 BDSG ohne Vorabentscheidungsverfahren durch den Gerichtshof der Europäischen Union mangels vernünftiger Zweifel von einer richtigen Anwendung des Unionsrechts durch den Gesetzgeber offenkundig ausgehen könne.[325] Das VG hegt hingegen Zweifel,[326] da die in Art. 88 Abs. 2 DSGVO gestellten Anforderungen weder in der Norm selbst, noch durch ergänzende Normvorgaben an anderer Stelle des jeweiligen Gesetzes erfüllt worden seien (Rn. 21). Der nationale Gesetzgeber sei insbesondere der in Abs. 2 geforderten Berücksichtigung von Überwachungssystemen am Arbeitsplatz nicht nachgekommen (Rn. 33). Das Regelwerk selbst müsse angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen (Rn. 35).

[324] VG Wiesbaden, Beschl. v. 21.12.2020 – 23 K 1360/20.WI.PV, BeckRS 2020, 40028.
[325] BAG, Beschl. v. 7.5.2019 – 1 ABR 53/17, NZA 2019, 1218 (1223), Rn. 48.
[326] VG Wiesbaden, Beschl. v. 21.12.2020 – 23 K 1360/20.WI.PV, BeckRS 2020, 40028, Rn. 21, 33, 35.

5.1.2 FACHLITERATUR

Bis der EuGH entscheidet, steht nur die in der Fachliteratur veröffentlichte Expertise zur Verfügung, um den Regelungsspielraum für ein nationales Beschäftigtendatenschutzgesetz auszumessen. In der Kommentarliteratur zu Art. 88 DSGVO findet sich ein breites Meinungsspektrum, dass im Folgenden in jeweils knapper Zusammenfassung wiedergegeben wird. Eine Vorsortierung von weitem zu engem Spielraum ist dabei bereits vorgenommen worden.

Thüsing und Traut kommen nach ausführlicher Auslegung des Wortlautes, der Systematik und der Entstehungsgeschichte zu dem Schluss, dass die Mitgliedsstaaten den Beschäftigtendatenschutz umfassend regeln können.[327] Im Anwendungsbereich dieser Regelung entfalle der Anwendungsvorrang der DSGVO,[328] die allerdings subsidiär gelte, wenn national nur Teilregelungen getroffen würden.[329] Eine Bindung an das Schutzniveau der DSGVO bestehe nicht, sondern an die in Art. 88 Abs. 2 DSGVO definierten Standards, also insbesondere an die europäischen Grundrechte.[330]

Ähnlich äußert sich *Riesenhuber*, demzufolge die Mitgliedstaaten einen eigenen Regelungsspielraum hätten, den sie mit Rücksicht auf die besonderen Sachgesetzlichkeiten des Beschäftigungsverhältnisses kreativ ausfüllen könnten. Dabei sollten sie sich gerade auch berufen fühlen, innovative Schutzmechanismen zu entwickeln, die der Beschäftigungskontext eröffne.[331] Die DSGVO sehe dafür weder ein generelles „Absenkungsverbot" noch einen „Höchststandard" vor.[332]

Auch *Forst* sieht einen weiten Korridor für nationale Regelungen des Beschäftigtendatenschutzes mit erheblichen Abweichungsmöglichkeiten von den Vorgaben der DSGVO „nach unten" und „nach oben".[333]

Zöll betont die Einschätzungsprärogative des Gesetzgebers für sachlich begründete Abweichungen mit nicht unbegrenztem Spielraum „nach oben" und unter Wahrung des Datenschutzniveaus der DSGVO auch „nach unten".[334]

Tiedemann geht zwar von einer „echten Öffnungsklausel" für mitgliedschaftliche Regelungen aus, die allerdings das Mindestdatenschutzniveau der DSGVO nur verbessern bzw. erhöhen dürften.[335]

Pauly betont, dass kein beliebiges Abweichen vom Sinn und Zweck der übrigen Bestimmungen der DSGVO zulässig sei. Durch den Verzicht auf die im Kommissions*entwurf* vorgesehene Zulässigkeit von Abweichungsmöglichkeiten lediglich „in den Grenzen dieser Verordnung" werde aber verdeutlicht, dass die DSGVO für den Beschäftigtendatenschutz lediglich einen Mindeststandard vorsehe und es den Mitgliedstaaten freistehe, ein „Mehr" an Datenschutz einzuführen.[336]

[327] Schwartmann et al./*Thüsing/Traut*, 2. Aufl., 2020, DS-GVO Art. 88 Rn. 19.
[328] Ebenda, Rn. 13.
[329] Ebenda, Rn. 20.
[330] Ebenda, Rn. 38.
[331] BeckOK DatenschutzR/*Riesenhuber*, 33. Ed. 1.5.2020, DS-GVO Art. 88 Rn. 69.
[332] Ebenda, Rn. 71 f.
[333] Auernhammer/*Forst*, 7. Aufl., 2020, DSGVO Art. 88 Rn. 18.
[334] Taeger/Gabel/*Zöll*, 3. Aufl., 2019, DS-GVO Art. 88 Rn. 21.
[335] Sydow/*Tiedemann*, 2. Aufl., 2018, DSGVO Art. 88 Rn. 3.
[336] Paal/Pauly/*Pauly*, DS-GVO Art. 88 Rn. 4.

Auch *Stamer* und *Kuhnke* folgern, dass Art. 88 Abs. 1 in Bezug auf spezifischeres nationales Recht lediglich Mindeststandards aufgeben wolle und darüber hinaus nationales Recht zulasse.[337]

Nach *Däubler* und *Wedde* gebe die DSGVO ein Mindestniveau vor, das überschritten werden dürfe. Allerdings sei eine Verstärkung des Schutzes im Vergleich zur DSGVO nur zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der Beschäftigten (Art. 88 Abs. 2 DSGVO) zulässig.[338]

Seifert vertritt prinzipiell eine enge Bindung an die DSGVO, da „spezifischere" Regelungen und nicht etwa „abweichende" (wie in Art. 85 Abs. 2 DSGVO) zugelassen würden, Spezifischere Vorschriften gingen allerdings nicht selten über die allgemeinen Regeln der DSGVO für den Bereich des Beschäftigtendatenschutzes hinaus und würden infolgedessen zwangsläufig auch Abweichungen von der Verordnung „nach oben" enthalten.[339]

Im Ergebnis ganz ähnlich sieht *Selk* wegen des Harmonisierungsanspruchs der DSGVO relativ wenig Spielraum. „Spezifischer" heiße, dass eine nationale Regelung die Regelungen der Verordnung aufgreifen müsse, aber „spezifizieren", also für bestimmte Einzelfälle speziellere Regelungen vorsehen dürfe.[340] Jedenfalls dürfe das Schutzniveau der DSGVO nicht unterschritten und „nur spezifizierend" überschritten werden.[341]

Die deutlichste Gegenposition vertritt *Maschmann*, der dem Begriff „spezifischere Vorschriften" in Art. 88 Abs. 1 DSGVO entnimmt, dass nur nationale Regelungen möglich sein sollen, mit denen die Mitgliedstaaten die allgemeinen Vorgaben der DSGVO für den Beschäftigtendatenschutz präzisieren und konkretisieren, aber nicht verschärfen dürften. Auch für diesen Bereich gelte das Prinzip der Vollharmonisierung, so dass das vorgegebene Niveau der DSGVO auch für den Beschäftigtendatenschutz verbindlich sei.[342]

Ähnlich formuliert *Pötters*, dass wegen des Anspruchs der Vollharmonisierung eine Öffnungsklausel ausdrücklich „Abweichungen" zulassen müsse, im Übrigen seien auf nationaler Ebene lediglich konkretisierende Regelungen zulässig.[343] Art. 88 DSGVO lasse aber keine Abweichungen zu, sodass vom materiellen Schutzstandard der DS-GVO nicht abgewichen werden dürfe, wohl aber dürften „gewisse Sonderwege im Hinblick auf formelle Aspekte" möglich sein.[344]

Ganz entsprechend betont *Franzen* den Aspekt des vollharmonisierenden Anspruchs der DSGVO, wonach keine Abweichungen von ausdrücklichen Vorgaben der DSGVO, sondern nur Konkretisierungen zuzulassen sind.[345]

Diese Liste ließe sich durch zahlreiche Beiträge aus Fachzeitschriften noch erheblich verlängern. Es geht aber hier nicht darum abzuzählen, welche Ansicht in der Mehrheit sein könnte. Die Botschaft der Analyse ist vielmehr, dass das Meinungsspektrum erstens sehr bunt und uneinheitlich ist. Es gibt kaum zwei Kommentare mit der gleichen Ansicht. Es ist aber zweitens nicht stark polarisiert, denn die größte Gruppe formuliert eine mittlere Linie. Mit etwas gutem Willen lassen sich die Autor*innen in drei Gruppen sortieren. Gruppe 1 sieht großen Spielraum des Gesetzge-

[337] Plath/*Stamer/Kuhnke*, 3. Aufl., 2018, DSGVO Art. 88 Rn.
[338] Däubler et al./*Däubler/Wedde*, 2. Aufl., 2020, DSGVO Art. 88 Rn. 14 f.
[339] Simitis/Hornung/Spiecker gen. Döhmann/*Seifert*, 1. Aufl., 2019, DSGVO Art. 88 Rn. 22 f.
[340] Ehmann/Selmayr/*Selk*, 2. Aufl., 2018, DS-GVO Art. 88 Rn. 71.
[341] Ebenda Rn. 75 f.
[342] Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, DS-GVO Art. 88 Rn. 40.
[343] Gola/*Pötters*, 2. Aufl., 2018, DS-GVO Art. 88 Rn. 3.
[344] Ebenda, Rn. 27.
[345] EuArbRK/*Franzen*, 3. Aufl., 2020, DS-GVO Art. 88 Rn. 10 f.

bers, der den Beschäftigtendatenschutz nahezu unbehelligt – abgesehen von Art. 88 Abs. 2 – von der DSGVO regeln kann. Gruppe 3 sieht einen engen rechtlichen Käfig des vollharmonisierenden Anspruchs der DSGVO und will daher spezifischere Regelungen nur in Abgrenzung zu abweichenden oder verschärfenden Regelungen zulassen. Die mittlere Gruppe 2 sieht mit gewissen Unterschieden erheblichen Regelungsspielraum für den Beschäftigtendatenschutz insbesondere oberhalb des Niveaus der DSGVO.

Triftige Argumente werden auf beiden Polen der Debatte genannt. Einerseits spricht für einen engen Spielraum der Vollharmonisierungsanspruch der DSGVO und der Umstand, dass es in Art. 88 Abs. 1 DSGVO „spezifischere Regelungen" und nicht wie in Art. 85 Abs. 2 DSGVO „Abweichungen" bzw. „Ausnahmen" heißt. Andererseits spricht für einen weiten Spielraum, dass in der Entstehungsgeschichte der DSGVO die Formulierung „in den Grenzen dieser Verordnung" fallen gelassen worden ist und Abs. 2 nur Sinn ergibt, wenn es gilt für Abweichungen eine untere Grenzlinie einzuziehen. Da aber nicht beide Meinungen gleichzeitig zum Zuge kommen können, ist über Wortlaut, Systematik und Formulierungsgeschichte noch hinauszuschauen.

Der europäische Gesetzgeber hat den nationalen Gesetzgebungsorganen mit Art. 88 DSGVO Handlungsmöglichkeiten eröffnet. Er hat das Regelungsfeld als bedeutsam erkannt, sich aber zu einer angemessenen speziellen Regelung des Feldes nicht in der Lage gesehen. Das mag teils an unüberbrückbaren Differenzen, teils an der Einsicht gelegen haben, dass die nationalen Interessen und Voraussetzungen zu unterschiedlich sind, um den Bereich einheitlich zu regeln. Unter diesen politischen Umständen kann es hilfreich sein, wenn auf nationaler Ebene mit unterschiedlichen Vorstellungen experimentiert wird, um zu einem späteren Zeitraum auf erweiterter Erkenntnisgrundlage eventuell einen neue Regelungsversuch zu starten. Das wäre jedenfalls eine rationale und in die Zukunft gerichtete Interpretation des Kompromisses, der hinter der Öffnungsklausel steckt. Es geht nicht nur um den Erlass von Durchführungsbestimmungen, sondern es gibt einen gewissen Regelungs- und Erprobungsspielraum.

Zwar kann der nationale Gesetzgeber auf die Formulierung „spezifischerer Regelungen" im Beschäftigtendatenschutz verzichten und dieses Feld damit der Rechtsprechung zur DSGVO sowie den Kollektivvertragsparteien ganz oder teilweise überlassen. Aber wenn er tätig wird, dann hat er für die jeweiligen Regelungsgegenstände *„geeignete und besondere Maßnahmen"* unter Abwägung der in Art. 88 Abs. 2 DSGVO genannten Grundwerte zu finden. Das ist ohne einen gewissen Regelungsspielraum gar nicht vorstellbar. Denn zugelassen wird hier durch die DSGVO eine konkretisierende Ausformulierung des Rechts nicht allein durch das Rechtssystem, sondern durch die politisch-demokratischen Instanzen der Legislative. In der Kommentarliteratur betont *Zöll* sehr zutreffend die *Einschätzungsprärogative des Gesetzgebers*[346], der im öffentlichen Meinungskampf nach Kompromissfindung und unter parlamentarischer Beschlussfassung zu eigenen Lösungen kommen muss, was unter den jeweiligen aktuellen Bedingungen geeignete und besondere Maßnahmen sind. Bei der Beurteilung, was geeignet ist, müssen auch Erfahrungen, die seit Beschluss der DSGVO gemacht worden sind, einfließen. Mit Art. 88 DSGVO ist der Beschäftigtendatenschutz nicht auf den Erkenntnisstand der europäischen Gesetzgebungsorgane vom 27. April 2016 festgefroren. Vielmehr muss jeweils aktuell politisch, ökonomisch, technisch (weniger rechtlich) beurteilt werden, was an Schutzregelungen zur Wahrung der in Abs. 2 genannten Grundwerte erfolgversprechend ist.

[346] Taeger/Gabel/*Zöll*, 3. Aufl., 2019, DS-GVO Art. 88 Rn. 21.

Der Ball liegt also *im Feld der Politik*. Die DSGVO diktiert kein Beschäftigtendatenschutzgesetz. Es sind jetzt auch nicht vorrangig Jurist*innen gefordert. Genauso wenig wie der Klimaschutz vorrangig eine Sache juristischer Expertise ist, ist dies auch der Datenschutz im Beschäftigungsverhältnis nicht.

Das heißt, dass die Akteure des Arbeitsschutzes diskutieren sollten, wieviel Datenschutz in ihrem Bereich möglich und vernünftig ist. Die Akteure des Personalwesens sollten dies für ihren Bereich tun. Die technischen Berufe sind aufgerufen zu klären, wieviel „Privacy by Design" machbar ist. Die Sozialpartner sind gefragt, ihre Interessengegensätze genauer zu bestimmen und nach Win-win-Lösungen zu forschen. Das alles ist nötig, um zu Regelungen zu kommen, die von der Praxis auch als eigene Regelungen getragen werden können.

Erst gegen Ende dieser Diskussion, wenn es um die konkrete Formulierung von Vorschriften geht, ist tatsächlich juristischer Sachverstand gefragt. Dabei kann dann auch ernst genommen werden, dass ein mögliches Beschäftigtendatenschutzgesetz von einem erheblichen Teil der juristischen Fachwelt sehr eng an den Vorgaben bzw. am Datenschutzniveau der DSGVO gemessen werden wird. Zwar ist diese Meinung nicht herrschend, aber doch relevant. In gerichtlichen Konflikten wird sie sicher eine Rolle spielen. Vertreten wird, dass der nationale Gesetzgeber den Beschäftigtendatenschutz präzisieren und konkretisieren, aber nicht verschärfen dürfe.[347] Damit ist sicherlich nicht gemeint, dass die praktische Durchführung des Beschäftigtendatenschutzes nicht verschärft werden darf. Denn jede Konkretisierung zielt ja selbstverständlich auf eine Verbesserung der praktischen Anwendung eines rechtlichen Standards. Jede Konkretisierung muss, sonst wäre sie wohl unzulässig, das *praktische* Datenschutzniveau verbessern. Zu vermeiden wäre nach dieser Auffassung aber, dass Verschärfungen, die nicht aus Konkretisierungen hervorgehen, auf der abstrakt-allgemeinen Ebene formuliert werden.

Das soll keineswegs bedeuten, dass ein eigenes Regelwerk mit Anspruch auf Vollständigkeit nicht möglich ist. Es sollte aber im Interesse möglichst breiter Unterstützung dabei darauf geachtet werden, dass es sich gleichzeitig als (im etwas engeren Sinne) „Spezifizierung" der in der DSGVO vorhandenen Instrumente darstellt und sich nicht in deutlichen Widerspruch zum dort vorgegebenen Datenschutzniveau setzt. Konkreter und damit wirkungsvoller, soviel Einigkeit besteht wohl, dürfen bzw. sollen die nationalen Regelungen auf jeden Fall sein.

5.2 INHALTLICHE REGELUNGSPROJEKTE

In Kap. 4 sind bereits viele konkrete Regelungsbedarfe bzw. Regelungsoptionen angesprochen worden, die hier nicht alle wiederholt werden sollen. Stattdessen werden hier zwei inhaltliche Regelungsprojekte etwas präziser skizziert. Im Anschluss folgen unter 5.3 zwei technisch-organisatorische Regelungsprojekte zur Verbesserung der praktischen Durchsetzung des Beschäftigtendatenschutzes.

Wie unter 5.1 betont, kann keines dieser Regelungsprojekte allein mit juristischem Sachverstand überzeugende Lösungen hervorbringen. Allerdings können aus juristischer Perspektive die Erfahrungen mit bestimmten Regelungsmodellen aus anderen Rechtsbereichen herangezogen werden. In Kap. 4.2.2. ist bereits das Regelungsmodell der „Blacklist" aus dem UWG als mögliches Vorbild betrachtet worden. Mehr noch könnten bewährte Verfahren aus dem Arbeitsschutz (wie

[347] Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, DS-GVO Art. 88 Rn. 40.

die Gefährdungsbeurteilung im Betrieb oder die Formulierung Technischer Regeln durch Arbeitsschutzausschüsse beim BMAS) auch für den Beschäftigtendatenschutz als Vorbild dienen.

5.2.1 DATENSCHUTZ IM PERSONALMANAGEMENT

Nach § 26 Abs. 1 Abs. 8 Satz 1 BDSG gelten Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis als Beschäftigte im Sinne des BDSG. Die Mitgliedsstaaten können nach Art. 88 Abs. 1 DSGVO insbesondere auch schon „für Zwecke der Einstellung" spezifischere Vorschriften vorsehen. Die Öffnungsklausel erlaubt also auch schon, den Datenschutz der Bewerber*innen, die also noch nicht in einem Arbeitsverhältnis zum verantwortlichen Arbeitgeber stehen, auf nationaler Ebene spezifisch zu regeln.[348] Darüber hinaus ist es sinnvoll, dass gesetzliche Regelungen auch künftig, wie bisher schon in § 26 Abs. 1 BDSG, nach Bewerber*innendaten und Beschäftigtendaten unterscheiden.

a) Recruiting

Beim Recruiting spricht wenig dagegen, dass für alle Unternehmen gleichermaßen verbindlich klare und eindeutige Regeln existieren, die vieles von dem, was technisch möglich ist, ausschließen. Denn weder der gesellschaftliche noch der unternehmerische Fortschritt durch Digitalisierung entscheidet sich daran, dass zügellos nach Daten bei Gewinnung und Auswahl von Bewerber*innen gefischt werden darf. Die weitere Digitalisierung der Arbeit ist auf Recruiting 4.0 nicht angewiesen.

Spielerische Bewerbungsformen im Netz, die auch den Kandidat*innen eine angemessene Gelegenheit geben, sich mit den Anforderungen verfügbarer Arbeitsplätze vertraut zu machen und das Unternehmen kennenzulernen, können ähnlich wie traditionelle Assessment-Center zu beiderseitigem Vorteil sein. Solange Bewerber*innen informiert werden, welche Aktivitäten in welcher Weise auswahlrelevant sind, kann das zulässig sein. Aber ausforschende psychologische Tests oder Sprachanalysen, erstrecht wenn sie etwa auf Grundlage eingesandter Videos heimlich erfolgen, können und sollten verboten werden. Eine Einwilligung in bestimmte Erhebungsverfahren ist im Bewerbungsverfahren niemals freiwillig. Ein Durchleuchten der Persönlichkeit ist in aller Regel nicht erforderlich. Ausnahmen mag es geben, wo zwingend hohe psychische Anforderungen bestehen.

Ansonsten könnte versucht werden, die hergebrachten, teilweise vom BAG mitgeprägten Grundsätze zum Fragerecht bei Bewerbungen, in Gesetzesrecht zu überführen und z. B. verbotene Fragen bzw. Ausforschungsgegenstände aufzulisten.

Die fortlaufende Aktualisierung der Beschränkungen, die angesichts der schnellen technischen Entwicklung von Management-Tools zügig organisiert sein sollte, kann auch Fachgremien unterhalb der Gesetzgebung per Gesetz übertragen werden.

[348] Gola/*Pötters*, 2. Aufl., 2018, DS-GVO Art. 88 Rn. 12; Kühling/Buchner/*Maschmann*, 3. Aufl., 2020, DS-GVO Art. 88 Rn. 14; Simitis/Hornung/Spiecker gen. Döhmann/*Seifert*, 1. Aufl., 2019, DSGVO Art. 88 Rn. 18; Ehmann/Selmayr/*Selk*, 2. Aufl., 2018, DSGVO Art. 88 Rn. 44.

b) Internes Personalmanagement

Beim internen Personalmanagement gegenüber Beschäftigten werden häufig *weitere Auswahlverfahren* oder *individuelle Motivationsmaßnahmen* durchgeführt. Hier ist die Interessenlage viel komplizierter als beim Recruiting, denn auch Beschäftigte haben ein Interesse an einer sinnvollen Förderung und Beförderung. Wo genau die Grenze für zulässige Big Data-Analysen eingezogen werden kann, ist eine Frage der Abwägung im Einzelfall. Aber Verfahren bzw. Instrumente, die die Menschenwürde verletzen, ließen sich wohl für eine „Blacklist" identifizieren.

Weiterhin stehen Chancen, durch wissenschaftliche „People Analytics"-Projekte Arbeitsprozesse zu verbessern, im Raum. Hier können ebenfalls sowohl betriebswirtschaftliche Effizienzgewinne als auch Gewinne in der Arbeitsqualität für die Beschäftigten erzielt werden. Um dennoch Datenschutz zu gewährleisten, geht es vorrangig um organisatorische Maßnahmen der Anonymisierung, Pseudonymisierung oder um eine klare zweckspezifische Trennung der Daten. Anders als bei individualisierten Auswahl- oder Motivationsprozessen ist auf der wissenschaftlichen Ebene der Personalforschung eine schnelle Anonymisierung vielfach wohl möglich, ohne die Ergebnisse zu gefährden. Partizipative Projekte sollten nicht von vornherein ausgeschlossen sein, bei denen Beschäftigte oder ihre Interessenvertretungen am wissenschaftlichen Personalmanagement mitwirken und dazu dann auch Daten aus ihrem Erfahrungsschatz beisteuern können.

Auf beiden Feldern wäre vollständige Transparenz der Zwecke und Methoden eine wichtige Voraussetzung. Soweit die technischen Voraussetzungen selbsterklärender KI bzw. Big Data-Analyse fehlen, kann durch eine Zertifizierung ausreichend transparenter Produkte die rechtskonforme Entscheidung des Personalmanagements gemäß Art. 25 DSGVO unterstützt werden. Zum Regelungsbedarf siehe 5.3.

5.2.2 DATENSCHUTZ IM ARBEITSSCHUTZ

Die zahlreichen Akteure des Arbeits- und Gesundheitsschutzes sind angesichts der fortschreitenden Digitalisierung ihres Bereichs und des permanenten Umgangs mit sensiblen Daten mehr denn je gehalten, den Datenschutz zu beachten.

a) Datenschutz als Querschnittsaufgabe im Arbeitsschutz

Dies dürfte am wirkungsvollsten dadurch zu erreichen sein, dass das Ziel Datenschutz mit in die arbeitsschutzrechtliche Regelsetzung aufgenommen wird. Die Aufnahme einer einfachen Bestimmung zum Datenschutz in das Arbeitsschutzgesetz und – wo sinnvoll – in die Arbeitsschutzverordnungen könnte durchaus helfen. Denn das wäre ein Anlass, auch in die sehr konkreten Technischen Regeln Überlegungen einfließen zu lassen, wie Datenschutz im Arbeitsschutz praktiziert werden kann, ohne die absolut sinnvolle und vielfach notwendige intensive Kommunikation im Arbeitsschutz zu beeinträchtigen.

b) Überwachung als psychische Belastung

Für den Teilbereich der Überwachung wäre es noch wirksamer, Formen der Überwachung als möglichen Stressfaktor und als mögliche Ursache psychischer Erkrankungen zu betrachten. Es gibt hierzu keine klaren wissenschaftlichen Erkenntnisse. Aber jedenfalls unter ungünstigen Um-

ständen kann Überwachung eine psychische Belastung im arbeitsschutzrechtlichen Sinne sein, wie eine BAuA Metastudie zeigt.[349] Dann ist es konsequent, auch hierfür Technische Regeln zu entwickeln, die Hinweise für eine gute Praxis geben. Die rechtlichen Grundlagen hierfür wären in einer eigenen Verordnung zu psychischen Belastungen festzulegen. Dort könnten auch Einzelheiten der Gefährdungsbeurteilung bzgl. psychischer Belastungen geregelt werden (z. B. Anonymisierungsgebote).

Alternativ wäre an bestehende Arbeitsschutzverordnungen anzuknüpfen. So heißt es z. B. in § 3 Abs. 2 Satz 2 Nr. 3 Betriebssicherheitsverordnung, dass bei der Gefährdungsbeurteilung insbesondere Folgendes zu berücksichtigen sei: „die physischen und psychischen Belastungen der Beschäftigten, die bei der Verwendung von Arbeitsmitteln auftreten“. Auch Überwachungstechnik gehört zu den Arbeitsmitteln. Kann davon gefährdender psychischer Druck ausgehen, wäre das ein Thema für die Technischen Regeln für Betriebssicherheit (TRBS). Auch im Bildschirmarbeitsrecht der ArbStättV gäbe es entsprechende Anknüpfungspunkte. Der zuständige Ausschuss für Arbeitsstätten beim BMAS könnte Technische Regeln entwickeln, die Formen der Überwachung bei der Bildschirmarbeit begrenzen.

Eine gewisse Verbindlichkeit erlangt eine solche Regel dadurch, dass der Arbeitgeber z. B. laut § 4 Abs. 3 BetrSichV bei der Festlegung der Schutzmaßnahmen die Vorschriften der Verordnung einschließlich der Anhänge zu beachten und die bekannt gegebenen Regeln und Erkenntnisse zu berücksichtigen hat. Bei Einhaltung dieser Regeln und Erkenntnisse ist davon auszugehen, dass die in dieser Verordnung gestellten Anforderungen erfüllt sind („Vermutungswirkung“).

Der Zusammenhang zwischen Überwachung am Arbeitsplatz und psychischen Belastungen ist allerdings gegenwärtig nicht hinreichend geklärt, so dass entsprechende wissenschaftliche Untersuchungen dringend erforderlich sind.

5.3 TECHNISCH-ORGANISATORISCHE REGELUNGSPROJEKTE

5.3.1 TRANSPARENZ

Art. 88 Abs. 2 DSGVO fordert für nationale Regelungen des Beschäftigtendatenschutzes geeignete und besondere Maßnahmen insbesondere im Hinblick auf die Transparenz der Verarbeitung. Unter „besondere Maßnahmen“ sind solche zu verstehen, die gerade den besonderen Umständen des Beschäftigungsverhältnisses gerecht werden. Je nach Art des Betriebes hat es der oder die Beschäftigte zunehmend mit sehr großen Datenmengen zu tun, die zu seiner oder ihrer Person erhoben werden. Gleichzeitig kann es dabei um sehr schwer durchschaubare Verwendungen etwa im Bereich KI gehen („Black Box“). Zu den Besonderheiten des Beschäftigungsverhältnisses gehört weiter, dass die Verarbeitung regelmäßig nicht punktuell erfolgt (wie etwa beim Onlineshopping), sondern eine dauerhafte, oft Tag für Tag über jeweils mehrere Stunden relevante Verarbeitung vorliegt. Das erhöht die Legitimität des Wunsches, die zur eigenen Person vorgenommene Verarbeitung tatsächlich überblicken und verstehen zu können.

[349] *Backhaus*, Review zur Wirkung elektronischer Überwachung am Arbeitsplatz und Gestaltung kontextsensitiver Assistenzsysteme, BAUA Forschung Projekt F 2419, 46 f.

Bei niedrigem Stand der betrieblichen Digitalisierung mögen hierfür die in Art. 13 ff. DSGVO eingeräumten Rechte genügen. Bei hohem Stand der betrieblichen Digitalisierung ist das nicht der Fall. Bei hochdigitalisierten Arbeitsprozessen bedarf es transparenzfreundlicher Technik und es bedarf digitaler Instrumente, die es Beschäftigten erlauben, ihre Datenbestände in geordneter Weise einzusehen und z. T. auch zu verwalten. Das Problem ist damit weitgehend eines der technisch-organisatorischen Gestaltung und sollte in diesem Zusammenhang (siehe 5.3.2) vorrangig benannt und berücksichtigt werden.

Transparenz personenbezogener Datenverarbeitung bei fortgeschrittener Digitalisierung ist eine besondere Herausforderung, die letztlich ihrerseits nur digital zu bewältigen ist. Das BMAS beabsichtigt bereits seit 2017, einen „Index Beschäftigtendatenschutz" zu entwickeln. Ziel sind wissenschaftlich fundierte, anwendungsbezogene Qualitätsmaßstäbe für den Beschäftigtendatenschutz, die als wissenschaftliche Tools für die Selbstbewertung oder auch im Rahmen einer Zertifizierung den Beschäftigtendatenschutz in Betrieben vergleichbarer und handhabbarer machen.[350]

Insgesamt sind drei Aufgaben zu bewältigen:

- Es gilt Maßstäbe zu entwickeln für transparenzfreundliche Technik, die sich z. B. selbst erklärt, gut dokumentiert ist oder Aufgaben und Zwecke überschaubar trennt, um diese von solcher zu unterscheiden, die solche Qualitäten nicht aufweist.
- Es gilt die Anwendung solcher Technik zu fördern z. B. durch eine bereichsspezifische Spezifizierung der Privacy by Design-Regelung und von Zertifizierungen.
- Beschäftigte benötigen transparenzschaffende Assistenzsysteme, die Ihnen den Stand der Datenverarbeitung veranschaulichen. Diese könnten in einen Katalog von ergänzenden spezifischen TOMs für den Beschäftigtendatenschutz aufgenommen werden.

5.3.2 TECHNIKGESTALTUNG

Wie schon erwähnt, erlaubt es Art. 88 DSGVO, den Datenschutz durch Technikgestaltung gemäß Art. 25 DSGVO für den Beschäftigtendatenschutz zu spezifizieren.[351] Das ist in Kollektivvereinbarungen, aber auch durch den nationalen Gesetzgeber möglich.

Einzelne Technologien werden gesetzlich nicht sinnvoll vorzuschreiben sein, aber bestimmte Verfahrensmuster und Auswahlkriterien könnten die Praxis deutlich unterstützen. Vorgeschrieben werden könnte zum Verfahrensablauf, dass der Arbeitgeber bei technischen Eigenentwicklungen die Anforderungen des Beschäftigtendatenschutzes bereits während der Planung, Konzeption und Konstruktion der informationstechnischen Systeme einfließen lassen muss. Entscheidet er sich für den Einkauf von Technik oder von technischen Dienstleistungen, hat er bei der Ausschreibung, der Auswahl zwischen verschiedenen Angeboten oder bei der Formulierung des Pflichtenhefts die Anforderungen des Beschäftigtendatenschutzes zu beachten.[352] Der angeschlossene Katalog sollte dann einzelne technische Anforderungen wie u.a. Möglichkeit zur technische Trennung von Datenbeständen, Zugangssperren, zwingende zeitliche Speicherbegrenzungen, Trans-

[350] *BMAS* (Hrsg.), Weissbuch Arbeiten 4.0, 2017, S. 150. Hinweis: Seit 2020 führt die INPUT Consulting gGmbH das Projekt Index Beschäftigtendatenschutz (BeDaX) mit dem im Weißbuch Arbeiten 4.0 genannten Zielen durch (https://www.input-consulting.de/projekte/bedax.html).
[351] *Körner*, Beschäftigtendatenschutz in Betriebsvereinbarungen unter der Geltung der DS-GVO, NZA 2019, 1389 (1394); Ehmann/Selmayr/*Selk*, 2. Aufl., 2018, DS-GVO Art. 88 Rn. 125; Schwartmann et al./*Thüsing/Traut*, 2. Aufl., 2020, DS-GVO Art. 88 Rn. 25.
[352] Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, 1. Aufl., 2019, DSGVO Art. 25 Rn. 19.

parenztools für die Beschäftigten, Pseudonymisierungs- und Verschlüsselungsroutinen enthalten.[353] Dies alles mag auch schon nach Auslegung des geltenden Rechts erforderlich sein, sollte aber klar aus einem künftigen Gesetz hervorgehen.

Einen Schritt weiter ginge eine geregelte Zertifizierung datenschutzfreundlicher Technik. Das könnte allerdings Art. 42 DSGVO sprengen, da dort ausdrücklich nur eine Zertifizierung von Verarbeitungsvorgängen der Verantwortlichen, aber nicht von technischen Produkten als solchen vorgesehen ist.[354] Art. 88 DSGVO dürfte aber auch insoweit eine spezifischere Regelung zulassen, die auch eine Zertifizierung von datenschutzfreundlichen technischen Produkten im Beschäftigtendatenschutz vorsieht.

Eine zu schaffende ständige Kommission (vergleichbar den Arbeitsschutzausschüssen) beim BMAS[355] beobachtet den Markt, bewertet technische Innovationen, spricht Empfehlungen aus und entwickelt Regeln für die Praxis. Zugleich sollten Forschungs- und Entwicklungsprojekte gezielt gefördert werden. Es gilt, Datenschutz als technisches Ziel auf dem Markt attraktiv zu machen, um damit Forschung und Entwicklung voranzutreiben.

Auf betrieblicher Ebene könnte die Bedeutung der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO im Bereich des Datenschutzes erhöht werden. Sie kann tendenziell an die Gefährdungsbeurteilung im Arbeitsschutz angeglichen werden. Bei erheblichem Umgang z. B. mit KI oder Robotik muss die Datenschutz-Folgenabschätzung verpflichtend sein. Spezifische Durchführungsbestimmungen der DSFA für den Beschäftigtendatenschutz wären denkbar.

[353] *Körner*, Beschäftigtendatenschutz in Betriebsvereinbarungen unter der Geltung der DS-GVO, NZA 2019, 1389 (1394).
[354] Umstritten; einerseits Auernhammer/*Hornung*, 7. Aufl., 2020, DSGVO Art. 42 Rn. 44 f.; andererseits Taeger/Gabel/*Kinast*, 3. Aufl., 2019, DS-GVO Art. 42 Rn. 23.
[355] Von einem „Kompetenzzentrum" sprechen *Weichert/Schuler*, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, S. 24.

6. SCHLUSS: WESENTLICHE ERGEBNISSE

In produzierenden Betrieben und in den vielen Unternehmen der Dienstleistungsbranchen ermöglicht zunehmend leistungsfähige, miniaturisierte und zugleich kostengünstige Sensorik sowie eine Vielzahl von IT-Systemen eine Digitalisierung der Arbeitsprozesse, die tatsächlich dem 4.0-Paradigma entsprechend alle relevanten Informationen aller an der Wertschöpfung beteiligten Instanzen in Echtzeit vernetzen kann. Wo dies geschieht, entstehen gewaltige Big-Data-Pools, die von fortschreitend leistungsfähiger Software unter verschiedensten Gesichtspunkten zum Zweck der Prozessoptimierung analysiert werden können. Dabei fallen zwar in großen Mengen und mit hoher Aussagekraft personenbezogene Daten an, die jedoch regelmäßig nicht als solche gespeichert und ausgewertet werden müssten, um Prozesse zu verbessern. Allerdings ist das Zusammenspiel zwischen Mensch und intelligenten Geräten bzw. Maschinen ein Kernproblem der Entwicklung. Soll dieses Zusammenspiel optimiert werden, wird der Personenbezug der Daten vielfach wichtig. Die Maschine der Zukunft lernt in der Interaktion mit dem Menschen – und zwar nicht punktuell, sondern fortgesetzt. Neue Formen intensiver Überwachung entstehen.

Bei der *Digitalisierung des Personalmanagements* ist klar, dass es um Big *Personal* Data geht. Bei den zahlreichen Auswahlentscheidungen, die zu treffen sind (Einstellung, Förderung, Aufstieg, Kündigung), geht nichts ohne klaren Personenbezug. Die Digitalisierung des Personalmanagements, das auf vorhandene betriebliche Big-Data-Pools zurückgreift, bei steigenden wissenschaftlichen Ansprüchen aber auch selbst Daten erheben wird, stellt die Belange des Beschäftigtendatenschutzes systematisch in Frage. Hinzu kommt, dass gerade das Personalmanagement auf umkämpften Arbeitsmärkten Ambitionen entwickeln könnte, tief in die Persönlichkeitsstruktur der Beschäftigten einzudringen.

Auch bei der *Digitalisierung des Arbeitsschutz- bzw. Gesundheitsschutzmanagements* ist der Personenbezug häufig als solches von Bedeutung. Zusätzlich gibt es hier zwei besonders brisante Besonderheiten. Erstens geht es hier ständig um *besonders sensible* Gesundheitsdaten. Das gilt verstärkt, seitdem die psychische Gesundheit im Arbeitsschutz ernsthaft zu berücksichtigen ist. Der Konflikt ist hier zweitens noch dadurch geprägt, dass der Arbeitgeber verpflichtet ist, Arbeitssicherheit nach modernsten Methoden zu gewährleisten. Digitalisierung ist hier – anders als im Personalmanagement – schlicht gesetzliche Pflicht.

Das *Potenzial des geltenden Beschäftigtendatenschutzes* aus § 26 BDSG und ergänzenden Vorschriften der DSGVO ist beachtlich und war, sofern es praktisch tatsächlich angewendet worden ist, durchaus geeignet, für angemessenen Datenschutz in den Betrieben zu sorgen. Die Zulässigkeitsmaßstäbe sind in der Auslegung des Bundesarbeitsgerichts ausreichend streng und die begleitenden Rechte der Beschäftigten sowie organisatorischen Pflichten aus der DSGVO sind vielversprechend.

Eine andere Frage ist, ob dieses Instrumentarium der Wucht einer allseitigen Digitalisierung aller betrieblichen Funktionen, wie sie das 4.0-Paradigma vorsieht, gewachsen ist. Es droht insbesondere eine drastische Überforderung der individuellen und tendenziell auch kollektiven Beteiligungsrechte. Das beginnt schon bei der Pflicht der Unternehmen, die Transparenz der Datenverarbeitung gegenüber betroffenen Beschäftigten herzustellen. Vor allem die Zweckbindung bzw. die Trennung der Datenbestände nach Zwecken droht sich aufzulösen. Datenschutzfreundliche

Technikgestaltung wäre möglich – auch im Sinne selbsterklärender Transparenz. Sie wird aber rechtlich nicht ausreichend eingefordert.

So solide der Beschäftigtendatenschutz in Deutschland als Gesamtsystem wirkt, so baufällig sind seine *gesetzlichen Grundlagen*. Das Problem ist dreifacher Natur. Der gesetzliche Beschäftigtendatenschutz ist zersplittert, teils irreführend und teils zu abstrakt geregelt. Wer nur die Rechtsquellen in DSGVO und BDSG zur Verfügung hat, hat keine Chance, seine tatsächlichen Inhalte zu verstehen. Text und Interpretation fallen zum Teil stark auseinander. Völlig zurecht besteht daher der Anspruch, ein benutzerfreundliches, klares und übersichtliches Regelwerk in einer Reform zu schaffen.

Die DSGVO lässt ein eigenständiges nationales *Beschäftigtendatenschutzgesetz* zu. Eine starke – wenn auch nicht mehrheitliche – Meinung in der Fachwelt gibt jedoch zu bedenken, dass die DSGVO keine Abweichungen, sondern nur Spezifizierungen zulasse. Dem kann Rechnung getragen werden, ohne an Substanz zu verlieren. Denn die DSGVO sieht bereits einen breiten Fächer an Durchsetzungsinstrumenten vor, der durch Spezifizierungen im Sinne des Beschäftigtendatenschutzes noch erheblich an Wirksamkeit gewinnen kann.

Die Erarbeitung eines Beschäftigtendatenschutzgesetzes ist damit *keine* vorrangig juristische Aufgabe. Sie wird *nicht durch europäisches Recht diktiert*, sondern unterliegt mit erheblichem Freiraum den Gestaltungsvorstellungen, die sich aus dem nationalen demokratischen Prozess ergeben. Je breiter dieser Prozess angelegt wird, desto größer die Chance, eine Kultur des Datenschutzes zu fördern. Dabei ist neben juristischem auch ökonomischer, sozialwissenschaftlicher und technischer Sachverstand dringend gefordert.

Hier wird – im Einklang mit zahlreichen anderen Stellungnahmen – vorgeschlagen, den *Schwerpunkt einer Reform* auf den Datenschutz durch Technikgestaltung (Privacy by Design) zu setzen. Präzise Verfahren und Kriterien sollten gesetzlich geregelt werden, wozu u. a. Art. 25 und 35 DSGVO deutlich konkretisiert in ein Beschäftigtendatenschutzgesetz aufzunehmen wären. Um auch Hersteller bzw. Entwickler in die Pflicht zu nehmen, sollte wenigstens die Möglichkeiten zur Zertifizierung auf technische Produkte ausgedehnt werden. Eine gesetzlich dauerhaft eingesetzte Kommission für Beschäftigtendatenschutz auf Bundesebene könnte u. a. für kontinuierliche und damit technisch aktuelle Empfehlungen (ggf. Regelungen) für datenschutzfreundliche Technik, Verfahren und Organisation der betrieblichen Praxis sorgen, um Arbeitgeber und Interessenvertretungen zu unterstützen. Für die Beschäftigten werden Instrumente wie der angekündigte Index Beschäftigtendatenschutz angeboten, die Transparenz der individuellen Betroffenheit durch die jeweilige betriebliche Datenverarbeitung unterstützen können. Entsprechende technische Assistenzsysteme sollten bei fortgeschrittener betrieblicher Digitalisierung für die Beschäftigten verpflichtend zur Verfügung stehen.

Unabhängig davon könnte das Personalmanagement und der betriebliche Arbeitsschutz explizit und konkret durch Datenschutzregelungen adressiert werden. Im *Personalmanagement* ist der „Krieg um Talente“ ohnehin eine Sackgasse. Mit der Menschenwürde der Bewerber*innen ist ein Überbietungswettbewerb um die beste technisch gestützte Durchdringung der menschlichen Psyche völlig unvereinbar. Es müsste möglich sein, sich in den Fachkreisen zwecks Abrüstung auf klare gesetzliche Einschränkungen zu einigen.

Im *Arbeitsschutz* sind Chancen und Risiken der Digitalisierung besonders eng verknüpft. Zugleich gibt es aber im Arbeitsschutz mit den Ausschüssen beim BMAS die erfolgreichsten Instanzen der untergesetzlichen Regelsetzung, die sich des Themas Datenschutz nur annehmen müssten. Erfor-

derlich wären knappe Hinweise auf den Datenschutz im einschlägigen Recht und Aufträge an die zuständigen Ausschüsse, den Datenschutz mit Hinweisen und Beispielen für eine gute betriebliche Praxis *in das Technische Regelwerk* aufzunehmen, nicht zuletzt um auch mögliche psychische Belastungen durch Überwachung zu begrenzen.

LITERATURVERZEICHNIS

Abend, Sonja, Mehr Durchblick dank Datenbrille? Wie virtuelle Realität die berufliche Teilhabe verbessern kann, IAB-Forum, 17. Januar 2019, www.iab-forum.de/mehr-durchblick-dank-datenbrille-wie-virtuelle-realitaet-die-berufliche-teilhabe-verbessern-kann/.

Adolph, Lars/Kirchhoff, Britta/Geilen, Jan-Hendrik, Sicherheit und Gesundheit in der digitalen Arbeitswelt, in: Maier, Günter W./Engels, Gregor/Steffen, Eckhard (Hrsg.), Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, 2020, 21-34.

Apt, Wenke/Priesack, Kai, KI und Arbeit – Chance und Risiko zugleich, in: Wittpahl, Volker (Hrsg.), Künstliche Intelligenz, Berlin/Heidelberg 2019, 221-238.

Ariel, Barak/Sutherland, Alex/Henstock, Darren/Young, Josh/Drover, Paul/Sykes, Jayne/Megicks, Simon/Henderson, Ryan, Paradoxical effects of self-awareness of being observed: testing the effect of police body-worn cameras on assaults and aggression against officers, Journal of Experimental Criminology 14, 2018, 19-47.

Armutat, Sascha, Leistungsmanagement: Das Ganze im Blick, in: Armutat, Sascha/ Bartholomäus, Natalie/ Franken, Swetlana/ Herzig, Volker/ Helbich, Bernd (Hrsg.), Personalmanagement in Zeiten von Demografie und Digitalisierung, Wiesbaden 2018, 261-284.

Arnhold, Katharina/Butschek, Sebastian/Grunau, Philipp/Kampkötter, Patrick/Petters, Lea/Sliwka, Dirk, Bericht zum Forschungsmonitor „Variable Vergütungssysteme“, BMAS Forschungsbericht 507, 2018.

Auernhammer/Eßer/Kramer/v. Lewinski (Hrsg.), DSGVO BDSG Kommentar, 7. Aufl., Hürth 2020.

Backhaus, Nils, Review zur Wirkung elektronischer Überwachung am Arbeitsplatz und Gestaltung kontextsensitiver Assistenzsysteme, BAUA Forschung Projekt F 2419.

Backhaus, Nils, Kontextsensitive Assistenzsysteme und Überwachung am Arbeitsplatz: Ein meta-analytisches Review zur Auswirkung elektronischer Überwachung auf Beschäftigte, Z.Arb.Wiss. 2019, 2-22.

Balikcioglu, Julia, Psychische Erkrankungen am Arbeitsplatz - Die zunehmende Bedeutung der Psyche im Gesundheitsschutz, NZA 2015, 1424-1433.

BAuA (Hrsg.), Head-Mounted Displays – Arbeitshilfen der Zukunft. Bedingungen für den sicheren und ergonomischen Einsatz monokularer Systeme, 2016.

Bauckhage, Christian/Bauernhansl, Thomas/Beyerer, Jürgen/Garcke, Jochen, Kognitive Systeme und Robotik, in: Neugebauer, Reimund (Hrsg.), Digitalisierung, Berlin/Heidelberg 2018, 239-255.

Baudach, Tino/Hellge, Viola/Schröder, Delia/Zink, Klaus J., Organisationen und Führung 4.0, in: Zink, Klaus J. (Hrsg.), Baden-Baden 2019, 143-186.

Bauer, Wilhelm/Hämmerle, Moritz/Bauernhansl, Thomas/Zimmermann, Thilo, Future Work Lab – Arbeitswelt der Zukunft, in: Neugebauer, Reimund (Hrsg.), Digitalisierung, Berlin/Heidelberg 2018, S. 179-195.

Bauer, Wilhelm/Hofmann, Josephine, Arbeit, IT und Digitalisierung, in: Hofmann, Josephine (Hrsg.), Arbeit 4.0 – Digitalisierung, IT und Arbeit, Wiesbaden 2018, 1-16.

Beck, David, Psychische Belastung als Gegenstand des Arbeitsschutzes, Arbeit 2019, 125-147.

Becker, Carlos/Seubert, Sandra, Privatheit, kommunikative Freiheit und Demokratie, DuD 2016, 73-78.

Behrendt, Hauke/Loh, Wulf/Matzner, Tobias/Misselhorn, Catrin, Einleitung, in: Behrendt, Hauke/Loh, Wulf/Matzner, Tobias/Misselhorn, Catrin (Hrsg.), Privatsphäre 4.0. Eine Neuverortung des Privaten im Zeitalter der Digitalisierung, Berlin 2019, 1-10.

Betz, Christoph, Automatisierte Sprachanalyse zum Profiling von Stellenbewerbern, ZD 2019, 148-152.

Biemann/Englmaier/Sliwka/Weller, People Analytics – Personaldaten als Erfolgsfaktor, PERSONAL-quarterly 3/2017, S. 8 (9 ff.).

BMAS (Hrsg.), Weißbuch Arbeiten 4.0, Berlin 2017.

Boehme-Neßler, Volker, Privacy: a matter of democracy. Why democracy needs privacy and data protection, International Data Privacy Law 2016, Vol. 6 No. 3, pp. 222-229.

Braehmer, Barbara, Warum Sie auf Twitter im Recruiting nicht verzichten dürfen, in: Dannhäuser, Ralph (Hrsg.), Praxishandbuch Social Media Recruiting, 4. Aufl., Wiesbaden 2020, 283-314.

Brink, Stefan/Wolff, Heinrich Amadeus (Hrsg.), BeckOK Datenschutzrecht, 34. Edition, München 2020.

Buxbaum, Hans-Jürgen (Hrsg.), Mensch-Roboter-Kollaboration, Wiesbaden 2020.

Buxbaum, Hans-Jürgen/Häusler, Ruth, in: Buxbaum, Hans-Jürgen (Hrsg.), Mensch-Roboter-Kollaboration, Wiesbaden 2020, 293-317.

Buxbaum, Hans-Jürgen/Kleutges Markus, Evolution oder Revolution? Die Mensch-Roboter-Kollaboration, in: Buxbaum (Hrsg.), Mensch-Roboter-Kollaboration, Wiesbaden 2020, 15-33.

Cernavin, Oleg/Lemme, Gordon, Technologische Dimensionen der 4.0-Prozesse, in: Cernavin, Oleg/Schröter, Welf/Stowasser, Sascha (Hrsg.), Prävention 4.0, Wiesbaden 2018, 21-55.

Chandna-Hoppe, Katja, Beweisverwertung bei digitaler Überwachung am Arbeitsplatz unter Geltung des BDSG 2018 und der DS-GVO – Der gläserne Arbeitnehmer?, NZA 2018, 614-619.

Conty, Laurence/George, Nathalie/Hietanen, Jari K., Watching Eyes effects: When others meet the self, Consciousness and Cognition 45, 2016, 184-197.

Corves, Burkhard/Hüsing, Mathias/Bezrucav, Stefan/Detert, Tim/Lauwigi, Johanna/Lorenz, Michael/Mandischer, Nils/Schmitz, Markus/Shahidi, *Amirreza,* Robotik 4.0, in: Frenz, Walter (Hrsg.), Handbuch Industrie 4.0: Recht, Technik, Gesellschaft, Berlin 2020, 569-589.

Culik, Nicolai/Döpke, Christian, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226-230.

Däubler, Wolfgang, Gläserne Belegschaften, 8. Aufl., Frankfurt a. M. 2019.

Däubler, Wolfgang, Digitalisierung und Arbeitsrecht, 7. Aufl., Frankfurt a. M. 2020.

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke, EU-DSGVO und BDSG Kompaktkommentar, 2. Aufl., Frankfurt a. M. 2020.

Dannhäuser, Ralph (Hrsg.), Praxishandbuch Social Media Recruiting, 4. Aufl., Wiesbaden 2020.

Dannhäuser, Ralph, Trends im Recruiting, in: Dannhäuser, Ralph (Hrsg.), Praxishandbuch Social Media Recruiting, 4. Aufl., Wiesbaden 2020, 1-35.

Diercks, Joachim, Online-Assessment, in: Verhoeven, Tim (Hrsg.), Digitalisierung im Recruiting, Wiesbaden 2020, 79-99.

Dietrich, Aljoscha/Bosse, Christian K./Schmitt, Hartmut, Kontrolle und Überwachung von Beschäftigten, DuD 2021, 5-10.

DSK, Kurzpapier Nr. 14, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf.

Duval, T. Shelley/Wicklund, Robert A., A theory of objective self-awareness, New York 1972.

Dzida, Boris, Big Data und Arbeitsrecht, NZA 2017, 541-546.

Ehmann, Eugen/Selmayr, Marin (Hrsg.), DS-GVO Kommentar, 2. Aufl., München 2018.

Ernst, Gerhard/Zühlke-Robinet, Klaus/Finking, Gerhard/Bach, Ursula (Hrsg.), Digitale Transformation – Arbeit in Dienstleistungssystemen, Baden-Baden 2020.

Evers, Maren/Krzywdzinski, Martin/Pfeiffer, Sabine, Wearable Computing im Betrieb gestalten, Arbeit 2019, 3-27.

Fellner, *Katrin,* Moderne Personalauswahl, Wiesbaden 2019.

Fortmann, Harald R./Kolocek, Barbara (Hrsg.), Arbeitswelt der Zukunft, Wiesbaden 2018.

Franzen, Martin/ Gallner, Inken/Oetker, Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 3. Aufl., München 2020.

Franken, Rolf/Franken, Swetlana, Wandel von Managementfunktionen im Kontext der Digitalisierung, in: Hirsch-Kreinsen/Ittermann/Niehaus (Hrsg.), 2. Aufl. 2017, 99-120.

Frost, Martina/Sandrock, Stephan, Neue Belastungsarten in der Arbeitswelt 4.0, ifaa – Factsheet, 2019, www.arbeitswissenschaft.net/fileadmin/Downloads/Factsheet_Belastungsarten.pdf.

Gärtner, Christian, Smart HRM – Digitale Tools für die Personalarbeit, Wiesbaden 2020.

Gervais, Will M./Norenzayan, Ara, Like a camera in the sky? Thinking about God increases public self-awareness and socially desirable responding, Journal of Experimental Social Psychology 48, 2012, 298-302.

Giesen, Richard, Materielles Betriebsverfassungsrecht und Digitalisierung, NZA 2020, 73-76.

Gilbert, Kristin/Kirmse, Karolina A./Pietrzyk, Ulrike/Steputat-Rätze, Anne, Gestaltungshinweise für die praktische Umsetzung der Gefährdungsbeurteilung psychischer Belastung, ZArbWiss 2020, 89-99.

Glancy, Dorothy J., The Invention of the Right to Privacy, Arizona Law Rev. 21, 1979, 1-39.

Gola, Peter (Hrsg.), DS-GVO Kommentar, 2. Aufl., München 2018.

Gola, Peter, Handbuch Beschäftigtendatenschutz, 8. Aufl., Frechen 2019.

Gola, Peter/Heckmann, Dirk (Hrsg.), BDSG Kommentar, 13. Aufl., München 2019.

Guilfoyle, Sarah/Bergman, Shawn m./Hartwell, Christopher/Powers, Jonathan, Social Media, Big Data, and Employment Decisions: Mo' Data, Mo' Problems?, in: Landers/Schmidt (Hrsg.), Social Media in Employee Selection and Recruitment, Switzerland 2016, 127-155.

Gusy, Christoph/Eichenhofer, Johannes, Kommentar zu § 1 BDSG, in: Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 33 Ed. 2020, BDSG § 1.

Haipeter, Thomas, Entwicklung, Herausforderungen und Perspektiven der Leistungsregulierung, in: WSI Mitteilungen 2020, 47-54.

Hartmann, Felix, Diskriminierung aus der Black Box – Neue Herausforderungen durch KI-gestützte Personalentscheidungen, EuZA 2019, 421-422.

Haußmann, Katrin/Thieme, Luca Maria, Reformbedarf und Handlungsoptionen in der IT-Mitbestimmung, NZA 2019, 1612-1620.

Hirsch-Kreinsen, Hartmut, Einleitung: Digitalisierung industrieller Arbeit, in: Hirsch-Kreinsen, Hartmut/Ittermann, Peter/Niehaus, Jonathan (Hrsg.), Digitalisierung industrieller Arbeit, Baden-Baden, 2. Aufl. 2018, 13-32.

Hirsch-Kreinsen, Hartmut/Ittermann, Peter/Niehaus, Jonathan (Hrsg.), Digitalisierung industrieller Arbeit, Baden-Baden, 2. Aufl., Baden-Baden 2018.

Hofmann, *Kai,* Smart Factory - Arbeitnehmerdatenschutz in der Industrie 4.0 - Datenschutzrechtliche Besonderheiten und Herausforderungen, ZD 2016, 12-17.

Holtbrügge, Dirk, Personalmanagement, 7. Aufl., Berlin 2018.

Holthausen, Joachim, Big Data, People Analytics, KI und Gestaltung von Betriebsvereinbarungen – Grund-, arbeits- und datenschutzrechtliche An- und Herausforderungen, RdA 2021, 19-32.

Holz, Anja/Herold, Robert/Friemert, Daniel/Hartmann, Ulrich/Harth, Volker/Terschüren, Claudia, Datenbrillen am Arbeitsplatz – Informationsdichte am Auge, ZblArbeitsmed 2021, 24-28.

Hornung, Gerrit/Hofmann, Kai, Datenschutz als Herausforderung der Arbeit in der Industrie 4.0, in: Hirsch-Kreinsen, Hartmut/Ittermann, Peter/Niehaus, Jonathan (Hrsg.), Digitalisierung industrieller Arbeit, Baden-Baden, 2. Aufl. 2018, 233-255.

Huf, Stefan, Personalmanagement, Wiesbaden 2020.

Huff, Julian/Götz, Thomas, Evidenz statt Bauchgefühl? – Möglichkeiten und rechtliche Grenzen von Big Data im HR-Bereich, NZA-Beilage 2019, 73-78.

Jacobs, Joh. Christian/Kagermann, Henning/Sattelberger, Thomas/Lange, Thomas, Zukunft der Arbeit: Die digitale Transformation gestalten, in: Werther, Simon/Bruckner, Laura (Hrsg.), Arbeit 4.0 aktiv gestalten, Berlin 2018, 24-29.

Jaspers, Andreas/Jacquemain, Tobias, Künstliche Intelligenz und ihre Auswirkungen auf den Beschäftigtendatenschutz, RDV 2019, 232-235.

Joos, Daniel, Einsatz von künstlicher Intelligenz im Personalwesen unter Beachtung der DS-GVO und des BDSG, NZA 2020, 1216-1221.

Junghanns, Gisa/Kersten, Norbert, Informationsüberflutung am Arbeitsplatz – Gesundheitliche Konsequenzen, ZblArbeitsmed 2020, 8-17.

Käde, Lisa/von Maltzan, Stephanie, Entmystifizierung der Black Box und Chancen für das Recht, CR 2020, 66-72.

Kagermann, Henning, Chancen von Industrie 4.0 nutzen, in: Bauernhansl, Thomas/ten Hompel, Michael/Vogel-Heuser, Birgit (Hrsg.), Industrie 4.0 in Produktion, Automatisierung und Logistik, Wiesbaden 2014, 603-614.

Kersting, Stefan/Naplava, Thomas/Reutemann, Michael/Heil, Marie/Scheer-Vesper, Carola, Die deeskalierende Wirkung von Bodycams im Wachdienst der Polizei Nordrhein-Westfalen: Abschlussbericht, 2019.

Kienbaum, Fabian/Gunnesch, Markus/Pacher, Sebastian, Geld und Vergütung im Zeitalter der Digitalisierung: Wie sieht das Performance Management von morgen aus?, in: Fortmann, Harald R./Kolocek, Barbara (Hrsg.), Arbeitswelt der Zukunft, Wiesbaden 2018, 27-49.

Kirchner, Stefan/Meyer, Sophie-Charlotte/Tisch, Anita, Digitaler Taylorismus für einige, digitale Selbstbestimmung für die anderen? Ungleichheit der Autonomie in unterschiedlichen Tätigkeitsdomänen, baua: Fokus, Juli 2020.

Klingbeil, Thilo/Kohm, Simon, Datenschutzfreundliche Technikgestaltung und ihre vertraglichen Implikationen, MMR 2021, 3-8.

Körner, Marita, Die Datenschutz-Grundverordnung und nationale Regelungsmöglichkeiten für Beschäftigtendatenschutz, NZA 2016, 1383-1386.

Körner, Marita, Beschäftigtendatenschutz in Betriebsvereinbarungen unter der Geltung der DS-GVO, NZA 2019, 1389-1395.

Kopp, Reinhold/Sokoll, Karen, Wearables am Arbeitsplatz - Einfallstore für Alltagsüberwachung?, NZA 2015, 1352-1359.

Kort, Michael, Rechte des Betriebsrats auf Daten der elektronischen Personalakte - Aufgabenerfüllung der Personalvertretung und Arbeitnehmerdatenschutz, ZD 2015, 3-6.

Kort, Michael, Eignungsdiagnose von Bewerbern unter der Datenschutz-Grundverordnung (DS-GVO), NZA-Beilage 2016, 62-71.

Kort, Michael, Die Bedeutung der neueren arbeitsrechtlichen Rechtsprechung für das Verständnis des neuen Beschäftigtendatenschutzes, NZA 2018, 1097-1105.

Kort, Michael, Neuer Beschäftigtendatenschutz und Industrie 4.0, RdA 2018, 24-33.

Kort, Michael, Arbeits- und Gesundheitsschutz – Technische Überwachung – Persönlichkeitsrecht, Anmerkung zu BAG v. 25.4.2017 – 1 ABR 46/15, RdA 2018, 242-248.

Krause, Rüdiger, Herausforderung Digitalisierung der Arbeitswelt und Arbeiten 4.0, NZA-Beilage 2017, 53-59.

Krause, Rüdiger, Digitalisierung und Beschäftigtendatenschutz, BMAS Forschungsbericht 482, 2017.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), DS-GVO BDSG Kommentar, 3. Aufl., München 2020.

Kulkarni, Vivek/Kern, Margaret L./Stillwell, David/Kosinsk, Michal/Matz, Sandra/Ungar, Lyle/Skiena, Steven/Schwartz, H. Andrew, Latent human traits in the language of social media: An openvocabulary approach, 2018, PLoS ONE 13(11): e0201703.

Lang, Franz Peter, Quo vadis Digitale Revolution, in: Hermeier, Burghard/Heupel, Thomas/ Fichtner-Rosada, Sabine (Hrsg.), Arbeitswelten der Zukunft, Wiesbaden 2019, 3-22.

Lindner, Josef Franz, Kognitive Neuroergonomie als Problem des Arbeitsrechts, NJOZ 2020, 321-326.

Lutz, Holger/Born, Tobias, Die Verarbeitung personenbezogener Daten durch Unternehmen zur Eindämmung der COVID-19-Pandemie, DB 2020, 1162-1167.

Lurtz, Helmut/Ruhmann, Maurice, Der lange Weg zu einem Beschäftigtendatenschutzgesetz?, ZD-Aktuell 2020, 07281.

Matusiewicz, David/Kaiser, Linda (Hrsg.), Digitales Betriebliches Gesundheitsmanagement, Wiesbaden 2018.

Martini, Mario/Botta, Jonas, Iron Man am Arbeitsplatz? – Exoskelette zwischen Effizienzstreben, Daten- und Gesundheitsschutz, Chancen und Risiken der Verschmelzung von Mensch und Maschine in der Industrie 4.0, NZA 2018, 625-637.

Maschmann, Frank, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, 115-124.

Mühlbauer, Daniel/Huff, Julian/Süß, Julian, People Analytics und Arbeit 4.0, in: Werther, Simon/Bruckner, Laura (Hrsg.), Arbeit 4.0 aktiv gestalten, Berlin 2018, 107-132.

Müller-Glöge, Rudi/Preis, Ulrich/Schmidt, Ingrid (Hrsg.), Erfurter Kommentar zum Arbeitsrecht, 21. Aufl., München 2021.

Munger, Kristen/Harris, Shelby J., Effects of an observer on handwashing in a public restroom, Perceptual and Motor Skills 69, 1989, 733-734.

Naber, Sebastian/Schulte, Willem, Können Arbeitnehmer zu einer Corona-Impfung oder einem Impfnachweis verpflichtet werden?, NZA 2021, 81-86.

Nebel, Maxi, Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht, ZD 2015, 517-521.

Nebel, Maxi, Big Data und Datenschutz in der Arbeitswelt, Risiken der Digitalisierung und Abhilfemöglichkeiten, ZD 2018, 520-524.

Neugebauer, Reimund (Hrsg.), Digitalisierung, Berlin/Heidelberg 2018.

Nürnberg, Volker, Optimierung von betrieblicher Bildung mit digitalen Lernformaten, SPA 2019, 149-151.

Paal, Boris P./Pauly, Daniel A. (Hrsg.), DS-GVO BDSG Kompakt-Kommentar, 3. Aufl., München 2021.

Pang, Dandan/Eichstaedt, Johannes C./Buffone, Anneke/Slaff, Barry/Ruch, Willibald/Ungar, Lyle H., The language of character strengths: Predicting morally valued traits on social media. Journal of Personality, 2020, 88: 287–306.

Park, Gregory/Schwartz, H. Andrew/Eichstaedt, Johannes C./Kern, Margaret L./Kosinski, Michal/Stillwell, David/Ungar, Lyle H./Seligman, Martin E. P., Automatic personality assessment through social media language. Journal of Personality and Social Psychology, 2015, 108(6), 934–952.

Plath, Kai-Uwe (Hrsg.), DSGVO BDSG Kommentar, 3. Aufl., Köln 2018.

Plattform Industrie 4.0 (Hrsg.), Umsetzungsstrategie Industrie 4.0, Berlin/Frankfurt a.M., 2015

Pluta, Werner, Aktives Exoskelett Cray X hilft beim Heben, golem.de 3. April 2019, www.golem.de/news/german-bionic-aktives-exoskelett-cray-x-hilft-beim-heben-1904-140431.html.

Reindl, Cornelia/Krügl, Stefanie, People Analytics in der Praxis, Freiburg 2017.

Reßut, Norman/Hoppe, Annette, Erfassung von individuellem Beanspruchungserleben bei kognitiven Belastungssituationen mittels *Mustererkennung* im Lidschlagverhalten, ZArbWiss 2020, 249-261.

Richardi, Reinhard (Hrsg.), Betriebsverfassungsgesetz Kommentar, 16. Aufl., München 2018.

Richter, Marcus, Begriff des Arbeitsgebers, in: Kiel, Heinrich/Lunk, Stefan/Oetker, Hartmut (Hrsg.), Münchener Handbuch zum Arbeitsrecht, 4. Aufl., München 2018, Band 1: Individualarbeitsrecht I, § 23.

Riesenhuber, Karl, Kommentar zu Art. 88 DSGVO, in: Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 33 Ed. 2020, DSGVO Art. 88.

Riesenhuber, Karl, Kommentar zu § 26 BDSG, in: Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 33 Ed. 2020, BDSG § 26.

Ritter, Franziska/Reibach, Boris/Lee, Morris, Lösungsvorschlag für eine praxisgerechte Risikobeurteilung von Verarbeitungen, ZD 2019 531-535.

Rose, Edgar, Arbeitsschutz vs. Datenschutz!?, in: Specht-Riemenschneider, Louisa/Buchner, Benedikt/Heinze, Christian/Thomsen, Oliver (Hrsg.), IT-Recht in Wissenschaft und Praxis, Festschrift für Jürgen Taeger, Frankfurt am Main 2020, 393-412.

Roßnagel, Alexander/Jandt, Silke/Skistims, Hendrik/Zirfas, Julia, Datenschutz bei Wearable Computing, Wiesbaden 2012.

Sagan, Adam/Brockfeld, Marius, Arbeitsrecht in Zeiten der Corona-Pandemie, NJW 2020, 1112-1117.

Sasse, Stefan/Schönfeld, Julia, Rechtliche Aspekte psychischer Belastungen im Arbeitsverhältnis, RdA 2016, 346-357.

Scataglini, Sofia/Truyen, Elie/Perego, Paolo/Gallant, Johan/Van Tiggelen, Damien/Andreoni, Giuseppe, Smart Clothing for Human Performance Evaluation: Biomechanics and Design Concepts Evolution, in: BAuA (Hrsg.), Proceedings of the 5th International Digital Human Modeling Symposium, 2017, 9-17.

Schaub, Günter/Ahrendt, Martina/Koch, Ulrich/Linck, Rüdiger/Treber, Jürgen/Vogelsang, Hinrich (Hrsg.), Arbeitsrechts-Handbuch, 18. Aufl., München 2019.

Schröder, Lothar, Die digitale Treppe, Frankfurt am Main 2016,

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.), Heidelberger Kommentar DS-GVO/BDSG, 2. Aufl., Heidelberg 2020.

Schwarz, Mathias, Arbeitnehmerüberwachung und Mitbestimmung, 1982.

Schwenke, Thomas, Private Nutzung von Smartglasses im öffentlichen Raum, Edewecht 2016.

Silvia, Paul J./Duval, T. Shelley, Objective Self-Awareness Theory: Recent Progress and Enduring Problems, Personality and Social Psychology Review 5, 2001, 230-241.

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.), Datenschutzrecht Kommentar, 1. Aufl., Baden-Baden 2019.

Staab, Philipp/Geschke, Sascha-Christopher, Ratings als arbeitspolitisches Konfliktfeld – Das Beispiel Zalando, HBS Study 429, Düsseldorf 2019.

Stock-Homburg, Ruth/Groß, Matthias, Personalmanagement, 4. Aufl., Wiesbaden 2019.

Steil, Jochen J./Maier, Günter W., Kollaborative Roboter: universale Werkzeuge in der digitalisierten und vernetzten Arbeitswelt, in: Maier, Günter W./Engels, Gregor/Steffen, Eckhard (Hrsg.), Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, Berlin 2020, S. 323-346.

Stück, Volker, Gefährdungsbeurteilung psychischer Belastungen in Recht und Praxis, ArbRAktuell 2015, 515-518.

Stück, Volker, Anmerkung zu BAG v. 23.10.2018 – 1 ABN 36/18, ZD 2019, 132.

Stück, Volker, Personalauswahl und -beurteilungsverfahren: Aktuelle arbeits- und datenschutzrechtliche Aspekte, ArbRAktuell 2020, 153-156.

Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung Handkommentar, 2. Aufl, Baden-Baden 2018.

Taeger, Jürgen/Gabel, Detlev (Hrsg.), Kommentar DSGVO – BDSG, 3. Aufl., Frankfurt a. M. 2019.

Taeger, Jürgen/Rose, Edgar, Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes, BB 2016, 819-831.

Tallgauer, Maximilian/Festing, Marion/Fleischmann, Florian, Big Data im Recruiting, in: Verhoeven, Tim (Hrsg.), Künstliche Intelligenz im Recruiting, Wiesbaden 2020, 25-39.

Ternés, Anabel/Wilke, Clarissa-Diana (Hrsg.), Agenda HR – Digitalisierung, Arbeit 4.0, New Leadership, Wiesbaden 2018.

Tiedemann, Jens, VI. Prozessuale Verwertbarkeit von Kontrollergebnissen, in: Kramer, IT-Arbeitsrecht, 2. Aufl. 2019, Kap B. Rn. 540-583.

Tolsdorf, Jan/Bosse, Christian K./Dietrich, Aljoscha/Feth, Denis/Schmitt, Hartmut, Privatheit am Arbeitsplatz, Transparenz und Selbstbestimmung bei Arbeit 4.0, DuD 2020, 176-181.

Treier, Michael, Wirtschaftspsychologische Grundlagen für Personalmanagement, Berlin 2019.

Trost, Armin, Neue Personalstrategien zwischen Stabilität und Agilität, Berlin 2018.

Varadinek, Brigitta/Indenhuck, Moritz/Surowiecki, Eva, Rechtliche Anforderungen an den Datenschutz bei adaptiven Arbeitsassistenzsystemen, BAUA Projekt F 2412, Dortmund/Berlin/Dresden 2018.

Verhoeven, Tim, Künstliche Intelligenz im Recruiting, in: Verhoeven, Tim (Hrsg.), Digitalisierung im Recruiting, Wiesbaden 2020, 113-128.

Villwock, Peer-Oliver/Serries, Christoph/Voigtländer, Thomas, Arbeitsschutz 4.0, in: Fortmann, Harald R./Kolocek, Barbara (Hrsg.), Arbeitswelt der Zukunft, Wiesbaden 2018, 299-315.

Weber, Robert/Kiefner, Alexander/Jobst, Stefan, Künstliche Intelligenz und Unternehmensführung, NZG 2018, 1131-1136.

Weckmüller, Heiko/Büttner, Ricardo, Big Data in der Personalauswahl, Personalmagazin 3/2017, 26-28.

Weibel, Antoinette/Schafheitle, Simon/Ebert, Isabel, Goldgräberstimmung im Personalmanagement? Wie Datafizierungs-Technologien die Personalsteuerung verändern, OrganisationsEntwicklung 3/2019, 23-29.

Weichert, Thilo, Die Verarbeitung von Wearable-Sensordaten bei Beschäftigten, NZA 2017, 565-570.

Weichert, Thilo, Datenschutz-Grundverordnung – arbeitsrechtlich spezifiziert, NZA 2020, 1597-1605.

Weichert, Thilo/Schuler, Karin, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2020_beschdsg_final.pdf.

Werning Sebastian/Berkemeier, Lisa/Zobel, Benedikt/Fitte, Christian/Ickerott, Ingmar/ Thomas, *Oliver,* Smart Glasses als Assistenzsystem in der betrieblichen Einarbeitung, HMD Praxis der Wirtschaftsinformatik 2019, 612-627.

Werther, Simon/Bruckner, Laura (Hrsg.), Arbeit 4.0 aktiv gestalten, Berlin 2018.

Weth, Stephan/Herberger, Maximilian/Wächter, Michael/Sorge, Christoph, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl., München 2019.

Wilkesmann, Maximiliane/Steden, Stephanie/Schulz, Maximilian, Industrie 4.0 – Hype, Hope oder Harm, Arbeit 2018, 129-150.

Winter, Max, Demokratietheoretische Implikationen des Rechts auf informationelle Selbstbestimmung, in: Friedewald, Michael/Lamla, Jörn/Roßnagel, Alexander (Hrsg.), 2017, 37-48.

Wirges, Felix/Ahlbrecht, Marlene/Neyer, Anne-Katrin, HR-Analytics, Wiesbaden 2020.

Wöllhaf, Konrad, Mensch-Roboter-Kollaboration – Wichtiges Zukunftsthema oder nur ein Hype?, in: Buxbaum, Hans-Jürgen (Hrsg.), Mensch-Roboter-Kollaboration, Wiesbaden 2020, 109-115.

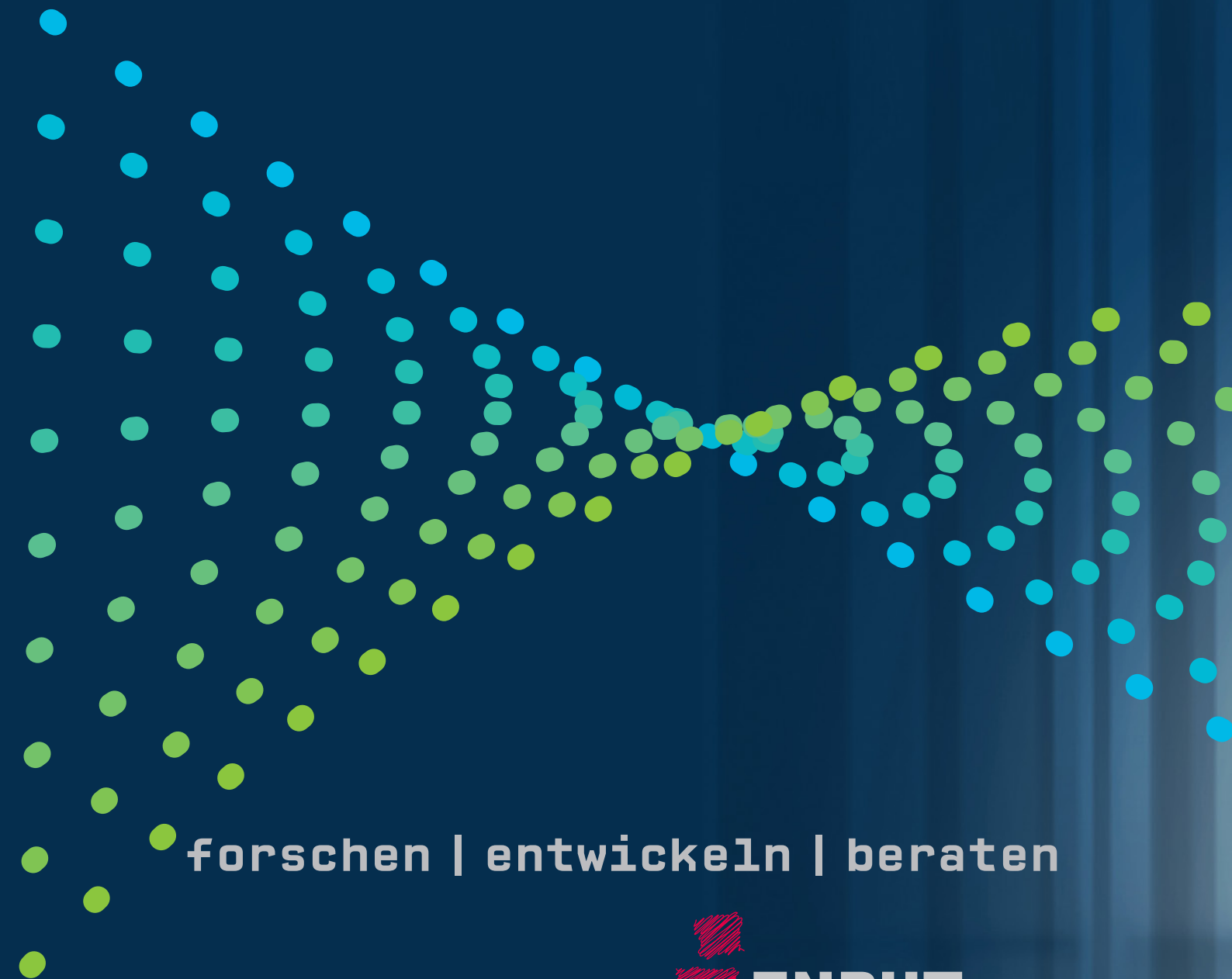
Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 33 Ed. 2020.

Wünschelbaum, Markus, COVID-19: Pandemiebewältigung und Datenschutz, Kollektivvereinbarungen als krisentaugliches DS-GVO-Instrument?, NZA 2020, 612-616.

Wybitul, Tim, Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DSGVO, NZA 2017, 413-419.

Youyou, Wu/Kosinski, Michal/Stillwell, David, Computer-based personality judgments are more accurate than those made by humans, Proceedings of the National Academy of Science of the United States of America (PNAS), vol. 112 no. 4, 1036–1040.

Zanker, Claus, Digitalisierung in der Logistik – Beschäftigung und Qualifikation im Wandel, in: Ernst, Gerhard/Zühlke-Robinet, Klaus/Finking, Gerhard/Bach, Ursula (Hrsg.), Digitale Transformation – Arbeit in Dienstleistungssystemen, Baden-Baden 2020, 55-63.



forschen | entwickeln | beraten

INPUT consulting

INPUT Consulting
Gemeinnützige Gesellschaft für Innovationstransfer,
Post und Telekommunikation mbH

Theodor-Heuss-Str. 2
70174 Stuttgart

Fon: +49 (0) 711 2 62 40 80
Mail: info@input-consulting.de

www.input-consulting.de