Bundesministerium
für Arbeit und Soziales

FORSCHUNGSBERICHT

482

Digitalisierung und Beschäftigtendatenschutz

April 2017

ISSN 0174-4992

Expertise

Digitalisierung und Beschäftigtendatenschutz

erstattet dem
Bundesministerium für Arbeit und Soziales

von

Professor Dr. Rüdiger Krause
Institut für Arbeitsrecht
Georg-August-Universität Göttingen

November 2016

Kurzbeschreibung

Die Expertise legt dar, wie sich neue digitale Technologien auf den Beschäftigtendatenschutz auswirken. Sie behandelt insbesondere Lokalisierungssysteme, biometrische Verfahren zur Identitätskontrolle, die Erfassung mobiler Arbeits- und Projektzeiten, die Messung von Nutzeraktivitäten im Betriebskontext, digitale Assistenzsysteme, die digitale Vernetzung der gesamten Wertschöpfungskette, Sprachgebrauchs- und Stimmungsanalyseverfahren sowie die digitale Auswertung innerbetrieblicher sozialer Netzwerke. Es werden Regelungslücken erörtert und Vorschläge für eine Erweiterung des Beschäftigtendatenschutzes in Deutschland gemacht.

Inhalt

Zusammenfassung

Die Expertise identifiziert vor dem Hintergrund der Digitalisierung des Wirtschafts- und Arbeitslebens folgende neueren technischen Entwicklungen bzw. Anwendungen, die mit einem Kontrollpotenzial im Hinblick auf die Erfassung und Auswertung von Beschäftigtendaten verbunden sind:

- Lokalisierungssysteme
- Biometrische Verfahren
- Mobile Arbeitszeit- und Projektzeiterfassung
- Nutzeraktivitäten an stationären und mobilen Endgeräten
- Industrie 4.0-Anwendungen
- Sonstige inner-und außerbetriebliche Assistenzsysteme
- Sprachgebrauchs- und Stimmungsanalyseverfahren
- Auswertung innerbetrieblicher sozialer Netzwerke
- Fitnessdaten
- Durchleuchtung der Persönlichkeit mittels Sprachanalyseverfahren

Das geltende Recht mit seinen zahlreichen Regelungen auf europäischer, deutscher und internationaler Ebene läuft im Kern darauf hinaus, dass der Arbeitgeber nur dann mit personenbezogenen Daten von Beschäftigten umgehen darf, wenn dies für die Zwecke des Beschäftigungsverhältnisses erforderlich und angemessen (verhältnismäßig) ist. Als konkretisierender Grundsatz bei der Beurteilung von einzelnen neueren Entwicklungen lässt sich insbesondere das grundsätzliche Verbot der Dauerüberwachung von Leistung und/ oder Verhalten des Beschäftigten festhalten. Außerdem müssen grundsätzlich der Zweck des jeweiligen Umgangs mit den Beschäftigtendaten vorab klar festgelegt und die Transparenz der Kontrolle gewahrt werden. Auch wenn sich mit dem geltenden Recht letztlich angemessene Ergebnisse erzielen lassen, sollte die Option in Art. 88 DS-GVO für „spezifischere Vorschriften“ auf der mitgliedstaatlichen Ebene für die Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes genutzt werden. Hierin sollte geregelt werden:

- 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
- Außerdem empfiehlt sich eine Änderung von § 87 Abs. 1 Nr. 6 BetrVG dahingehend, dass der Umgang mit personenbezogenen bzw. personenbeziehbaren Daten von Beschäftigten der Mitbestimmung des Betriebsrats unterliegt.

1. Einleitung

Die Digitalisierung der Arbeitswelt schreitet mit großem Tempo voran. Die zunehmende Durchdringung von Produktions- und Dienstleistungsvorgängen mit Informations- und Kommunikationstechnologien (IKT) verbunden mit einem unaufhörlichen Wachstum datenverarbeitender Prozesse führt zu grundlegenden Veränderungen des Wirtschafts- und Arbeitslebens. Dabei greifen mehrere Entwicklungsstränge ineinander: Erstens die permanente Steigerung der Leistungsfähigkeit von IKT im Hinblick auf die Erfassung analoger Informationen, ihre Umwandlung in digitale Daten sowie ihre Speicherung und Auswertung;[1] zweitens die organisatorische Umgestaltung von Arbeitsabläufen sowie die Entwicklung neuer Geschäftsmodelle. Beide Treiber bewirken, dass im Zusammenhang mit betrieblichen Prozessen eine noch nie dagewesene Menge an Daten erhoben und verarbeitet wird. Diese Entwicklung bezieht sich nicht nur auf den industriellen Bereich, der unter dem Schlagwort „Industrie 4.0" vielfach im Vordergrund steht, sondern ergreift in einem mehr oder weniger starken Maße alle Bereiche des Arbeitslebens und damit insbesondere auch große Teile des Dienstleistungssektors, in dem mittlerweile fast drei Vierteil der Erwerbstätigen arbeiten.[2] Bei diesen Abläufen werden häufig nicht lediglich reine Betriebsdaten erhoben und ausgewertet. Vielmehr hat der ubiquitäre Einsatz von IKT bei Produktions- und Dienstleistungsvorgängen zur Folge, dass auch die Menge der personenbezogenen Daten von Beschäftigten, die erfasst und verarbeitet werden, ständig anwächst.

Dabei lassen sich phänomenologisch drei Grundkonstellationen des Umgangs mit Beschäftigtendaten unterscheiden: Zum einen kann die Erhebung von solchen Daten eine bloße Begleiterscheinung der Optimierung von betrieblichen Prozessen sein, deren eigentliches Ziel in der Steigerung der Effektivität technischer oder logistischer Abläufe liegt. Zum anderen können die technischen Möglichkeiten aber auch gezielt dazu genutzt werden, die Leistung und/oder das Verhalten von Beschäftigten zu steuern und zu überwachen. Gleichsam dazwischen liegt die Fallgruppe, in denen die Daten von Beschäftigten, die zunächst zur Prozessoptimierung generiert worden sind, anschließend bewusst zur Leistungs- bzw. Verhaltenskontrolle verwendet werden.

Dies alles ist im Grundansatz nicht neu. Die jeweils zur Verfügung stehenden technischen Möglichkeiten wurden seit jeher nicht nur zur Substitution menschlicher Arbeit und zur Steigerung der Effizienz, sondern auch zur Überwachung der Beschäftigten verwendet, um das Transformationsproblem der Umwandlung menschlicher Arbeitskapazität in ökonomisch verwertbare Arbeitsresultate zu bewältigen.[3] Die geradezu exponentiell

---

[1] Pars pro toto sei die Entwicklung des neuen Chips „Pascal" durch das kalifornische Unternehmen NVIDIA erwähnt, dessen Rechenleistung durch den Einsatz von fast 4.000 Rechenkernen und 15 Milliarden Transistoren mit 21,2 Billionen Operationen pro Sekunde (21,2 TFlops) in eine neue Dimension vorstößt und Anwendungen wie künstliche Intelligenz, Deep Learning und 3D-Grafik beschleunigen soll, vgl. http://www.heise.de/newsticker/meldung/GTC-2016-Nvidia-enthuellt-Monster-Chip-Pascal-mit-16-GByte-HBM2-und-bis-zu-3840-Kernen-3163143.html.

[2] IAB (Hrsg.), Daten zur kurzfristigen Entwicklung von Wirtschaft und Arbeitsmarkt (Stand: 8.6.2016).

[3] Vgl. Pfeiffer, Technisierung von Arbeit, in: Böhle/Voß/Wachtler, Handbuch Arbeitssoziologie (2010), S. 231-261 (231).

anwachsenden Möglichkeiten der Erfassung und Auswertung von Beschäftigtendaten mithilfe immer komplexerer Analyse-Algorithmen (*Data Mining*, *Big Data*) bei vergleichsweise geringen Kosten führen indes zu verschärften Risiken für die Beschäftigten unter dem Blickwinkel des Persönlichkeits- und Datenschutzes. Vor diesem Hintergrund hat das Grünbuch des BMAS „Arbeiten 4.0“ zu Recht die Leitfrage aufgeworfen: „Wie müssen die Regelungen des Beschäftigtendatenschutzes ausgestaltet werden, um die Interessen der Arbeitnehmerinnen und Arbeitnehmer angemessen zu schützen?“.[4]

Die vorliegende Expertise soll dazu beitragen, auf diese Fragestellung aus rechtswissenschaftlicher Perspektive Antworten zu formulieren. Sie folgt dabei dem in der Leistungsbeschreibung formulierten grundsätzlichen Ziel eines angemessenen Ausgleichs zwischen dem berechtigten Interesse des Arbeitgebers, betriebliche Prozesse zu verbessern und die Leistung der Beschäftigten zu kontrollieren, und dem Interesse der Arbeitnehmerinnen und Arbeitnehmer[5] an einem Schutz ihrer Persönlichkeit im Zusammenhang mit der von ihnen ausgeübten Beschäftigung, wobei dieser Interessenausgleich auch den Herausforderungen eines immer schnelleren digitalen Wandels standhalten muss.

Im Einzelnen soll zunächst auf einer rechtstatsächlichen Ebene ermittelt werden, welche neueren technischen Entwicklungen mit Bezug auf den Beschäftigtendatenschutz in den betrieblichen Alltag Einzug gehalten haben oder zumindest zu erwarten sind (unter II). Auf der Grundlage dieses Befundes ist sodann zu untersuchen, ob das geltende Recht die Interessen der Beteiligten angemessen austariert (unter III). Schließlich soll der Frage nachgegangen werden, ob es auf der Ebene des deutschen Rechts einen Fortentwicklungsbedarf gibt, der sich selbstverständlich in den Grenzen des Unionsrechts, konkret nunmehr der ab dem 25. Mai 2018 geltenden Europäischen Datenschutz-Grundverordnung (DS-GVO)[6] zu halten hat (unter IV).

2. Neuere technische Entwicklungen mit Kontrollpotenzial

Obgleich das traditionelle Thema der Überwachung von Arbeitnehmern durch Videokameras in der gerichtlichen Praxis nach wie vor eine erhebliche Rolle spielt,[7] konzentrieren sich die folgenden Überlegungen doch primär auf neuere technische Entwicklungen, die im Beschäftigungszusammenhang ein Kontrollpotenzial entfalten. Der Schutz der Daten natürlicher Personen soll nach der erklärten Philosophie der neuen DS-GVO zwar „technologieneutral“ sein, was mit dem Ziel begründet wird, hierdurch ein „ernsthaftes Risiko einer Umgehung der Vorschriften“ zu vermeiden.[8] Daran ist richtig, dass sich ein effektiver Datenschutz nicht darauf beschränken darf, lediglich den zu einem

---

4 BMAS (Hrsg.), Grünbuch „Arbeiten 4.0“ (2015), S. 67.

5 Im Folgenden wird um der besseren Lesbarkeit willen nur von Arbeitnehmern gesprochen sowie im Übrigen nicht näher zwischen Arbeitnehmern und Beschäftigten differenziert.

6 ABlEU 2016 Nr. L 119/1.

7 Vgl. BAG 21.6.2012 – 2 AZR 153/11, BAGE 142, 176 = NZA 2012, 1025; BAG 21.11.2013 – 2 AZR 797/11, BAGE 146, 303 = NZA 2014, 243.

8 So Erwägungsgrund 15 DS-GVO.

bestimmten Zeitpunkt erreichten Stand der Technik zu berücksichtigen. Vielmehr muss der Datenschutz zukunftsoffen gestaltet sein, um auch künftige Risiken als Folge der technischen Weiterentwicklung von vornherein rechtlich einzufangen. Ohne eine nähere Betrachtung der technischen Möglichkeiten zur Überwachung von Beschäftigten als Regulierungskontext kann indes weder eine realistische Einschätzung dieser Risiken für den Persönlichkeits- und Datenschutz noch eine angemessene rechtliche Architektur entwickelt werden.[9] Dabei kommt es freilich regelmäßig nicht auf alle Details der verwendeten Technologien an, sondern darauf, welche konkreten Aspekte der Persönlichkeit der Arbeitnehmer von einer Kontrolltechnik betroffen werden, weil aus datenschutzrechtlicher Perspektive stärker die Wirkung auf die Beschäftigten und weniger die genaue Funktionsweise der eingesetzten Technik relevant ist.

2.1 Lokalisierung von Beschäftigten

Die Lokalisierung von Beschäftigten durch digitale Techniken ist keineswegs neu. Allerdings erlaubt der technische Fortschritt eine immer feinmaschigere Feststellung ihres konkreten Aufenthaltsortes einschließlich der Erstellung von Bewegungsprofilen. Zum besseren Verständnis empfiehlt es sich, zwischen der Lokalisierung innerhalb und außerhalb der Betriebsstätte zu unterscheiden.

2.1.1 Innerhalb der Betriebsstätte

Innerhalb von Betriebsstätten kommt im Allgemeinen die RFID-Technik[10] zum Einsatz.[11] Eine RFID-Anwendung besteht zunächst aus einem Lesegerät (Erfassungsgerät) und einem Transponder (auch RFID-Tag). Sofern ein Transponder in den Empfangsbereich eines Lesegeräts kommt, wird mithilfe eines elektromagnetischen Feldes eine berührungslose Kommunikation ausgelöst. So wird dem Transponder durch das Lesegerät Energie zugeführt, die den Transponder sodann in die Lage versetzt, dem Lesegerät gespeicherte Daten zu übermitteln, die häufig nur in einer bestimmten, weltweit einmaligen Identifikationsnummer (Code) bestehen. Regelmäßig ist das Lesegerät mit einer Datenbank verbunden, die den Code mit weiteren Informationen verknüpft. Schon auf dem RFID-Tag selbst können aber personenbezogene Daten unmittelbar fest gespeichert werden, die dann durch das Erfassungsgerät ausgelesen werden. Passive Transponder ohne eigene Energieversorgung haben nur eine geringe Reichweite (einige Millimeter bis wenige Meter). Aktive Transponder mit eigener Energieversorgung erlauben eine größere Reichweite (bis 100 m). Zudem können solche Transponder gegebenenfalls weitere Informationen über den Gegenstand oder die Person, die mit dem RFID-Tag versehen worden ist, aufnehmen und zu einem späteren Zeitpunkt an ein anderes Lesegerät übermitteln. Allerdings sind aktive Transponder deutlich teurer und bislang offenbar weniger verbreitet.

---

[9] In diesem Sinne auch WHW/Herberger, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014), A.IV. Rn. 2 f. im Hinblick auf die „Internet-Grundgegebenheiten“. Ferner Sydow/Kring, Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug, ZD 2014, 271-276.

[10] Radio Frequency Identification.

[11] Zu den technischen Grundlagen http://emf3.bundesnetzagentur.de/pdf/RFID-BNetzA.pdf.

Im Arbeitsleben werden RFID-Anwendungen augenscheinlich häufig zur Zeiterfassung genutzt, indem etwa ein Mitarbeiterausweis mit einem RFID-Tag ausgestattet und der Ausweis zu Beginn und Ende des Dienstes vor ein Lesegerät gehalten wird, um die Information über diese Zeitpunkte in der angeschlossenen Datenbank mit den Daten über die Identifikation des Mitarbeiters zu verknüpfen. Weiter kann auf diese Weise der Zutritt zu bestimmten Räumlichkeiten dadurch geregelt werden, dass etwa nur Personen mit einer in der Datenbank hinterlegten Berechtigung der Zugang automatisch gestattet wird, während die Räumlichkeit ansonsten versperrt bleibt.

Je mehr sichtbare oder auch unsichtbare Lesegeräte an den unterschiedlichsten Stellen in der Betriebsstätte installiert sind, desto stärker kann aber auch der konkrete Bewegungsablauf eines Mitarbeiters, der seinen Dienstausweis permanent mit sich führt, festgehalten und nachverfolgt werden. Hierdurch kann etwa der Rundgang eines Wachmanns oder die Durchführung einer Routineuntersuchung durch einen Wartungstechniker kontrolliert werden. Entsprechendes gilt für die Häufigkeit und Dauer des Besuches sanitärer Einrichtungen.[12] Verstärkt werden kann dieser Effekt noch dadurch, dass der Mitarbeiter nicht darüber informiert wird, dass ein ihm ausgehändigter und mitzuführender Gegenstand (etwa ein Kleidungsstück) ein RFID-Tag enthält. Aus den USA und auch aus Schweden sind darüber hinaus schon Fälle bekannt geworden, in denen sich Personen, teilweise auch Arbeitnehmer, „freiwillig" einen RFID-Tag mit dem Ziel haben implantieren lassen, sich hierdurch unabhängig von der Mitführung eines gesonderten Gegenstandes im Hinblick auf einen Zutritt oder einen Aufenthalt als berechtigt identifizieren zu können. Um dieser Praxis entgegenzuwirken, haben mehrere US-amerikanische Bundestaaten bereits Regelungen erlassen, die es einem Arbeitgeber untersagen, ein entsprechendes Ansinnen an Bewerber oder Arbeitnehmer zu richten.[13]

2.1.2 Außerhalb der Betriebsstätte

Außerhalb der Betriebsstätte ist zunächst die Mobilfunkendgerät-Ortung (Handy-Ortung) zu nennen, die angesichts der heutzutage praktisch flächendeckenden Ausstattung von mobilen Beschäftigten mit Smartphones von besonderem Interesse ist. Insoweit bieten die Netzbetreiber oder Dritte den Inhabern von Mobilfunkverträgen sog. Location-based Services (LBS) an, mit deren Hilfe der jeweilige Standort eines Handys in Echtzeit übermittelt werden kann, wobei das Ziel zumeist darin besteht, dem Nutzer für seinen jeweiligen Standort nützliche Informationen zu übermitteln. Als Technik dient herkömmlich die Ortung mittels des GSM-Standards,[14] auf dessen Grundlage das D-Netz und das E-Netz betrieben werden und das (weltweit) den größten Verbreitungsgrad hat. Im Einzelnen ergibt sich die Ortungsmöglichkeit daraus, dass jedes im Stand-by-Modus betriebene Mobilfunkgerät, das aufgrund seiner IMSI[15] grundsätzlich eindeutig identifiziert werden kann, automatisch mit einer eindeutig identifizierbaren Location Area verbunden ist und somit zu jedem beliebigen Zeitpunkt festgestellt werden kann, in welcher Location

---

[12] Vgl. Gola, Datenschutz bei der Kontrolle „mobiler" Arbeitnehmer – Zulässigkeit und Transparenz, NZA 2007, 1139-1144 (1140); ders., Die Ortung externer Beschäftigter, ZD 2012, 308-311.

[13] Vgl. http://www.ncsl.org/research/telecommunications-and-information-technology/radio-frequency-identification-rfid-privacy-laws.aspx.

[14] Global System for Mobile Communications.

[15] International Mobile Subscriber Identity.

Area sich das Endgerät gerade befindet, wobei die Genauigkeit (allerdings nur) wenige hundert Meter beträgt.[16]

Eine noch genauere Ortung ist auf der Grundlage von GPS[17] möglich. Hierzu bedarf es zunächst eines GPS-Empfangsgerätes, das in der Lage ist, seinen eigenen Aufenthaltsort mithilfe von im Weltraum platzierten Satelliten bis auf wenige Meter genau zu bestimmen. Dieses Gerät wird sodann mit einem aktiven Sender kombiniert, der die ermittelten Positionsdaten später oder gegebenenfalls auch in Echtzeit weitergibt. GPS-Empfangschips befinden sich praktisch in allen modernen Smartphones, aber auch in zahlreichen anderen Geräten (z.B. Tablets, Navigationsgeräte).

Entsprechende Anwendungen werden mittlerweile verbreitet beim Flottenmanagement eingesetzt, um zu jedem beliebigen Zeitpunkt den Aufenthaltsort eines Lkw oder Pkw bzw. die gefahrene Route bestimmen zu können, wobei auf diese Weise mit einiger Sicherheit auch der jeweilige Aufenthaltsort des Fahrers festgestellt werden kann.[18] Entsprechendes gilt für Geld- und Werttransporte. Für die Zwecke der Lokalisierung von Fahrzeugen wird aber offenbar auch auf Dienste auf der Basis von GPRS[19] zurückgegriffen.[20] Eine spezielle Anwendungsform ist das sog. Geofencing, durch das ein gedachter räumlicher Bereich abgegrenzt werden kann, dessen Überschreiten durch das GPS-Gerät zur automatischen Übermittlung einer gespeicherten Information, aber auch zu weiteren Aktionen (z. B. Aktivierung einer Wegfahrsperre) führen kann.

2.2 Biometrische Verfahren

Weitere Entwicklungen mit Relevanz für den Beschäftigtendatenschutz betreffen Fortschritte bei biometrischen Systemen, die für die Authentifizierung und Autorisierung von Arbeitnehmern nutzbar gemacht werden können. Dabei kann grundsätzlich an physiologische oder verhaltensbezogene Merkmale angeknüpft werden. Im Einzelnen geht es darum, bestimmte Merkmale einer Person mithilfe von Sensoren aufzunehmen, die erhobenen Daten zu einem Extrakt zu verarbeiten und schließlich einen Vergleich zwischen dem Merkmalsextrakt und den in einer Datenbank hinterlegten Merkmalen durchzuführen, um bei einer hinreichenden Übereinstimmung der Datensätze eine Personenidentität bestätigen zu können.

Zu erwähnen ist in diesem Zusammenhang der kontaktlose dreidimensionale Fingerabdruck[21] und die 3D-Handgeometrie,[22] aber auch die Stimmerkennung[23] sowie die

---

16 Eine noch genauere Lokalisierung ist mithilfe eines IMSI-Catchers möglich. Diese Technik spielt im Beschäftigungskontext aber soweit ersichtlich keine Rolle.

17 Global Positioning System.

18 Vgl. ArbG Kaiserslautern 27.8.2008 – 1 BVGa 5/08, Juris; ArbG Dortmund 12.3.2013 – 2 BV 196/12, NZA-RR 2013, 474 (GPS-gestütztes Fleetboard-Management).

19 General Packet Radio Service.

20 Vgl. BAG 26.9.2012 – 4 AZR 782/10, AP TVG § 1 TVG Bewachungsgewerbe Nr. 25.

21 Koller, Kontaktlose dreidimensionale Erfassung eines Fingerabdrucks, DuD 2011, 175-178.

22 Drahanský/Dvořák/Váňa, Personenerkennung mittels 3D Handgeometrie, DuD 2011, 169-174.

23 Tillenburg, Stimmt die Stimme?, DuD 2011, 197-199.

Nutzerauthentifizierung anhand des Tippverhaltens[24]. Weitere Beispiele sind die Gesichtserkennung (2D und 3D), die Augenerkennung (Iris oder Retina) sowie die Venengeometrie (Handinnenfläche oder Handrücken).[25] So soll beim Flughafen Berlin-Brandenburg International (BBI) für die Authentifizierung beim Zugang zu sicherheitsrelevanten Bereichen die Venengeometrie in der Handinnenfläche als Identitätsmerkmal genutzt werden.[26]

2.3 Überwachung des Arbeitsverhaltens

Die prinzipielle größte Relevanz dürfte allen digitalen Techniken zukommen, die das Arbeitsverhalten der Beschäftigten („Performance") über eine Feststellung des bloßen Aufenthaltsorts hinaus kontrollieren sollen oder zumindest können.

2.3.1 Mobile Arbeitszeit- und Projektzeiterfassung

Zunächst geht es um solche Systeme, deren Funktion (nur) darin besteht, die traditionellen handschriftlichen Aufzeichnungen („Stundenzettel") durch eine Eingabe in mobile Endgeräte zu ersetzen, wobei die erhobenen Daten entweder zu einem späteren Zeitpunkt über eine stationäre Schnittstelle ausgelesen oder bei einer permanenten Internetanbindung direkt an die betriebliche EDV übermittelt werden. Hierdurch können je nach dem Umfang der (manuell) eingegebenen Daten und der Verknüpfungen dieser Daten Arbeitszeit- und Projektzeitnachweise erstellt werden, um hiermit Abrechnungen im Außenverhältnis gegenüber Kunden vornehmen zu können. Zugleich können die Daten im Innenverhältnis zu den Beschäftigten für die Arbeitskontenführung, die Entgeltberechnung sowie die Reisekostenabrechnung genutzt werden.

2.3.2 Nutzeraktivitäten an stationären und mobilen Endgeräten

Weiter sind solche Anwendungen zu erwähnen, mit denen das Nutzerverhalten an stationären und mobilen digitalen Endgeräten als solches umfassend dokumentiert und ausgewertet werden kann. Die insoweit vorhandenen technischen Möglichkeiten sind nicht etwa nur für staatliche Stellen oder IT-Spezialisten verfügbar, sondern problemlos auf dem freien Markt erhältlich.

Wohl am deutlichsten bringt dies der Hersteller des offenbar verbreiteten Spionageprogramms mSpy[27] zum Ausdruck, der sein Produkt als „ultimatives Monitoring-Tool für alle Devices" anpreist.[28] Dieses Programm kontrolliert zum einen sämtliche Vorgänge auf Computer-Desktops. Hierzu gehören automatische Aufnahmen

---

[24] Dotzler, Eine datenschutzrechtlich motivierte Untersuchung Tippverhalten basierender Authentifizierungssysteme, DuD 2011, 192-196.

[25] Umfassende Auflistung bei WHW/Kramer, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014), B.IV. Rn. 2; ferner Hornung/Steidle, Biometrie am Arbeitsplatz - sichere Kontrollverfahren versus ausuferndes Kontrollpotential, AuR 2005, 201-207.

[26] Weigmann et al., Biometrie am BBI – Chancen und Randbedingungen, DuD 2011, 179-182.

[27] Hierbei handelt es sich um das britische Unternehmen Bitex Group Ltd., was sich allerdings nur über Umwege herausfinden lässt.

[28] https://www.mspy.com.de/.

(*Screenshots*), sodass der Arbeitgeber jederzeit sehen kann, womit sich der Nutzer beschäftigt. Auf diese Weise erhalten Unternehmer, so die Produktbeschreibung, ein klares Bild darüber, was genau ihre Angestellten während der Arbeitszeit tun, ohne ständig vor Ort sein zu müssen. Weiter registriert mSpy jede einzelne vom Nutzer gedrückte Taste und zwar auch dann, wenn die Eingabe sofort wieder gelöscht wurde (*Keylogging*). Auf diese Weise kann kontrolliert werden, nach welchen Suchbegriffen auf Google oder anderen Suchmaschinen gesucht wird. Ferner können alle Chat-Mitteilungen des Nutzers unabhängig davon gesichtet werden, über welchen Instant-Messenger sie verschickt wurden. Dasselbe gilt für alle gängigen E-Mail-Services, sodass sämtliche ein- und ausgehenden E-Mail einschließlich aller Anhänge umfassend ausgelesen und darauf bezogene Aktionen des Nutzers nachvollzogen werden können. Sodann dokumentiert mSpy, wie lange ein Nutzer während einer Computer-Session aktiv oder inaktiv ist. Weitere Funktionen betreffen eine Auflistung sämtlicher Programme und Anwendungen, die auf dem Computer zum Einsatz kommen. Dasselbe gilt für den gesamten Internetverlauf. Bei alledem lassen sämtliche Funktionalitäten die normale Nutzeraktivität vollkommen unberührt und werden nicht angezeigt, sodass sie von einem mit dem Endgerät tätigen Mitarbeiter grundsätzlich nicht wahrgenommen werden können. Ähnliche Anwendungen werden auch von anderen Herstellern angeboten.[29]

Für Smartphones und Tablets enthält mSpy zahlreiche vergleichbare Funktionalitäten. So können alle empfangenen/getätigten Anrufe samt Dauer und Zeitmarken abgerufen werden, alle Text- und Multimedianachrichten gelesen werden, die von dem Nutzer des Zielgerätes gesendet oder empfangen wurden, der Inhalt aller ein- und ausgehenden E-Mails kontrolliert werden[30], die GPS-Position des Endgeräts geortet werden,[31] alle besuchten URL-Adressen im Browser des Smartphones eingesehen werden, sämtliche Nutzeraktivitäten über Skype, WhatsApp, iMessage und Viber erfasst werden sowie auf alle im Adressbuch eingetragenen Kontakte und Termine zugegriffen werden.

Diese verschiedenen Anwendungen setzen freilich voraus, dass der Arbeitgeber ein entsprechendes Programm auf dem Endgerät installiert, was wohl nur in Betracht kommt, wenn es sich um ein dem Beschäftigten zur Verfügung gestelltes Gerät handelt. Demgegenüber dürfte es kaum vorkommen, dass es dem Arbeitgeber gelingt, auf einem eigenen Endgerät des Arbeitnehmers, dass dieser für dienstliche Zwecke einsetzt (*Bring Your Own Device*) ein solches Programm zu laden. Immerhin zeigt eine Entscheidung des ArbG Augsburg, dass die heimliche Installation und Anwendung eines Kontrollprogramms auf dem Arbeitsplatzrechner eines Mitarbeiters nicht als pure Phantasie abgetan werden kann.[32]

---

[29] So etwa vom (zurückhaltender auftretenden) israelischen Unternehmen NICE Systems (mit einem Büro auch in Frankfurt), vgl. http://www.nice.com/engage/customer-analytics/desktop-analytics.

[30] Produktbeschreibung: „Mit dieser Smartphone-App stellen Sie sicher, dass die Zeit Ihrer Angestellten nicht mit dem Schreiben privater E-Mails verschwendet wird."

[31] Produktbeschreibung: „Finden Sie heraus, ob Ihr Angestellter wirklich im Verkehrsstau steckt."

[32] Vgl. ArbG Augsburg 4.10.2012 – 1 BV 36/12, Juris.

2.3.3 Industrie 4.0-Anwendungen

Ein weiteres bedeutsames Feld betrifft die unter dem Schlagwort „Industrie 4.0“ verlaufende Entwicklung zu einer umfassend vernetzten Fabrik.[33] In dieser „Smart Factory“ sollen in Maschinen und Werkstücke eingebettete Systeme (*Cyber-Physical Systems*) einen möglichst großen Teil der Wertschöpfungskette durch einen automatisierten Datenaustausch selbsttätig steuern, um hierdurch Flexibilität und Effizienzgewinne zu erzielen.[34] Das Leitbild besteht in einer digitalen Organisation und Steuerung des Wertschöpfungsvorgangs, der sich auf den gesamten Lebenszyklus von Erzeugnissen erstreckt und vertikal von der Produktentwicklung über Produktion und Logistik bis hin zum Vertrieb und Service sowie horizontal über die Unternehmensgrenzen hinweg von Zulieferern und Dienstleistern über das Herstellungsunternehmen bis hin zum Endkunden und zum Recycling reicht. Um die erforderlichen Abläufe umfassend und in Echtzeit steuern zu können, bedarf es der massenhaften Erhebung und Analyse von Daten. Soweit es sich hierbei um reine Betriebsdaten oder definitiv anonymisierte Daten von Beschäftigten handelt, ist dies datenschutzrechtlich unproblematisch. Tatsächlich geht aber man davon aus, dass mit neuartigen Industrie 4.0-Anwendungen in vielen Fällen zwangsläufig auch personenbezogene Daten von Beschäftigten zumindest miterhoben werden.[35]

Hauptgrund hierfür ist der Umstand, dass es bei Industrie 4.0 keineswegs nur um eine Perfektionierung der M2M-Kommunikation geht, sondern anders als bei der – niemals realisierten – Vision der CIM (*Computer Integrated Manufactory*) das Ziel nicht in der menschenleeren Fabrik, sondern in der optimalen Interaktion zwischen Mensch und Maschine liegt.[36] An dieser augenscheinlich immer wichtiger werdenden Schnittstelle kommt eine ständig wachsende Anzahl unterschiedlicher mobiler Systeme zum Einsatz.

Neben den beinahe schon „klassischen“ Geräten wie Smartphone, Tablet und Notebook geht es hierbei zunehmend um Rechner, die unmittelbar am Körper getragen werden (*Wearables*)[37] und deren Funktion darin besteht, die betrieblichen Arbeitsabläufe zu

---

[33] Hierzu grundlegend Bauernhansl/ten Hompel/Vogel-Heuser (Hrsg.), Industrie 4.0 in Produktion, Automatisierung und Logistik (2014).

[34] Die hohe Zahl der mittlerweile verfügbaren IP-Adressen (340 Sextillionen) setzt der technischen Weiterentwicklung insoweit keine Grenzen.

[35] Zum Folgenden etwa Hofmann, Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0, ZD 2016, 12-17; Kopp/Sokoll, Wearables am Arbeitsplatz – Einfallstor für Alltagsüberwachung ?, NZA 2015, 1352-1359; Wulf/Burgenmeister, Industrie 4.0 in der Logistik – Rechtliche Hürden beim Einsatz neuer Vernetzungstechnologien, CR 2015, 404-412.

[36] Dazu zahlreiche Beiträge in Bauernhansl/ten Hompel/Vogel-Heuser (Hrsg.), Industrie 4.0 in Produktion, Automatisierung und Logistik (2014), ab S. 451 ff.

[37] Vgl. die „offizielle“ Definition von Steve Mann (1998): Wearable computing facilitates a new form of human--computer interaction comprising a small body--worn computer (e.g. user--programmable device) that is always on and always ready and accessible. In this regard, the new computational framework differs from that of hand held devices, laptop computers and personal digital assistants (PDAs). The ``always ready'' capability leads to a new form of synergy between human and computer, characterized by long-term adaptation through constancy of user--interface.“, http://wearcam.org/wearcompdef.html.

erleichtern und zu verbessern (z.B. Datenbrille,[38] intelligenter Handschuh[39] etc.). So kann den einzelnen Beschäftigten durch Wearables ebenso wie durch Smartphones oder Tablets vorgegeben werden, welche konkreten Arbeitsaufgaben zu erledigen sind (digitale Weisungen). Zugleich können entsprechende Systeme auch spezielle Vorschläge unterbreiten, wie etwa eine Wartung oder eine Montage vorzunehmen ist. Gegebenenfalls werden detaillierte Arbeitsschritte vorgegeben und ihre Ausführung durch Kameras überwacht. Weiter kann der Standort von Spezialwerkzeugen oder Experten angezeigt werden, die für eine schnelle Störungsbeseitigung beigezogen werden müssen. Ferner kann zugleich festgehalten werden, wie schnell der Arbeitnehmer einen Auftrag erledigt hat und wie nachhaltig etwa eine Störungsbeseitigung war. Alle diese Daten können wiederum zusammengeführt werden, um bei der Aufgabenverteilung je nach der Schwierigkeit und Dringlichkeit der zu lösenden Arbeitsaufgabe den jeweils am besten geeigneten Mitarbeiter auszuwählen und schwächere Mitarbeiter für einfachere Routineaufgaben vorzusehen.

Derartige Anwendungen setzen regelmäßig individualisierte Nutzerkonten voraus, bei denen die verfügbaren Daten zusammengeführt und ausgewertet werden, um daraus eine optimale Aufgabenerfüllung bzw. Verteilung der zu erledigenden Aufgaben zu generieren. Dies wird nicht zuletzt dadurch erleichtert, dass jedes Endgerät auf der Basis von GSM oder UMTS[40] über eine eigene und unverwechselbare IMEI[41] verfügt, die eine eindeutige Zuordnung gewährleistet.

Eine weitere an Bedeutung zunehmende Anwendung stellt die vorausschauende Wartung (*Predictive Maintenance*) dar. Hierbei geht es darum, Wartungen aufgrund einer Selbstdiagnose von Maschinen und Fahrzeugen individuell vornehmen zu können und hierdurch unnötige Stillstände und Schäden zu vermeiden, um auf diese Weise Ressourcen zu schonen und Kosten zu sparen. Diese Systeme können so ausgestaltet sein, dass sie zugleich die Daten von Beschäftigten (Maschinenbenutzer, Lkw-Fahrer) mit dem Ziel erheben, die Wartungsvorgänge weiter zu optimieren oder auch unmittelbar das Arbeitsverhalten der Mitarbeiter zu kontrollieren.[42]

Eine zunehmend wichtigere Form der Mensch-Maschine-Interaktion besteht ferner im Einsatz von Industrierobotern, die nur dann gefahrlos unmittelbar mit Menschen zusammenarbeiten können, wenn sie ihre Umgebung umfassend kontrollieren und damit auch die körperlichen Eigenheiten und Verhaltensweisen der Beschäftigten jederzeit durch Kameras, Sensoren o.ä. hinreichend erfassen und die erhobenen Daten anschließend in eigene Aktionen umsetzen.

---

38 Siehe dazu das Pilotprojekt von DHL einer Augmented-Reality-unterstützten Kommissionierung (*Vision Picking*) in einem niederländischen Lagerbetrieb, http://www.dpdhl.com/de/presse/pressemitteilungen/2015/dhl_testet_augmented_reality-anwendung.html.

39 Zu letzterem siehe http://www.proglove.de/; ferner Handelsblatt Nr. 99 vom 25.5.2016, S. 22.

40 Universal Mobile Telecommunications System.

41 International Mobile Station Equipment Identity.

42 Vgl. Wulf/Burgenmeister, Industrie 4.0 in der Logistik – Rechtliche Hürden beim Einsatz neuer Vernetzungstechnologien, CR 2015, 404-412 (409).

2.3.4 Sonstige inner- und außerbetriebliche Assistenzsysteme

Neben den Neuerungen im industriellen Bereich ist der Blick auch auf den in der Digitalisierungsdebatte nicht selten vernachlässigten Dienstleistungssektor zu lenken. Als Prototyp für eine bis ins Detail digital durchstrukturierte Prozesskontrolle können die bei *Amazon* eingesetzten Handscanner gelten.[43] Diese Geräte werden von sog. Pickern genutzt, deren Aufgabe darin besteht, in den weiträumigen Lagerhallen die einzelnen Produkte einzusammeln und zu den Packstationen zu transportieren. Die Handscanner, die bei nahezu jedem einzelnen Arbeitsschritt eingesetzt werden, dienen zum einen der Prozessoptimierung. Zum anderen wird aber auch darüber berichtet, dass auf diese Weise die individuelle Arbeitsleistung der Beschäftigten gemessen und aufgrund der Vielzahl der gesammelten Daten die gesamte während der Arbeitszeit erbrachte Performance für das Management völlig transparent wird, sodass sowohl eine auf den einzelnen Mitarbeiter gemünzte individuelle Beurteilung als auch ein systematischer Leistungsvergleich aller Mitarbeiter untereinander ermöglicht wird. So werden offenbar Inaktivitätsprotokolle geführt.[44] Mit Hilfe des augenscheinlich auch in Deutschland eingesetzten „Anytime Feedback Tool" können Lob über bzw. Kritik an den Kollegen unmittelbar an Vorgesetzte weitergeleitet werden, wobei solche Mitteilungen offenbar durch Voreinstellungen erleichtert werden.[45]

Schließlich können Wearables auch außerhalb der Betriebsstätte verwendet werden, sodass je nach eingesetzter Technik die einzelnen Arbeitsschritte gegebenenfalls visualisiert und in Echtzeit aus der Entfernung nachvollzogen werden können.

Im Übrigen gilt für alle auf der Basis von Mobilfunk arbeitenden Anwendungen, dass es auf diesem Gebiet mit der Entwicklung neuer Generationen von Mobilfunkstandards explosionsartige Leistungssteigerungen zu erwarten sind. So wird im Anschluss an den 2G-Standard GSM (zweite Generation) und den aktuellen 3G-Standard UMTS (dritte Generation) gegenwärtig der 4G-Standard LTE-Advanced[46] (vierte Generation) aufgebaut, der die Datenübertragungsrate von wenigen Megabit auf 3 Gigabit pro Sekunde erweitern und dadurch die permanente Verbindung mobiler Endgeräte mit dem Internet („always on") noch einmal ganz erheblich effektivieren soll. Darüber hinaus wird schon jetzt am 5G-Standard gearbeitet, dessen technische Eigenschaften unter anderem darin bestehen soll, dass weltweit 100 Milliarden Mobilfunkgeräte in Echtzeit vernetzt werden können.

---

[43] Zum Folgenden Staab/Nachtwey, Die Digitalisierung der Dienstleistungsarbeit, APuZ 2016, 24-31.

[44] http://www.sueddeutsche.de/wirtschaft/online-versandhaendler-auch-deutsche-amazon-mitarbeiter-berichten-von-schikane-1.2611333.

[45] So lautet eine derartige (zumindest in den USA verwendete) Voreinstellung zu einer Beschwerde über einen Kollegen: „Ich mache mir Sorgen über seine mangelnde Flexibilität und sein offenes Klagen über kleinere Aufgaben."; vgl. http://www.sueddeutsche.de/wirtschaft/mitarbeiterkontrolle-petzen-per-software-1.2611874

[46] Long Term Evolution.

2.3.5 Sprachgebrauchs- und Stimmungsanalyseverfahren

Ein weiteres Feld digitaler Technologie wird mit dem Bereich der Sprachgebrauchs- und Stimmungsanalyse betreten, die in unterschiedlichen Schattierungen auftritt, wobei es hier zunächst nur um die Kontrolle und Verbesserung des Arbeitsverhaltens insbesondere von Call-Center-Mitarbeitern gehen soll.[47]

Ein Analyseverfahren ist das sog. *Keyword Spotting*. Durch entsprechende Algorithmen kann ermittelt werden, welche Namen und Begriffe in Gesprächen mit welcher Häufigkeit in welchem Kontext verwendet werden.[48] Auf diese Weise kann etwa herausgefunden werden, ob ein Call-Center-Mitarbeiter ein zu vermarktendes Produkt in einem Telefonat hinreichend oft genannt oder etwa ein Konkurrenzprodukt mit negativen Konnotationen belegt hat. Entsprechende Gesprächsanalysen können dem Beschäftigten zu einem späteren Zeitpunkt gespiegelt werden, um ihn zu einem aus Sicht des Arbeitgebers „besseren" Sprachgebrauch anzuhalten. Eine weitere Anwendung baut auf dem Umstand auf, dass die menschliche Stimme aufgrund ihrer Modulation Informationen unabhängig vom Inhalt transportiert, die vom Empfänger unbewusst wahrgenommen werden und ihn in eine positive oder negative Grundstimmung versetzen.[49] Diesen psychologischen Mechanismus kann man sich zunutze machen, indem einem Call-Center Mitarbeiter digital unterstützt bestimmte positive Schlüsselerlebnisse vor Augen geführt werden, die ihn selber in eine positive Grundstimmung versetzen, um hierdurch auch den Anrufer positiv zu stimmen.

2.4 Auswertung innerbetrieblicher sozialer Netzwerke

Ein vergleichsweise neuer Trend bildet die zunehmende Etablierung sozialer Netzwerke innerhalb von Unternehmen bzw. Konzernen, deren Nutzung von allen Beschäftigten erwartet wird, um die innerbetriebliche Kommunikation zu fördern. Insoweit ist zunächst klarzustellen, dass es im Spannungsverhältnis von sozialen Medien und Beschäftigtendaten zahlreiche unterschiedliche Fallkonstellationen gibt.[50] Im Folgenden nicht angesprochen werden sollen die öffentlichen sozialen Netzwerke wie etwa Facebook, Twitter und WhatsApp. Bei diesen Netzwerken hat der Arbeitgeber praktisch nur dann Zugang zur Kommunikation von Arbeitnehmern, wenn er ebenfalls gleichsam „horizontal" zu den Teilnehmern des sozialen Netzwerks gehört und auf diese Weise zu den Daten des Arbeitnehmers vordringt oder aber er sich gleichsam „vertikal" über den Account des Arbeitnehmers anmeldet, weil ihm dieser die Zugangsdaten „freiwillig" zur Verfügung gestellt hat bzw. er ebenfalls „vertikal" über das Nutzerverhalten deshalb informiert ist, weil die Aktivitäten des Arbeitnehmers auf einem digitalen Endgerät stattfinden, das mit einer entsprechenden Spionagesoftware im oben beschriebenen Sinne ausgestattet ist. Stattdessen sollen die vom Arbeitgeber selber aufgesetzten sozialen Netzwerke thematisiert werden, die sich von vornherein zumindest im Wesentlichen nur an die Beschäftigten richten. Tatsächlich belegen Daten, dass diese Form der innerbetrieblichen

---

[47] Zur darüber hinausgehenden Durchleuchtung der gesamten Persönlichkeit siehe unten sub II 6.

[48] Zum Folgenden Kiesche/Wilke, Neue Überwachungsformen in Call-Centern, CuA 2012, 5-12; siehe auch Däubler, Gläserne Belegschaften?, 6. Aufl. (2015), Rn. 378g-378h.

[49] Näher Zoebisch, Stimmungsanalyse durch Call-Center, DuD 2011, 394-397.

[50] Dazu umfassend Thüsing/Wurth (Hrsg.), Social Media im Betrieb (2015).

Kommunikation immer wichtiger wird und die mittlerweile schon „klassische“ Form der Kommunikation durch E-Mail zunehmend ergänzt oder sogar ersetzt.[51]

Sofern der Arbeitgeber das System selbst administriert, sind verschiedene Anwendungen möglich. Neben dem Zugriff auf einzelne Kommunikationsvorgänge ist in jüngster Zeit vor allem die Herstellung eines sozialen Graphen des Unternehmens (*Enterprise Social Graph*) in das Blickfeld geraten.[52] Hierbei geht es um die datenmäßige Erfassung und Darstellung der gesamten unternehmensinternen Kommunikationsstruktur als solcher. Auf diesem Graphen aufbauend kann die innerbetriebliche Kommunikation wiederum beeinflusst werden, indem jedem Nutzer qua Data Mining aus Milliarden von Einzeldaten die für ihn (wahrscheinlich) relevantesten Aktivitäten anderer Nutzer zugänglich gemacht werden.[53] Auch kann mit entsprechenden Tools die Stellung einzelner Beschäftigten etwa als zentral oder nur am Rande stehend analysiert werden, um hierdurch Meinungsführer oder Gruppenbildungen zu identifizieren. Eine weitere Anwendung, die auf der Analyse des sozialen Graphen aufbaut, betrifft die Erstellung eines Engagement Scores, der sich aus den Nutzeraktivitäten sowie den Reaktionen der anderen Belegschaftsmitglieder ergibt und der anzeigen soll, wie wertvoll die Beiträge eines Mitarbeiters für die innerbetriebliche Kommunikation (und damit offenbar auch die betriebliche Wertschöpfung) sind.

2.5 Fitnessdaten

Eine vergleichsweise neue gesellschaftliche Entwicklung ist die „Quantified-Self“-Bewegung. Hierbei geht es um die permanente Vermessung des eigenen Selbst (*Self-Tracking*) mithilfe digitaler Technologien, die am Körper getragen werden (Wearables), um auf diese Weise einen bewussteren Umgang mit den eigenen physiologischen Gegebenheiten zu erzielen und das Gesundheitsbewusstsein zu fördern (*Self Knowledge Through Numbers*). Insoweit finden sich erste Überlegungen wird, ob und inwieweit die daraus gewonnenen Daten auch für das betriebliche Gesundheitsmanagement[54] oder gegebenenfalls noch darüber hinausgehend für personalpolitische Entscheidungen verwendet werden dürfen.

2.6 Durchleuchtung der Persönlichkeit qua Sprachanalyseverfahren

Zu den neuesten Trends gehören schließlich Sprachanalyseprogramme. Insoweit sei das Tool *Precire* erwähnt, das von dem 2012 in Aachen gegründeten Unternehmen *Psyware* angeboten wird.[55] Das Programm basiert auf dem Grundphänomen, dass sich jeder Mensch

---

[51] Thüsing/Wurth (Hrsg.), Social Media im Betrieb (2015), Kap. 1 Rn. 3 ff.

[52] Zum Folgenden Höller, Mining the Enterprise Social Graph, CuA 2016, 8-13.

[53] Ein Beispiel ist das Microsoft-Programm „Delve“, wobei die Produktbeschreibung auf der Support-Seite von Microsoft jeder Beschreibung spottet: „Delve hilft Ihnen, die Informationen ermitteln, die wahrscheinlich am interessantesten Sie sofort - über Office 365 sein. Suchen nach Informationen zu Personen - sowie durch Personen - und können Sie andere Personen Sie finden.“ (Wortlaut im Original beibehalten).

[54] Dazu Kopp/Sokoll, Wearables am Arbeitsplatz – Einfallstor für Alltagsüberwachung ?, NZA 2015, 1352-1359 (1356-1357).

[55] Zum Folgenden https://www.psyware.de/.

zwar in seiner Wortwahl und Sprechweise unterscheidet, dass sich aber gleichwohl unter Heranziehung linguistischer, psychologischer und kommunikationsbezogener Merkmale gewisse Verhaltensmuster identifizieren lassen, in denen bestimmte Persönlichkeitsmerkmale zum Ausdruck kommen.

Grundlage des Programms ist ein Referenzdatensatz, der in einem ersten Schritt aus einer großen Anzahl von gesprochener Sprache und geschriebenen Texten generiert worden ist und in dem aus der Art und Weise des Sprechens und Schreibens bestimmte Persönlichkeitsgruppen gebildet worden sind. *Precire* zerlegt nun in einem zweiten Schritt die von einer unbekannten Person gesprochenen und geschriebenen Worte in zehntausende kleiner digitaler Bausteine und vergleicht die hierdurch gewonnenen Daten anhand von rund 180.000 Parametern mit dem Referenzdatensatz. Anhand dieses Ähnlichkeitsvergleichs werden sodann Analysen und Vorhersagen über die sprachliche Kompetenz, die emotionale Verfasstheit wie auch über bestimmte Eigenschaften dieser Person getroffen (z.B. „sehr", „wenig" oder „nicht zielorientiert"). Mittlerweile haben augenscheinlich mehrere Unternehmen diese Technologie bei Beschäftigten bzw. Bewerbern eingesetzt.[56]

3. Gegenwärtiger Rechtsrahmen

Im Anschluss an diesen rechtstatsächlichen Befund soll nunmehr der Frage nachgegangen werden, wie diese verschiedene Entscheidungsformen nach geltendem Recht zu beurteilen sind, weil sie erst auf dieser Basis ein etwaiger Bedarf nach weiteren Regelungen ermitteln lässt. Hierbei ist vorab der allgemeine Rechtsrahmen zu skizzieren, bevor dann die einzelnen Gestaltungen beurteilt werden. Außerdem sind die individuellen Rechte der Betroffenen sowie die Beteiligungsrechte des Betriebsrats in die Betrachtungen einzubeziehen.

3.1 Allgemeine Grundlagen

Das geltende Beschäftigtendatenschutzrecht ist mit dem allgemeinen Datenschutzrecht untrennbar verwoben und teilt hierdurch dessen äußerliche Unübersichtlichkeit. Im Einzelnen wird der gegenwärtige Rechtsrahmen für den Schutz von Beschäftigtendaten durch eine Vielzahl von Regelungen und Prinzipien auf europäischer, nationaler und internationaler Ebene aufgespannt.[57]

3.1.1 Europäisches Recht

Im Hinblick auf das europäische Recht ist auf der primärrechtlichen Ebene Art. 8 der EU-Grundrechtecharta (GRC) zu nennen, der ein Grundrecht auf den Schutz der sie betreffenden personenbezogenen Daten enthält. Dieses Grundrecht verpflichtet zwar gemäß Art. 51 Abs. 1 GRC unmittelbar nur die Union selbst (Organe, Einrichtungen sonstige Stellen) sowie die Mitgliedstaaten bei der Durchführung des Unionsrechts. Das

---

[56] Die Homepage von Psyware nennt u.a. die Unternehmen Fraport, Kienbaum und Randstad.

[57] Zum Folgenden statt aller Däubler, Gläserne Belegschaften?, 6. Aufl. (2015), Rn. 39-66.

Grundrecht entfaltet aber auch in privatrechtlichen Beziehungen dadurch Wirkung, dass einschlägiges Sekundärrecht existiert (dazu sogleich) und das auf einen Streitfall anzuwendende nationale Recht somit europarechtskonform einschließlich der Berücksichtigung des Datenschutzgrundrechts auszulegen ist. Dabei ist insbesondere in Rechnung zu stellen, dass auch europarechtliche Grundrechte im Rahmen ihres Anwendungsbereichs eine Schutzpflichtfunktion enthalten.[58]

Mit Art. 16 Abs. 1 AEUV stellt das Primärrecht eine weitere Regelung bereit, die auf den Schutz von personenbezogenen Daten abzielt. Die Interpretation dieser Vorschrift bereitet gewisse Schwierigkeiten, weil sie anders als Art. 8 GRC keine näheren Schrankenbestimmungen enthält und deshalb vor dem Hintergrund von Art. 52 Abs. 2 GRV prima facie als ein schrankenloses Grundrecht erscheint. Tatsächlich geht die überwiegende Ansicht davon aus, dass es sich bei Art. 16 Abs. 1 AEUV zwar um ein echtes Grundrecht handelt, dieses Grundrecht aber durch die Bestimmungen der GRC näher ausgeformt wird.[59] Im Übrigen ist von einer Art Wechselwirkung zwischen dem Grundrecht und dem Sekundärrecht auszugehen, weil es zwar einerseits des konkretisierenden Sekundärrechts bedarf, um das Datenschutzgrundrecht effektiv ausüben zu können,[60] andererseits aber die Bestimmungen des Sekundärrechts im Lichte des Grundrechts auszulegen sind[61].

Auf der sekundärrechtlichen Ebene ist zunächst die Datenschutzrichtlinie 95/46/EG zu nennen, die noch bis zum 24. Mai 2018 gilt[62] und die bei der Auslegung des BDSG zu beachten ist.[63] Zu den Kerngedanken der Datenschutzrichtlinie gehört der auch aus dem deutschen Recht (dazu sogleich) geläufige Grundsatz des Verbots der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt (Art. 7 DSRL). Im Hinblick auf den Grad der Harmonisierung hat der EuGH in mehreren Entscheidungen zu erkennen gegeben, dass er die DSRL nicht lediglich als eine Mindestharmonisierung begreift, sondern grundsätzlich im Sinne einer Vollharmonisierung versteht, die allerdings Ausnahmen und Umsetzungsspielräume eröffnet,[64] wobei die Interpretation der nicht ganz klaren Aussagen des EuGH allerdings im Einzelnen umstritten ist.[65] Weitere sekundärrechtliche Regelungen betreffen den Umgang mit personenbezogenen Daten im Bereich der elektronischen Kommunikation (RL 2002/58/EG).

3.1.2 Deutsches Recht

Auf der Ebene des deutschen Rechts wird der Datenschutz verfassungsrechtlich vor allem durch das vom BVerfG entwickelte Recht auf informationelle Selbstbestimmung

---

58 Siehe (zu Art. 8 GRC) etwa Streinz/Streinz, EUV/AEUV, 2. Aufl. (2012), Art. 8 GR-Charta Rn. 6.

59 Streinz/Herrmann, EUV/AEUV, 2. Aufl. (2012), Art. 16 AEUV Rn. 4 ff.

60 Vgl. Streinz/Herrmann, EUV/AEUV, 2. Aufl. (2012), Art. 16 AEUV Rn. 4 ff.

61 Zu Letzterem EuGH 13.5.2014 – C-131/12, NJW 2014, 2257 Rn. 68 m.w.N. – Google Spain.

62 Vgl. Art. 94 Abs. 1 DS-GVO.

63 Vgl. BAG 7.2.2012 – 1 ABR 46/10, BAGE 140, 350 = NZA 2012, 744 Rn. 31; BAG 16.2.2012 – 6 AZR 553/10, BAGE 141, 1 = NZA 2012, 555 Rn. 26.

64 EuGH 6.11.2003 – C-101/01, Slg. 2003, I-12971 Rn. 96 – Lindquist; EuGH 24.11.2011 – C-468/10 u. 469/10, Slg. 2011, I-12181 – ASNEF und FECEMD; aktuell EuGH 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 – Breyer.

65 Eingehend Pötters, Grundrechte und Beschäftigtendatenschutz (2013), S. 239-245.

(Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) überwölbt,[66] dem das BVerfG vor einigen Jahren das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zur Seite gestellt hat[67]. Einfachrechtlich stellt das BDSG das Zentrum des Datenschutzes dar, das ebenfalls vom Grundsatz des Verbots des Umgangs mit personenbezogenen Daten mit Erlaubnisvorbehalt beherrscht wird (§ 4 Abs. 1 BDSG). Dabei kann sich eine Erlaubnis zur Erhebung, Verarbeitung und Nutzung solcher Daten grundsätzlich aus dem BDSG selbst oder einer anderen Rechtsvorschrift oder aber einer wirksamen Einwilligung des Betroffenen ergeben, wobei letztere den Vorgaben des § 4a BDSG genügen, also insbesondere auf einer freien Entscheidung des Betroffenen beruhen muss.

Ob es eine derartige freie Entscheidung im Rahmen von Arbeitsverhältnissen bzw. in Bewerbungssituationen überhaupt geben kann, ist freilich seit jeher umstritten.[68] Im Allgemeinen spricht die Imparität zwischen den Parteien eher dafür, eine freie Entscheidung zu verneinen. Ausgeschlossen ist sie allerdings nicht. So kann eine freie Entscheidung etwa dann angenommen werden, wenn der Umgang mit personenbezogenen Daten für den Arbeitnehmer bei objektiver Betrachtung vorteilhaft ist oder nur eine geringe Eingriffstiefe vorliegt.[69] Dementsprechend hat BAG im Zusammenhang mit der kurzfristigen Sichtbarkeit eines Arbeitnehmers in einem Werbefilm für die Produkte eines Unternehmens die Wirksamkeit einer Einwilligung durch den Betroffenen anerkannt.[70] Da die Einwilligung nach allgemeiner Ansicht jederzeit ohne einen Grund mit Wirkung für die Zukunft widerrufen werden kann,[71] ist ihre Bedeutung im Arbeitsverhältnis als einem Dauerschuldverhältnis freilich von vornherein begrenzt. Hinzu kommt, dass zahlreiche Formen der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von Beschäftigten nur dann effektiv sind, wenn die gesamte Belegschaft erfasst wird. Damit ist schon ein einziger bzw. sind zumindest einige wenige „Akkordstörer" in der Lage, die Wirkung einer Anwendung erheblich zu beeinträchtigen, wenn der Arbeitgeber lediglich auf die Einwilligung der Betroffenen setzt. Daher dürfte das Vorhandensein einer gesetzlichen oder sonstigen normativen Erlaubnis in der Praxis vielfach eine größere Rolle für die Frage der Rechtmäßigkeit des Umgangs mit personenbezogenen Beschäftigtendaten spielen.

Insoweit enthält das Gesetz seit der Novelle von 2009 mit § 32 BDSG erstmals eine Vorschrift, welche ausdrücklich die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses[72] adressiert. Die in dieser Bestimmung enthaltene Erweiterung des Anwendungsbereichs durch Abs. 2 auf manuell erhobene, verarbeitete

---

66 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1.

67 BVerfG 27.2.2008 – 1 BvR 370/07 u.a., BVerfGE 120, 274.

68 Siehe dazu nur Gola/Schomerus, BDSG, 11. Aufl. (2012), § 4a Rn. 22.

69 Vgl. DKWW/Däubler, BDSG, 5. Aufl. (2016), § 4a Rn. 23.

70 BAG 11.12.2014 – 8 AZR 1010/13, BAGE 150, 195 = NZA 2015, 604 (für § 22 KUG). Die Wirksamkeit einer Einwilligung bei einer Schrankkontrolle ohne weiteres bejahend BAG 13.12.2007 – 2 AZR 537/06, NZA 2008, 1008 Rn. 37.

71 Siehe etwa Gola/Schomerus, BDSG, 11. Aufl. (2012), § 4a Rn. 38; Simitis/Simitis, BDSG, 8. Aufl. (2014), § 4a Rn. 94; Taeger/Gabel/Taeger, BDSG, 2. Aufl. (2013), § 4a Rn. 81. Unter völliger Ausblendung der Literatur einschränkend dagegen BAG 11.12.2014 – 8 AZR 1010/13, BAGE 150, 195 = NZA 2015, 604 Rn. 38 ff. (Widerruf nur nach Maßgabe einer Interessenabwägung).

72 Zum Beschäftigtenbegriff siehe § 3 Nr. 11 BDSG.

oder genutzte Daten ist im vorliegenden Zusammenhang allerdings bedeutungslos. Zentraler Maßstab für die Rechtmäßigkeit des Umgangs mit Beschäftigtendaten ist der Verhältnismäßigkeitsgrundsatz, der mit der ausdrücklichen Nennung der Erforderlichkeit im Gesetzestext seinen Niederschlag gefunden hat.[73] Jede Erhebung, Verarbeitung oder Nutzung von personenbezogenen Beschäftigtendaten ist von vornherein gemäß § 32 Abs. 1 S. 1 BDSG nur dann rechtmäßig, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach der Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Darüber hinaus bedarf es nach allgemeiner Ansicht einer Angemessenheitsprüfung und damit einer Bewertung der gegenläufigen Interessen von Arbeitgeber und Arbeitnehmer.[74] Der Umgang mit personenbezogenen Daten von Beschäftigten muss somit für die Erreichung eines auf das Beschäftigungsverhältnis bezogenen rechtmäßigen Zwecks nicht nur geeignet und erforderlich, sondern über den Wortlaut von § 32 Abs. 1 S. 1 BDSG hinaus auch verhältnismäßig im engeren Sinne sein. In diese Struktur des Verhältnismäßigkeitsgrundsatzes lassen sich die allgemeinen Grundsätze der Datenvermeidung und Datensparsamkeit gemäß § 3a BDSG problemlos integrieren. Im Übrigen wird man einen Kern der Persönlichkeitssphäre des Arbeitnehmers anzuerkennen haben, in den auch bei gewichtigen ökonomischen Interessen zu Arbeitgebers nicht eingegriffen werden kann.[75] Zudem gilt das persönlichkeitsrechtliche Verbot der Totalüberwachung.[76] Soweit es um das repressive Aufdecken von Straftaten geht, richtet sich der Umgang mit personenbezogenen Daten nach der spezielleren Norm des § 32 Abs. 1 S. 2 BDSG.

Ein Zusatzfrage besteht seit jeher darin, ob und inwieweit Kollektivvereinbarungen, d. h. neben Tarifverträgen vor allem Betriebsvereinbarungen, als Erlaubnistatbestand im Sinne von § 4 Abs. 1 BDSG fungieren können und vor allem ob auf diesem Wege das Schutzniveaus des BDSG gegebenenfalls unterschritten werden kann. Das BAG hat sich in einer älteren Entscheidung für die Statthaftigkeit einer gewissen Unterschreitung des gesetzlichen Schutzniveaus ausgesprochen[77] und hält an dieser Judikatur bis in die jüngste Zeit offenkundig fest[78]. Große Teile des Schrifttums gehen dagegen mit beachtlichen Gründen davon aus, dass untergesetzliche Normen zwar die Vorgaben des BDSG konkretisieren, nicht aber „nach unten“ davon abweichen können.[79]

---

[73] Simitis/Seifert, BDSG, 8. Aufl. (2014), § 32 Rn. 9.

[74] Statt vieler Wybitul, Wie viel Arbeitnehmerdatenschutz ist "erforderlich"?, BB 2010, 1085-1089; die Rolle des Verhältnismäßigkeitsgrundsatzes als Prüfungsmaßstab für den Umgang mit Arbeitnehmerdaten hervorhebend bereits BAG 22.10.1986 – 5 AZR 660/85, BAGE 53, 226 = NZA 1987, 415.

[75] Vgl. Däubler, Gläserne Belegschaften, 6. Aufl. (2015), Rn. 119 ff.

[76] Vgl. BAG 29.6.2004 – 1 ABR 21/03, BAGE 111, 173 = NZA 2004, 1278.

[77] BAG 27.5.1986 – 1 ABR 48/84, BAGE 52, 88 = NZA 1986, 643.

[78] Vgl. BAG 15.4.2014 – 1 ABR 2/13 (B); BAGE 148, 26 = NZA 2014, 551 Rn. 49; BAG 25.9.2013 – 10 AZR 270/12, BAGE 146, 109 = NZA 2014, 41 Rn. 32; bestätigend bereits BAG 30.8.1995 – 1 ABR 4/95, BAGE 80, 366 = NZA 1996, 218 (unter II 3).

[79] Simitis/Scholz/Sokol, BDSG, 8. Aufl. (2014), § 4 Rn. 17, DKWW/Weichert, BDSG, 5. Aufl. (2016), § 4 Rn. 2.

Von ganz erheblicher Bedeutung ist weiter der Grundsatz der Zweckbindung, der sich u. a. aus § 4 Abs. 3 S. 1 Nr. 2 und § 28 Abs. 1 S. 2 BDSG sowie mittelbar auch aus § 31 BDSG ergibt. Danach dürfen personenbezogene Daten grundsätzlich nur für bestimmte Zwecke erhoben, verarbeitet oder genutzt werden, wobei der Zweck bereits vor der Datenerhebung festzulegen ist. Hierdurch soll eine Vorratsdatenspeicherung verhindert werden. Allerdings ist eine Verwendung rechtmäßig erhobener Daten für einen anderen Zweck gemäß § 28 Abs. 2 Nr. 1 i.V.m. Abs. 1 S. 1 Nr. 2 BDSG im Allgemeinen zulässig. Dies ist dann der Fall, wenn die Verarbeitung für einen anderen Zweck zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ob eine solche nachträgliche Zweckänderung auch im Hinblick auf Daten zulässig ist, die für Zwecke des Beschäftigungsverhältnisses im Sinne von § 32 BDSG erhoben worden sind, ist umstritten.[80] Die Rechtsprechung scheint eine solche „Umwidmung“ zu bejahen, ohne diese Frage aber näher zu thematisieren.[81]

Hinzu treten die Vorschriften, die der Transparenz der Datenerhebung für den Betroffenen dienen, nämlich insbesondere das grundsätzliche Gebot der Direkterhebung (§ 4 Abs. 2 BDSG) sowie die Pflicht zu bestimmten Informationen (§ 4 Abs. 3 BDSG). Außerdem sind gegebenenfalls spezielle Rechtmäßigkeitsanforderungen zu beachten (§ 6b BDSG bei der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen; § 6c BDSG im Hinblick auf den Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien).

Ferner wird derjenigen Stelle, die selbst oder im Auftrag personenbezogene Daten erhebt verarbeitet oder nutzt, durch § 9 BDSG auferlegt, die technischen und organisatorischen Maßnahmen zu treffen, um die Einhaltung des Gesetzes sowie die in der Anlage genannten Anforderungen zu gewährleisten. Diese Vorschrift fordert als Flankierung eines effektiven Datenschutzes somit eine hinreichende Datensicherheit.[82]

Für den Bereich des Telekommunikationsrechts greifen unter Umständen spezielle Vorschriften zum Fernmeldegeheimnis bzw. zum Datenschutz (§§ 88 bis 107 TKG sowie §§ 11 bis 15a TMG), die in ihrem jeweiligen Anwendungsbereich den allgemeinen Vorschriften des BDSG vorgehen (§ 1 Abs. 3 S. 1 BDSG).

3.1.3 Internationales Recht

Eine weitere Rechtsquelle stellt Art. 8 EMRK dar. Ein Teilaspekt des in dieser Bestimmung verankerten Rechts u.a. auf Achtung des Privatlebens ist nach der Rechtsprechung des EGMR der Bereich des Datenschutzes bzw. der informationellen Selbstbestimmung.[83] Darüber hinaus enthält dieses Grundrecht gemäß der Judikatur des EGMR nicht nur einen Schutz gegenüber staatlichen Eingriffen, sondern verpflichtet die Mitgliedstaaten auch

---

[80] Befürwortend Däubler, Gläserne Belegschaften, 6. Aufl. (2015), Rn. 418 ff.; abl. DKWW/Wedde, BDSG, 5. Aufl. (2016), § 32 Rn. 134 ff. (etwas anders aber Rn. 9).

[81] Vgl. LAG Köln 29.9.2014 – 2 Sa 181/14, NZA-RR 2015, 128: Nutzung von der Qualitätskontrolle dienenden Datenbankeingaben für Arbeitszeitkontrolle.

[82] Abzugrenzen von der Informationssicherheit, die sich auf die Verfügbarkeit, Integrität und Vertraulichkeit elektronischer Informationen jeglicher Art bezieht.

[83] Vgl. EUArbR/Schubert (2016), Art. 8 EMRK Rn. 7 m.w.N.

dazu, ihre Bürger vor Übergriffen anderer privater Akteure zu schützen. Damit kann Art. 8 EMRK insbesondere auch in Arbeitsbeziehungen Bedeutung erlangen und zur Notwendigkeit der Verankerung eines Schutzes des Arbeitnehmers vor Überwachungsmaßnahmen durch den Arbeitgeber in Rechtsordnungen der Mitgliedstaaten beitragen. Allerdings hat sich der EGMR zur konkreten Reichweite des Schutzes in einer aktuellen Entscheidung vergleichsweise zurückhaltend geäußert,[84] sodass sich unter diesem rechtlichen Blickwinkel im Allgemeinen kein höheres Schutzniveau als aus den zuvor geschilderten rechtlichen Grundlagen ergibt.

3.2 Konkrete Beurteilung neuerer Gestaltungen nach geltendem Recht

Vor dem Hintergrund des soeben skizzierten allgemeinen Rechtsrahmens kann nunmehr danach gefragt werden, wie die einzelnen neueren Gestaltungen digitalisierter Kontrollmechanismen nach bestehendem Recht zu beurteilen sind.

3.2.1 Lokalisierung von Beschäftigten

Im Hinblick auf die Lokalisierung von Beschäftigten fehlt es zwar bislang weitgehend an konkretisierender Rechtsprechung[85]. Allerdings wird diese Fallgruppe schon seit längerem im Schrifttum diskutiert, sodass sich gewisse Grundsätze herausgebildet haben, die zumindest überwiegend konsentiert werden.[86]

3.2.1.1 Telekommunikations- und Telemedienrecht

Datenschutzrechtlich geht es bei der „klassischen" Handyortung via Location Based Services (LBS) zunächst um die Reichweite der telekommunikations- und telemedienrechtlichen Sondervorschriften, die in ihrem Anwendungsbereich wie erwähnt den Rückgriff auf das BDSG ausschließen (§ 1 Abs. 3 S. 1 BDSG). Im Grundsatz sind bei diesem Lokalisierungsverfahren vier Beteiligte zu unterscheiden, nämlich neben dem Arbeitgeber und dem Arbeitnehmer auch der Netzbetreiber (Telekommunikations-Diensteanbieter) und der LBS-Anbieter (Telemedien-Diensteanbieter). Dabei muss grundsätzlich für jede verantwortliche Stelle eigenständig geklärt werden, ob der Umgang mit personenbezogenen Daten rechtmäßig ist.[87] Weiter kann dieses Verfahren praktisch nur durchgeführt werden, wenn der Arbeitgeber zum einen mit dem Netzbetreiber einen

---

[84] Vgl. EGMR 12.1.2016 – 61496/08, DuD 2016, 395 – Bärbulescu/Romania: Gerichtliche Billigung des Zugriffs des Arbeitgebers auf dienstlichen Internet-Account des Arbeitnehmers, um unbefugte umfangreiche Privatnutzung während der Arbeitszeit nachzuweisen, ist zulässig.

[85] Eine Ausnahme ist LAG Baden-Württemberg 25.10.2002 – 5 Sa 59/00, Juris (GPS-Überwachung).

[86] Zum Folgenden aktuell Göpfert/Pabst, Digitale Überwachung mobiler Arbeit, DB 2016, 1015-1020; ferner WHW/Byers, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014), B.V. Rn. 1 ff.; Gola, Datenschutz bei der Kontrolle „mobiler" Arbeitnehmer – Zulässigkeit und Transparenz, NZA 2007, 1139-1144; ders., Die Ortung externer Beschäftigter, ZD 2012, 308-311

[87] Der Netzbetreiber und der LBS-Anbieter sind allerdings häufig identisch.

Mobilfunkvertrag[88] und zum anderen mit dem LBS-Anbieter einen Standortbestimmungsvertrag geschlossen hat.

Die Erhebung der Standortdaten (§ 3 Abs. 1 Nr. 19 TKG) durch den Netzbetreiber als erster Schritt richtet sich nach § 98 TKG und ist zulässig, wenn der Arbeitgeber als Vertragspartner und damit als Teilnehmer (§ 3 Nr. 20 TKG) seine Einwilligung erklärt hat (§ 98 Abs. 1 S. 1 TKG).[89] Der Arbeitgeber muss den Arbeitnehmer als Nutzer des Smartphones (§ 3 Nr. 14 TKG) zwar an sich (über das Unionsrecht in Gestalt von Art. 9 Abs. 1 RL 2002/58/EG hinausgehend) gemäß § 98 Abs. 1 S. 7 TKG über die Einwilligung zur Erhebung der Standortdaten unterrichten. Diese Anforderung betrifft aber nur das Innenverhältnis zwischen Teilnehmer und Nutzer, nicht jedoch die Rechtmäßigkeit des Handelns durch den Netzbetreiber.

Die Rechtmäßigkeit der weiteren Verarbeitung und Nutzung der Standortdaten durch den LBS-Anbieter richtet sich entgegen dem ersten Anschein nicht nach den §§ 11 bis 15a TMG, sondern nach dem BDSG. Soweit im Rahmen eines LBS arbeitgeberbezogene Daten verarbeitet werden, greift der Ausschlusstatbestand des § 11 Abs. 1 Nr. 2 TMG ein, weil es nur um die Steuerung von Arbeits- bzw. Geschäftsprozessen geht. Soweit dagegen arbeitnehmerbezogene Daten verarbeitet werden, handelt es sich um eine Nutzung von Telemedien in einem Arbeitsverhältnis zu einem ausschließlich beruflichen Zweck, sodass § 11 Abs. 1 Nr. 1 TMG zur Unanwendbarkeit der telemedienrechtlichen Sondervorschriften führt. Im Übrigen ist für die Beurteilung der datenschutzrechtlichen Zulässigkeit der Verarbeitung arbeitnehmerbezogener Daten im Rahmen des Vertragsverhältnisses zwischen LBS-Anbieter und Arbeitgeber auf das Innenverhältnis zwischen Arbeitgeber und dem Arbeitnehmer abzustellen.

Wird die Lokalisierung durch GPS vorgenommen, ist das TKG demgegenüber von vornherein nicht anwendbar, weil das GPS selber nicht als Telekommunikationsnetz (§ 3 Nr. 27 TKG) eingestuft werden kann, sondern eine Feststellung der Position durch Dritte nur dadurch möglich ist, dass der Standort eines GPS-Empfangsgeräts durch einen weiteren Sender aktiv übermittelt wird, während § 98 TKG den umgekehrten Fall regelt, dass der Netzbetreiber den Standort eines Mobilfunkendgeräts von sich aus ermittelt.[90]

Falls eine Lokalisierung mittels RFID-Technik stattfindet, geht man im Allgemeinen davon aus, dass kein Telekommunikationsdienst (§ 3 Nr. 24 TKG) vorliegt, sondern der Arbeitgeber mit der Etablierung eines betriebsinternen RFID-Systems als Verwender lediglich eigene Zwecke verfolgt. Damit ist § 98 TKG von vornherein nicht anwendbar.[91]

---

[88] Dies kommt nur bei einem dem Arbeitnehmer überlassenen dienstlichen Mobiltelephon in Betracht. Die Ortung eines dem Beschäftigten gehörenden Endgeräts (BYOD) ist technisch zwar natürlich ebenfalls möglich, praktisch aber ausgeschlossen.

[89] Die in der Literatur vereinzelt unter Berufung auf Art. 9 Abs. 1 RL 2002/58/EG vertretene Sichtweise, nach der die Einwilligung durch den Nutzer genügt (vgl. Geppert/Schütz, BeckTKG-Komm/Braun (2013), § 98 Rn. 13) ist im vorliegenden Kontext unerheblich.

[90] Vgl. Jandt/Schnabel, Location Based Services im Fokus des Datenschutzes, K&R 2008, 723-729.

[91] Näher dazu Jandt/Schnabel, Location Based Services im Fokus des Datenschutzes, K&R 2008, 723-729 (726-727).

3.2.1.2 Fälle gesetzlicher Erlaubnis und Grenzen

Für das Innenverhältnis zwischen Arbeitgeber und Arbeitnehmer spitzt sich somit alles auf die Vorgaben des BDSG zu.[92] Betrachtet man zunächst die Zwecke, für die nach den Vorgaben des § 32 Abs. 1 S. 1 BDSG überhaupt ein Umgang mit personenbezogenen Beschäftigtendaten in Betracht kommt, ist als grundsätzlich zulässiges Ziel einer Ortung zunächst die persönliche Sicherheit des Mitarbeiters zu nennen, also wenn hierdurch etwa eine schnelle Rettung auf einer Bohrinsel oder nach einem Unfall insbesondere mit einem Gefahrguttransport ermöglicht werden soll. In diesen Fällen dient die Datenerhebung und Übermittlung der gefahrlosen Durchführung des Arbeitsverhältnisses.[93] Entsprechendes gilt, wenn es nicht um die Unfallrettung, sondern um den Schutz des Mitarbeiters vor Straftaten Dritter, etwa bei der Durchführung von Geldtransporten oder bei der Beförderung sonstiger wertvoller Güter insbesondere in gefährliche Regionen geht. Im Hinblick auf den Schutz von Arbeitgebereigentum und sonstigen dem Arbeitgeber zuzuordnenden Vermögenswerten (etwa Waren) vor dem Zugriff Dritter scheidet § 32 Abs. 1 BDSG als Rechtfertigungstatbestand dagegen aus, weil hierbei nicht die Durchführung des Beschäftigungsverhältnisses in Rede steht.

Vor diesem Hintergrund wird in der Literatur die Frage diskutiert, ob sich der Arbeitgeber gegebenenfalls auf § 28 Abs. 1 S. 1 Nr. 2 BDSG stützen kann oder ob § 32 BDSG für den Bereich des Arbeitnehmerdatenschutzes diese Vorschrift völlig verdrängt.[94] In diesem Zusammenhang dürfte es weiterhelfen, genauer zu unterscheiden: Wenn es dem Arbeitgeber nur darum geht, bestimmte Betriebsmittel zu sichern, genügt es für die Erreichung dieses (zulässigen) Zwecks regelmäßig, wenn auch nur diese Betriebsmittel lokalisiert werden können. Eine zusätzliche Lokalisierung derjenigen Mitarbeiter, die gezielt oder auch nur zufällig mit den fraglichen Betriebsmitteln umgehen, ist zur Erreichung dieses Zieles dagegen im Allgemeinen nicht erforderlich. Lassen sich bei der Ortung die rein betrieblichen und die personenbezogenen Daten nicht trennen, gebietet es die Grundsätze der Datensparsamkeit (§ 3a BDSG) und der Zweckbindung, dass die gewonnenen Daten nur für die Sicherung bzw. das Wiederauffinden der Betriebsmittel genutzt werden dürfen, nicht aber für eine Leistungs- oder Verhaltenskontrolle der Beschäftigten. Auch wenn eine „Umwidmung" der personenbezogenen Daten gemäß § 28 Abs. 2 BDSG nicht völlig ausgeschlossen ist, wäre sie in diesem Fall doch unverhältnismäßig.

Dieselben Grundsätze müssen dann gelten, wenn der Arbeitgeber sein Eigentum vor einem Zugriff durch die Beschäftigten selbst schützen will. Auch insoweit wird es regelmäßig genügen, wenn die fraglichen Gegenstände als solche geortet werden können, ohne dass es etwa notwendig wäre, Bewegungsprofile aller in einer bestimmten Abteilung tätigen Arbeitnehmer zu erstellen. Gerade bei elektronischen Schutzmaßnahmen zugunsten bestimmter betrieblicher (Wert-)Gegenstände, bei denen im Falle eines unbefugten Entfernens aus einer bestimmten räumlichen Sphäre etwa ein Signal ausgelöst wird (*Geofencing*) wird deutlich, dass zwischen sachbezogenen und personenbezogenen Ortungen zu differenzieren ist und die Lokalisierung von Personen häufig nicht

---

92 Die Sonderregeln über den digitalen Tachographen der VO (EG) Nr. 561/2006 sowie § 21a Abs. 7 ArbZG und § 4 Abs. 3 FPersG bleiben hier unberücksichtigt.

93 WHW/Byers, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014), B.V. Rn. 15.

94 Vgl. WHW/Byers, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014), B.V. Rn. 19 ff.

erforderlich ist und durch die konkrete Ausgestaltung der jeweiligen Schutzmaßnahme problemlos vermieden werden kann, ohne dass die Effektivität der Sicherungsmaßnahmen beeinträchtigt wird.

Als weiterer zulässiger Zweck ist eine Effektivierung der betrieblichen Abläufe anzuerkennen. Dies betrifft etwa das Flottenmanagement eines Speditions- oder Taxiunternehmens. In diesen Fällen kann die Einsatzplanung der Fahrzeuge und die Zuordnung der jeweils zur Verfügung stehenden Fahrer mithilfe von Ortungssystemen gegebenenfalls in Echtzeit unterstützt werden. Entsprechendes gilt für Arbeitnehmer, die in einer bestimmten Region für die Beseitigung von Störungen an Leitungen, auf Baustellen oder in Kundenunternehmen zuständig sind und deren Einsatzplanung optimiert werden soll. Auch wenn in diesen Gestaltungen Vorgänge außerhalb der Betriebsstätte im Vordergrund stehen, können innerhalb einer Betriebsstätte ebenfalls Situationen auftreten, in denen durch Lokalisierung der Mitarbeitereinsatz optimiert wird. Dies kommt etwa in Betracht hinsichtlich des genauen Standorts eines Experten, um bei einer plötzlich auftretenden Störung eines Produktionsprozesses auf einem weitläufigen Betriebsgelände genau denjenigen Mitarbeiter, der über das nötige Know-How zur Störungsbeseitigung verfügt und der am schnellsten zu Stelle sein kann, ausfindig zu machen. Auch in diesen stärker auf konkrete Arbeitnehmer bezogenen Konstellationen ist die Datenerhebung und -verarbeitung auf das für die Aufgabenerfüllung notwendige Maß zu beschränken. So bedarf es im Allgemeinen keiner kontinuierlichen Feststellung des jeweiligen Aufenthaltsorts, um das jeweilige Ziel einer optimalen Einsatzplanung zu erreichen. Vielmehr genügt es etwa in einem Störungsfall, wenn genau in diesem Zeitpunkt die Lokalisierung vorgenommen wird, während es für die Erledigung von Routinearbeiten und damit für den größten Teil des betrieblichen Alltags regelmäßig keine Rolle spielt, wo sich der Experte exakt aufhält.

Eine weitere Fallgruppe betrifft Zugangskontrollen, die durch RFID-Systeme unterstützt werden können, um die Identität desjenigen feststellen, der ein Gelände oder bestimmte Räumlichkeiten betreten will, wobei freilich für jede einzelne Kontrollmaßnahme ein berechtigtes Interesse des Arbeitgebers zu fordern ist. Dies kann für das grundsätzliche Betreten der Betriebsstätte ebenso bejaht werden wie für solche Bereiche oder Räumlichkeiten innerhalb der Betriebsstätte, für die objektiv besondere Sicherheitsanforderungen gelten. Dagegen wäre es unzulässig, ohne ein solches Interesse jeden einzelnen Raum (Büros, Teeküche, Sanitärräum etc.) und Flurabschnitt mit einer entsprechenden Zugangskontrolle zu versehen, um minutiös nachverfolgen zu können, an welchem Ort sich ein Arbeitnehmer während seines Arbeitstages wie lange aufgehalten hat. Insoweit stößt die Lokalisierung von Beschäftigten innerhalb eines räumlichen Bereiches, der keine unterschiedlich schützenswerten Sicherheitszonen aufweist, an rechtliche Grenzen.

Denkbar sind schließlich betriebliche Arbeitsabläufe, bei denen räumlich voneinander entfernte Orte vom selben Mitarbeiter mehr oder weniger regelmäßig aufgesucht werden müssen, etwa ein Rundgang mit Türkontrollen durch Sicherheitspersonal oder die unmittelbare Inaugenscheinnahme eines aus verschiedenen Stufen bestehenden Produktionsvorgangs. In diesen Gestaltungen wäre es ebenfalls zulässig, die Vornahme der für den Betriebsablauf erforderlichen und vertraglich geschuldeten Handlung durch den Beschäftigten mittels einer RFID-gestützten Identitätsfeststellung zu überwachen, während eine Lokalisierung in den dazwischenliegenden Zeiträumen unverhältnismäßig und damit unzulässig wäre.

3.2.1.3 Erlaubnis kraft Einwilligung

Entsprechend den geschilderten allgemeinen Grundsätzen kommt darüber hinaus eine Zulässigkeit der Ortung kraft Einwilligung des bzw. der betroffenen Beschäftigten (§§ 4 Abs. 1, 4a BDSG) in Betracht.[95] Angesichts der hohen Anforderungen, die an die Freiwilligkeit der Entscheidung zu stellen sind, wird man darin eine rechtssichere Grundlage aber regelmäßig nur dann sehen können, wenn die Lokalisierung dem Arbeitnehmer zugutekommt (etwa in riskanten Arbeitskonstellationen seinem eigenen Schutz dient) oder es nur um punktuelle Kontrollen geht (morgendliches Betreten und abendliches Verlassen eines großräumigen Firmengeländes). In denjenigen Gestaltungen, in denen die Lokalisierung einer intensiveren Überwachung des Beschäftigten dient, ist die Freiwilligkeit der Entscheidung als tatsächliche Wirksamkeit der Einwilligung eher zweifelhaft, ohne jedoch per se ausgeschlossen zu sein. Eine konkludente Einwilligung des Beschäftigten kann jedenfalls nicht allein daraus abgeleitet werden, dass Lokalisierungstechniken in der Praxis weit verbreitet sind und der Arbeitnehmer nicht vorsorglich widersprochen hat.[96]

3.2.1.4 Transparenz

Für jede Form der Lokalisierung gilt grundsätzlich das Transparenzprinzip, d.h. der Betroffene ist prinzipiell vorab konkret darüber zu informieren, dass sein Standort festgestellt werden kann. Das mittlerweile verbreitete allgemeine Wissen darüber, dass insbesondere eine Handyortung technisch möglich ist, genügt nicht. Dieses Transparenzgebot ergibt sich für den Bereich der Ermittlung von Standortdaten durch einen Mobilfunknetzbetreiber zunächst aus der bereits erwähnten Pflicht zur Unterrichtung des Arbeitnehmers als Nutzer des Mobilfunkendgerätes durch den Arbeitgeber als Teilnehmer gemäß § 98 Abs. 1 S. 7 TKG über das Vorhandensein einer erteilten Einwilligung.[97] Darüber hinaus hat der Diensteanbieter bei jeder Standortfeststellung, die nicht nur auf dem Endgerät selber angezeigt wird, den Nutzer durch eine Textmitteilung an das Mobilfunkendgerät nach § 98 Abs. 1 S. 2 TKG zu informieren. Diese Regelung dient ausweislich der Gesetzesbegründung der Transparenz bei einer Fremdortung, zu der es deshalb kommen kann, weil der Nutzer nicht zwingend mit dem Teilnehmer, der den Mobilfunkvertrag geschlossen hat, identisch ist.[98] Allerdings kann der Arbeitgeber dem Transparenzgebot, das im BDSG nicht ausdrücklich als allgemeiner Grundsatz geregelt ist, sich aber aus einer Zusammenschau verschiedener

---

[95] WHW/Byers, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014), B.V. Rn. 43. Die an dieser Stelle näher skizzierten Grundsätze gelten auch für die im Folgenden untersuchten Fallgruppen, was aus Raumgründen indes nicht jeweils gesondert wiederholt wird.

[96] Ebenso die Wertung in BVerfG 9.10.2002 – 1 BvR 1611/96 u.a., BVerfGE 106, 28 (46-47), zum vergleichbaren Fall des heimlichen Mithörens eines Telefonats.

[97] Nach vereinzelter Ansicht soll diese Unterrichtungspflicht durch eine analoge Anwendung von § 99 Abs. 1 TKG effektiviert werden, vgl. Säcker/Klesczewski, TKG (2013), § 98 Rn. 11. Danach müsste der Diensteanbieter den Teilnehmer auf dessen Informationspflicht hinweisen und von ihm eine Erklärung in Textform einholen, dass er alle Arbeitnehmer, die das Mobilfunkendgerät nutzen, entsprechend unterrichtet hat.

[98] Vgl. BT-Drucks. 17/5707, S. 79.

Einzelregelungen[99] ergibt,[100] im Innenverhältnis zum Arbeitnehmer auch auf andere Weise Rechnung tragen.

Sofern mobile personenbezogene Speicher- und Verarbeitungsmedien im Sinne von § 6c BDSG verwendet werden, was bei einer GSM-Ortung oder GPS-Ortung stets der Fall ist, treten die dort genannten Informationspflichten noch hinzu.[101] Wird die Lokalisierung mittels RFID-Technik vorgenommen, ist nach wohl überwiegender Ansicht aufgrund der Definition in § 3 Abs. 10 Nr. 2 BDSG, die eine aktive Datenverarbeitung auf dem Datenträger selber fordert, danach zu unterscheiden, ob es sich um einen aktiven Transponder mit einer eigenen Rechnereinheit handelt oder nur um einen passiven Transponder, dessen Daten lediglich ausgelesen werden können.[102] Andere Teile der Literatur wollen dagegen auch passive RFID-Tags unter § 6c BDSG fallen lassen, weil es unter Schutzgesichtspunkten keine Rolle spielen könne, ob die Datenverarbeitung auf dem Datenträger oder im Rechenzentrum der verantwortlichen Stelle stattfinde.[103]

Folgt man der herrschenden Meinung, unterliegen die klassischen Hausausweise, mit denen sich Mitarbeiter beim Zutritt zur Betriebsstätte oder bestimmten Bereichen innerhalb der Betriebsstätte vor einem Lesegerät identifizieren, nicht den zusätzlichen Anforderungen von § 6c BDSG. Ebenfalls von dieser Vorschrift nicht erfasst werden solche Speichermedien, bei denen die Lokalisierung nicht automatisch, sondern erst aufgrund einer Dateneingabe durch den jeweiligen Nutzer erfolgt, wie dies bei einem dem Arbeitnehmer ausgehändigten Notebook der Fall sein kann.[104] Bei einer automatisierten Bestimmung und Übermittlung des jeweiligen Standorts durch eine auf dem Medium stattfindende Datenverarbeitung greift § 6c BDSG dagegen ein. Daher bedarf es grundsätzlich einer Erkennbarkeit des jeweiligen Kommunikationsvorgangs gemäß § 6c Abs. 3 BDSG, etwa durch ein akustisches Signal.

Auch unabhängig von § 6c BDSG ist eine heimliche Lokalisierung von Arbeitnehmern grundsätzlich unzulässig, weil sie zur Durchführung des Beschäftigungsverhältnisses im Allgemeinen nicht erforderlich ist.[105] Dies betrifft insbesondere alle Formen des effektiven Personaleinsatzes, die nicht davon abhängen, dass der Arbeitnehmer über die Bestimmung seines Standorts und dessen Übermittlung an einen Kollegen oder Disponenten im Unklaren gelassen wird. Allerdings hat die Rechtsprechung in eng umgrenzten Ausnahmefällen eine heimliche Videoüberwachung von Beschäftigten zugelassen, wenn dies das einzige Instrument war, um auf andere Weise nicht ermittelbaren Straftaten auf

---

99 Insbesondere §§ 4 Abs. 2 und 3, 34 BDSG.

100 Siehe etwa Brink, in: Wedde (Hrsg.), Handbuch Datenschutz und Mitbestimmung (2016) Rn. B 136 f.

101 Meyer, Mitarbeiterüberwachung: Kontrolle durch Ortung von Arbeitnehmern, K&R 2009, 14-20 (19-20).

102 Ausführlich Gola/Schomerus, BDSG, 11. Aufl. (2012), § 6c Rn. 2 ff.

103 Taeger/Gabel/Zscherpe, BDSG, 2. Aufl. (2013), § 6c Rn. 21 u. 23 f.

104 Vgl. Gola/Schomerus, BDSG, 11. Aufl. (2012), § 6c Rn. 4; Taeger/Gabel/Zscherpe, BDSG, 2. Aufl. (2013), § 6c Rn. 22.

105 Zur Strafbarkeit der Anfertigung von Bewegungsprofilen von Arbeitnehmern mittels GPS-Empfängern durch einen Detektiv gemäß § 44 BDSG BGH 4.6.2013 – 1 StR 32/13, BGHSt 58, 268 = NJW 2013, 2530.

die Spur zu kommen.[106] Den Grundgedanken dieser Judikatur kann man auf die Lokalisierung durchaus übertragen,[107] wobei in einem solchen Fall zusätzlich die Voraussetzungen des § 32 Abs. 1 S. 2 BDSG zu beachten sind. Allerdings sollten die Ortsbestimmung und erst recht das Nachverfolgen von Bewegungsabläufen nicht einfach als eine im Vergleich zu einer Videoüberwachung mildere Maßnahme eingestuft werden, weil es an einer optischen Gesamtbetrachtung des Beschäftigten fehle. Während eine Videoüberwachung nämlich regelmäßig nur aus einem bestimmten Blickwinkel einen bestimmten Ausschnitt des Arbeitnehmerverhaltens festhält, würde jedenfalls eine kontinuierliche bzw. in kurzen Abständen wiederholte Ortsbestimmung dazu, dass sich hierdurch ein Bewegungsprofil ergibt. Sofern eine heimliche Lokalisierung überhaupt erforderlich sein sollte, weil es etwa um die Frage geht, wer sich in einen an sich abgesicherten Bereich begeben hat, um dort wichtige Baupläne verbotswidrig zu kopieren, ist die Überwachungstechnik entsprechend dem Prinzip der Datensparsamkeit (§ 3a BDSG) auf das für die Überführung des Täters erforderliche Maß zu beschränken.

3.2.2 Biometrische Verfahren

Mangels spezieller Vorschriften[108] richtet sich die datenschutzrechtliche Zulässigkeit biometrischer Verfahren nach der allgemeinen Norm des § 32 Abs. 1 S. 1 BDSG. Dabei wird als legitimer Zweck für den Einsatz dieser Technik grundsätzlich nur die Authentifizierung und Autorisierung von Beschäftigten anerkannt,[109] während darüber hinausgehende Vermessungen von allen möglichen physiologischen und verhaltensbezogenen Merkmalen, sofern diese sich nicht auf die konkrete Eignung eines Arbeitnehmers für die in Aussicht genommene bzw. vertraglich geschuldete Tätigkeit beziehen, von vornherein als unzulässig anzusehen sind. Darüber hinaus müssen die Verfahren so ausgestaltet sein, dass nur diejenigen Daten erhoben und verarbeitet werden, die für den jeweiligen Zweck erforderlich sind. So dürfen betriebliche Abläufe etwa nicht so organisiert sein, dass sich Beschäftigte ohne hinreichenden Anlass immer wieder einer biometrischen Autorisierung unterziehen müssen, um ihr Bewegungs- und Arbeitsverhalten einer feinmaschigen Kontrolle zu unterwerfen. Die Überwachung der Zugangsberechtigung zu sensiblen Bereichen (Flughafen, Entwicklungslabor o.ä.) mittels biometrischer Verfahren ist dagegen deshalb als grundsätzlich zulässig anzusehen, weil andere Verfahren, wie etwa ein RFID-gestützter Dienstausweis, aufgrund des Verlust- und Diebstahlsrisikos ein geringeres Sicherheitsniveau aufweisen. Dabei sind solche Messmethoden einzusetzen, die eine vergleichsweise geringe Eingriffstiefe haben, weil sie an solche (körperlichen) Merkmale anknüpfen, die vor dem Hintergrund der allgemeinen soziokulturellen Gepflogenheiten in Deutschland im allgemeinen zwischenmenschlichen Verkehr ohnehin wahrnehmbar sind (z.B. Hand- oder Gesichtsmerkmale), während eine Messung von Körperteilen, die im

---

[106] Vgl. BAG 27.3.2003 – 2 AZR 51/02, BAGE 105, 356 = NZA 2003, 1193; BAG 21.6.2012 – 2 AZR 153/11, BAGE 142, 176 = NZA 2012, 1025; BAG 21.11.2013 – 2 AZR 797/11, BAGE 146, 303 = NZA 2014, 243 Rn. 50.

[107] Ebenso WHW/Byers, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014), B.V. Rn. 37; ferner bereits LAG Baden-Württemberg 25.10.2002 – 5 Sa 59/00, Juris (GPS-Überwachung zwecks Aufdeckung eines Spesenbetrugsversuchs).

[108] Bei biometrischen Merkmalen dürfte es sich im Allgemeinen nicht um Gesundheitsdaten im Sinne von § 3 Abs. 9 BDSG handeln.

[109] Siehe WHW/Kramer, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014), B.IV. Rn. 10.

Allgemeinen verdeckt sind, zu intensiv in die Persönlichkeitsrechte der Betroffenen eingreifen würde.

3.2.3 Überwachung des Arbeitsverhaltens

Schon mithilfe von Lokalisierungsverfahren kann das Arbeitsverhalten von Beschäftigten bis zu einem gewissen Grade kontrolliert werden. Darüber hinaus sind weitere digital basierte Überwachungsmechanismen nicht von vornherein unstatthaft, müssen sich allerdings an bestimmte Grenzen halten.

3.2.3.1 Mobile Arbeitszeit- und Projektzeiterfassung

Im Ausgangspunkt unproblematisch sind mobile Arbeitszeits- und Projektzeiterfassungssysteme, die so konzipiert sind, dass der Beschäftigte die entsprechenden Daten in mobile Endgeräte eingibt und auf der Basis dieser Daten die gesamte Arbeitszeit oder auch die auf bestimmte Projekte verwendete Arbeitszeit dokumentiert wird. Diese Form der Datenerhebung- und verarbeitung substituiert lediglich handschriftliche Aufzeichnungen, zu denen der Arbeitgeber die Arbeitnehmer schon deshalb ohne weiteres verpflichten kann, weil er als Gläubiger der Arbeitsleistung zur Feststellung berechtigt ist, ob der Beschäftigte seine Soll-Arbeitszeit erbracht hat.

Hinzu tritt die aus dem ArbZG resultierende Pflicht des Arbeitgebers, die Grenzen des Arbeitszeitrechts zu kontrollieren. Außerdem bedarf es für die Entgeltberechnung häufig der Ermittlung der konkreten Arbeitszeiten einschließlich Überstunden und Fehlzeiten. Damit ist eine entsprechende Zeiterfassung zur Durchführung des Arbeitsverhältnisses im Sinne von § 32 Abs. 1 S. 1 BDSG erforderlich. Hierbei spricht auch nichts gegen vergleichsweise detaillierte Aufstellungen, die etwa dann erforderlich sind, wenn im Außenverhältnis zu Kunden eine genaue Abrechnung der aufgewendeten Stunden erfolgt (*billable hours*). Wird die Dateneingabe durch die Beschäftigten vorgenommen, sind angesichts der geringen Eingriffstiefe auch sonst keine Bedenken ersichtlich.

3.2.3.2 Nutzeraktivitäten an stationären und mobilen Endgeräten

Deutlich problematischer ist dagegen die automatische Aufzeichnung sämtlicher Nutzeraktivitäten an stationären und mobilen Endgeräten, weil insoweit nicht nur ein Anfangszeitpunkt und ein Endzeitpunkt festgehalten werden, sondern der Beschäftigte einer kontinuierlichen Kontrolle seines Arbeitsverhaltens unterzogen werden soll. Prima facie könnte man zwar auch in diesen Gestaltungen argumentieren, dass es dem Arbeitgeber durch ein permanentes Monitoring nur darum geht, den Principal-Agent-Konflikt zu bewältigen, er den Arbeitnehmer also nur deshalb ständig überwacht, um die Erbringung der arbeitsvertraglich geschuldeten Leistung sicherzustellen, die elektronische Kontrolle mithin der Durchführung des Beschäftigungsverhältnisses dient. Dementsprechend wäre es nicht rechtswidrig, wenn der Arbeitgeber in eigener Person oder durch Vorgesetzte die Arbeitsleistung vergleichsweise engmaschig überwacht, auch wenn sich die Arbeitnehmer hierdurch bedrängt fühlen.

Aus der Zulässigkeit einer kontinuierlichen oder doch zumindest eng getakteten menschlichen Kontrolle kann man indes nicht darauf schließen, dass auch eine elektronisch unterstützte Kontrolle des Arbeitsverhaltens dem in § 32 Abs. 1 S. 1 BDSG verankerten Verhältnismäßigkeitsgrundsatz standhält. Zum einen ist der Eingriff in das

Persönlichkeitsrecht des Beschäftigten intensiver, wenn er sich bei seinem Arbeitsverhalten einer unpersönlichen digitalen Überwachungsarchitektur gegenübersieht, als wenn das Gegenüber ein lebendiger Mensch ist. Zum anderen besteht die technische Eigenheit der oben beschriebenen Aufzeichnungssysteme darin, dass jede noch so minimale wirkliche oder auch nur vermeintliche Verhaltensanomalie, die selbst einem geübten menschlichen Beobachter entgehen würde, dauerhaft fixiert wird und noch nach Jahr und Tag in den unterschiedlichsten Hinsichten ausgewertet werden kann.

Das Bewusstsein des Arbeitnehmers, dass jede einzelne Nutzeraktivität protokolliert wird und dem Arbeitgeber für eine Auswertung dauerhaft zur Verfügung steht, bewirkt Verhaltensänderungen bzw. führt mentale Zustände dabei, die der natürlichen Entfaltung der Persönlichkeit des Beschäftigten, die auch im Arbeitsverhältnis nicht zuletzt auf der Basis des grundrechtlichen Wertesystems zu gewährleisten ist, in einer erheblichen Weise zuwiderlaufen und deshalb durch das grundsätzlich schutzwürdige Interesse des Arbeitgebers an einer Überwachung des Arbeitsverhaltens nicht mehr gedeckt ist. Eine elektronische Dauerkontrolle sämtlicher Arbeitsschritte, die an stationären und mobilen Endgeräten vorgenommen werden, ist daher unverhältnismäßig.

Dies gilt erst recht für heimliche Dauerüberwachungen von Arbeitnehmern, wie sie der Hersteller des erwähnten Spionageprogramms mSpy unverhohlen anbietet. In diesen Gestaltungen hat der Beschäftigte zwar nicht das subjektive Gefühl, dass seine Nutzeraktivitäten einer kontinuierlichen Kontrolle unterzogen werden. Dennoch handelt es sich hierbei um einen besonders intensiven Eingriff in das Persönlichkeitsrecht, weil nicht anders als bei einer verdeckten Videoüberwachung natürliche Schutzmechanismen überwunden werden und zudem der Rechtsschutz verwehrt bzw. erschwert wird.[110] Zudem sieht die Bildschirmarbeitsverordnung in ihrem Anhang unter Nr. 22 ausdrücklich vor, dass ohne Wissen der Benutzer keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden darf. Schließlich kann im Einzelfall sogar ein strafbewehrtes unbefugtes Ausspähen von Daten im Sinne von § 202a StGB vorliegen, was vornehmlich davon abhängt, ob der Arbeitgeber bei seiner Kontrolle auf private Daten des Beschäftigten zugreift oder ob die Überwachung lediglich anhand geschäftlich veranlasster Daten vorgenommen wird.[111]

Vor diesem Hintergrund ist es zumindest zweifelhaft, ob man wiederum in Anlehnung an die Sichtweise des BAG zur heimlichen Videoüberwachung annehmen kann, dass eine dem Arbeitnehmer nicht bewusste Protokollierung seines Nutzerverhaltens ausnahmsweise punktuell ausgelesen werden darf, wenn dies die einzige Möglichkeit ist, jedenfalls einem strafbaren Verhalten auf die Spur zu kommen. Das ArbG Augsburg hatte zwar in einem vergleichbaren Fall die heimliche Installation und Anwendung eines Kontrollprogramms als unverhältnismäßig angesehen, gegen die verdeckte Kontrolle als solche aber keine

---

[110] Auf letzteres stellt maßgeblich ab BAG 26.8.2008 – 1 ABR 16/07, BAGE 127, 276 = NZA 2008, 1187 Rn. 21, im Anschluss an BVerfG 11.3.2008 – 1 BvR 2074/05 u.a., BVerfGE 120, 378 Rn. 79.

[111] Vgl. Lenckner/Eisele, in: Schönke/Schröder, StGB, 29. Aufl. (2014), § 202a Rn. 9. Näher dazu Eisele, Arbeitnehmerüberwachung und Compliance unter Berücksichtigung der Cybercrime-Konvention, ZIS 2012, 402-408; Weißgerber, Das Einsehen kennwortgeschützter Privatdateien des Arbeitnehmers durch den Arbeitgeber, NZA 2003, 1005-1009. Diese Frage wird in der arbeitsrechtlichen Judikatur soweit ersichtlich ausgeblendet. Für eine Unzulässigkeit der Durchsuchung privater Laufwerke auf dienstlichen Rechnern auch BVerwG 31.3.2011 – 2 A 11/08, NVwZ-RR 2011, 698.

grundsätzlichen Bedenken erhoben.[112] Sofern sich der Arbeitgeber stichprobenartige Kontrollen von privaten Aktivitäten vorbehält, tendieren die Gerichte allerdings zu der Ansicht, dass es von vornherein an einer berechtigten Vertraulichkeitserwartung des Arbeitnehmers fehlt und Nutzungsprotokolle gespeichert und (dann offenbar auch systematisch) ausgewertet werden dürfen, um missbräuchlichen Nutzungen[113] bzw. illegalen Aktivitäten[114] auf die Spur zu kommen.

Ein hiervon zu unterscheidender Fall der „Umwidmung" von Nutzeraktivitäten kommt in einer Entscheidung des LAG Köln zum Ausdruck. In dem zugrunde liegenden Sachverhalt hatte der Arbeitgeber eine Krankenhausdatenbank betrieben, in die von Arbeitnehmern Datensätze eingepflegt wurden. Hierbei wurde elektronisch festgehalten, durch welchen Arbeitnehmer in welchen Zeiträumen Dateneingaben vorgenommen wurden, um eine Qualitätskontrolle zu ermöglichen. Die betroffene Arbeitnehmerin führte ein Teil dieser Tätigkeiten an drei Wochentagen von zu Hause aus. Ihre Arbeitszeiten trug sie manuell in eine Excel Datei ein. Als die Arbeitnehmerin Freizeitausgleich zum Abbau von Überstunden beantragte, hielt ihr der Arbeitgeber Datenlisten entgegen, aus denen sich eine nicht unerhebliche Diskrepanz zwischen den manuell aufgelisteten Arbeitszeiten und den Zeitstempel der elektronischen Auswertung der Dateneingaben ergab, woraufhin die Arbeitnehmerin fristlos gekündigt wurde. Das LAG Köln hielt die Verwertung der Datenauswertung für statthaft. Zunächst habe der Arbeitgeber ein berechtigtes Interesse daran gehabt, die Datenbankeingaben überhaupt einzelnen Mitarbeiter zuzuordnen, um auf diese Weise angesichts der Wichtigkeit der eingegebenen Datensätze eine Qualitätsverbesserung herbeiführen zu können. Ohne sich explizit mit dem Aspekt der Zweckänderung zu beschäftigen, war das LAG Köln sodann der Auffassung, dass die gespeicherten Daten auch zur Arbeitszeitkontrolle verwendet werden dürfen, weil gegen die Arbeitnehmerin ein Verdacht entstanden sei und der Arbeitgeber keine andere Überprüfungsmöglichkeit zur Härtung des Verdachts gehabt habe. In den saloppen Worten des LAG Köln: „Das vorrangige Ziel des Datenschutzes ist nicht der Täterschutz".[115]

3.2.3.3 Industrie 4.0-Anwendungen

Industrie 4.0-Anwendungen zeichnen sich vorwiegend dadurch aus, dass sie auf eine Optimierung der Betriebsabläufe abzielen. Wenn und soweit personenbezogene Daten von Beschäftigten erhoben werden, besteht der Zweck also darin, die Arbeitsvorgänge möglichst effektiv zu gestalten und Interaktionen zwischen Mensch und Maschine zu verbessern. Dagegen bezweckt die Datenerhebung im Allgemeinen nicht, die Leistung oder das Verhalten von Arbeitnehmern deshalb zu kontrollieren, um daraus arbeitsrechtliche Konsequenzen zu ziehen. Diese Ausgangssituation ist bei der vorwiegend nach § 32 Abs. 1 S. 1 BDSG durchzuführenden Rechtmäßigkeitsprüfung zu berücksichtigen.

---

[112] Vgl. ArbG Augsburg 4.10.2012 – 1 BV 36/12, Juris. Andere Wertung in LAG Baden-Württemberg 25.10.2002 – 5 Sa 59/00, Juris („überschießende" GPS-Überwachung für Verwertbarkeit irrelevant).

[113] LAG Baden-Württemberg 14.1.2016 – 5 Sa 657/15, BB 2016, 891 (Browserverlauf); gleichsinnig EGMR 12.1.2016 – 61496/08, DuD 2016, 395 – Bärbulescu/Romania.

[114] LAG Hamm 10.7.2012 – 14 Sa 1711/10, ZD 2013, 135 (Chat-Protokoll).

[115] LAG Köln 29.9.2014 – 2 Sa 181/14, NZA-RR 2015, 128.

Zunächst sind technische Innovationen mit dem Ziel, die betrieblichen Abläufe zu effektivieren, grundsätzlich statthaft, auch wenn hierbei personenbezogene Beschäftigtendaten erhoben und verarbeitet werden. Der Umgang mit solchen Daten ist für die Durchführung des Beschäftigungsverhältnisses schon dann erforderlich, wenn nicht unerhebliche Effizienzgewinne erzielt werden. Würde man eine Erhebung und Verarbeitung personenbezogener Daten nur unter der Voraussetzung als „erforderlich" ansehen, dass andernfalls die Funktionsfähigkeit des Unternehmens beeinträchtigt wird,[116] würden technischen Innovationen zu enge Fesseln angelegt. Diese Zweck-Mittel-Relation darf indes weiterer Konkretisierung. So gilt im Rahmen der Angemessenheitsprüfung als äußerste Grenze in jedem Fall wieder das Verbot der Totalkontrolle.[117] Im Übrigen hängt die Beurteilung sehr stark von den konkreten Anwendungen ab. Geht es lediglich darum, dass Industrieroboter gefahrlos agieren und die in Ihrer Nähe arbeitenden oder mit ihnen sogar unmittelbar kollaborierenden Menschen nicht verletzt werden, wird es im Allgemeinen genügen, wenn die Sensoren des Roboters überhaupt wahrnehmen, dass sich Menschen seiner Umgebung befinden, und diese Daten sodann in Echtzeit in Steuerungsimpulse umgesetzt werden.

Demgegenüber ist eine biometrische Identifikation der einzelnen Beschäftigten und erst recht eine Speicherung solcher Daten für diesen Zweck nicht erforderlich. Geht es um die möglichst zeit- und ressourcensparende Koordinierung des Einsatzes etwa von Störungsmechanikern auf einem weiträumigen Betriebsgelände, wird es grundsätzlich ausreichen, wenn die Arbeitsaufträge so vergeben werden, dass dem nach den einschlägigen Parametern jeweils am besten geeigneten Mitarbeiter der Auftrag zugewiesen wird. Demgegenüber ist es für diesen Zweck unnötig, die hierbei erhobenen personenbezogenen Daten dauerhaft zu speichern. Zudem wird es vielfach genügen, einen Beschäftigten erst in dem Augenblick zu lokalisieren und ihm anschließend einen Auftrag zu erteilen, wenn ein Störungsfall eingetreten ist. Auch sind Anwendungen vorzugswürdig, in denen Spezialwerkzeuge dem Arbeitnehmer anzeigen, wo sie im Einzelnen zu finden sind, während die Information, welcher andere Mitarbeiter zuvor mit dem Werkzeug gearbeitet hat und es deshalb wahrscheinlich noch in seinem „Besitz" hat, entbehrlich ist.

Darüber hinaus kann aus verschiedenen Gründen eine Verknüpfung der Erledigung konkreter Arbeitsaufgaben mit einem Nutzerkonto erforderlich sein. So kann es darum gehen, dass ein Beschäftigter im Laufe der Zeit ein bestimmtes Fähigkeitsprofil herausbildet und hierdurch die Einsatzplanung verbessert werden kann. Denkbar ist auch, dass andere Arbeitnehmer hierdurch in die Lage versetzt werden, etwa zur Erfüllung von Anschlussaufgaben Rücksprache halten zu können. Ferner kommt in Betracht, die Bewältigung der verschiedenen Aufgaben zu analysieren, um daraus auf einen individuellen Qualifizierungsbedarf zu schließen. Auch insoweit gilt aber wiederum das persönlichkeitsrechtliche Verbot der Totalüberwachung. Letztlich darf das Arbeitsverhalten somit nur punktuell zum Gegenstand von Datenerhebungen gemacht werden.

Schließlich ist angesichts der höchst unterschiedlichen Zwecke, die mit der Erhebung von Beschäftigtendaten verfolgt werden können, nochmals der Grundsatz der Zweckbindung hervorzuheben, der gegebenenfalls durch eine Trennung von Datenbeständen befördert

---

[116] So Däubler, Gläserne Belegschaften, 6. Aufl. (2015), Rn. 117.

[117] Hofmann, Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0, ZD 2016, 12-17 (15).

werden kann. Zudem kann es für die Zweckerreichung zuweilen genügen, wenn die personenbezogenen Daten der Arbeitnehmer pseudonymisiert werden.[118] Gleichwohl ist eine Zweckänderung nicht per se ausgeschlossen. Insoweit können im Einzelfall personenbezogene Daten, die zur besseren Steuerung betrieblicher Abläufe generiert wurden, durchaus für einen vorübergehenden Zeitraum zur punktuellen Leistungs- und Verhaltenskontrolle herangezogen werden, während eine Nutzung von Daten aus länger zurückliegenden Zeiträumen unverhältnismäßig wäre.[119] Außerdem gilt für mobile Assistenzsysteme gemäß § 6b Abs. 3 BDSG wiederum das Gebot der Erkennbarkeit von Kommunikationsvorgängen.

3.2.3.4 Sonstige inner- und außerbetriebliche Assistenzsysteme

Soweit Assistenzsysteme wie etwa die bei *Amazon* eingesetzten Handscanner lediglich der besseren Koordinierung innerbetrieblicher Abläufe dienen und etwa die Wege, die von den Mitarbeitern beim Einsammeln von Waren in weitläufigen Lagerhallen zurückzulegen sind, optimiert werden, ist hiergegen grundsätzlich nichts einzuwenden. Die hierbei erhobenen und verarbeiteten personenbezogenen Daten dienen der Durchführung des Beschäftigungsverhältnisses gemäß § 32 Abs. 1 S. 1 BDSG.

Allerdings ist schon fraglich, ob es für die Ermittlung der bestmöglichen Wege für den jeweiligen Arbeitnehmer erforderlich ist, dass der Handscanner mit einem personifizierten Nutzerkonto verbunden ist. Geht es nur darum, das Wareneinsammeln als solches so effizient wie möglich zu gestalten, würde es genügen, wenn unter Zuhilfenahme eines entsprechenden Algorithmus auf dem jeweiligen Handscanner angezeigt wird, welcher Weg als nächstes einzuschlagen ist, ohne dass der hierdurch angeleitete Mitarbeiter konkret identifiziert werden müsste. Auch wenn man sich über diesen Aspekt noch hinwegsetzt, dessen Berechtigung letztlich davon abhängig ist, ob bereits eine ausschließlich zwischen beweglichen und stationären Betriebsmitteln eingerichtete drahtlose Kommunikation einen reibungslosen Betriebsablauf hinreichend gewährleistet, bedarf es für diesen Zweck jedenfalls keiner minutiösen Erhebung der Performanz eines jeden einzelnen Beschäftigten. Selbst wenn einzelne Arbeitsprozesse, wie etwa der Umgang mit hochsensiblen Substanzen, nur dann optimal gelingen, wenn bestimmte Parameter des Arbeitnehmerverhaltens kontinuierlich erhoben, in Echtzeit verarbeitet und in Anweisungen an Maschinen oder an den Mitarbeiter selbst rückgekoppelt werden, ist eine dauerhafte Speicherung dieser Daten regelmäßig entbehrlich.

Erst recht entspricht es nicht der Zwecksetzung der erhobenen Daten, wenn diese für eine engmaschige Kontrolle des Arbeitsverhaltens eingesetzt werden und die Arbeitnehmer unter Heranziehung dieser Daten damit konfrontiert werden, dass sie etwa bestimmte Wege „zu langsam“ zurückgelegt, „unnötige“ Verschnaufpausen oder sich „zu lange“ in den sanitären Räumlichkeiten aufgehalten haben. Einer solchen umfassenden Nutzung der gewonnenen Daten stünde das grundsätzliche Verbot der Zweckänderung entgegen. Als verhältnismäßig sind Überwachungen des reinen Arbeitsverhaltens mit einer großen Eingriffstiefe nur dann anzusehen, wenn sie lediglich punktuell und jeweils nur über kurze Zeiträume stattfinden sowie volle Transparenz für die Beschäftigten gewährleistet ist, um etwa einen auf den konkreten Beschäftigten zugeschnittenen Qualifizierungsbedarf zu

---

[118] Hofmann, Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0, ZD 2016, 12-17 (16).

[119] Hofmann, Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0, ZD 2016, 12-17 (15).

ermitteln oder um Anhaltspunkte für eine Prozessoptimierung zu gewinnen, die ansonsten nicht festgestellt werden könnten.

3.2.3.5 Sprachgebrauchs- und Stimmungsanalyseverfahren

Ob die geschilderten Verfahren überhaupt legitimiert werden können, ist bislang nur vereinzelt untersucht worden. Ein Teil des Schrifttums hält Anwendungen wie „Keyword Spotting" und Stimmungsanalyse offenbar per se für unzulässig, weil es sich um einen gravierenden Eingriff in das Persönlichkeitsrecht des Beschäftigten handele, er in eine Objektstellung versetzt werde und letztlich die Menschenwürde verletzt sei.[120] Andere Autoren äußern bei der Schilderung derartiger Verfahren ersichtlich keine Bedenken.[121] Tatsächlich kann man sich nicht einfach mit einem Verweis auf eine Entscheidung des BAG von 1995 begnügen. Darin wurde das Mithören des Arbeitgebers von Telefonaten von Mitarbeitern der Reservierungszentrale eines Luftfahrtunternehmens für zulässig erklärt, wobei das BAG wesentlich darauf abstellte, dass sich die Eingriffe auf die Probezeit beschränkten und zudem in Gegenwart des Arbeitnehmers, also mit seiner vollen Kenntnis erfolgten.[122] Die Besonderheit der hier in Rede stehenden Techniken besteht nämlich in einer digital unterstützten Analyse von Sprache und Stimme, die durch das noch so aufmerksame bloße Zuhören eines anderen Menschen niemals geleistet werden könnte.

Gleichwohl spricht mehr für eine mittlere Lösung.[123] Danach ist darauf abzustellen, ob mithilfe der verwendeten Techniken umfassend auf die Persönlichkeit eingewirkt werden soll, um den Arbeitnehmer in eine bestimmte Richtung zu formen. In diesen Gestaltungen ist tatsächlich eine absolute Grenze erreicht, die einer Relativierung durch betriebsorganisatorische und ökonomische Zielsetzungen entgegensteht. Handelt es sich dagegen nur um punktuelle Eingriffe, werden die Techniken also nur sporadisch und nicht dauerhaft eingesetzt, um die Kundenbetreuung zu optimieren, greift es zu weit, pauschal von einem Verstoß gegen die Menschenwürde zu sprechen. Wenn es beispielsweise um die Kommunikation mit Kunden auf Englisch oder Französisch geht, leuchtet es nicht ein, wenn man annehmen würde, dass ein Beschäftigter durch ein digital unterstütztes Verfahren zur Verbesserung der Aussprache zu einem „Objekt" herabgewürdigt wird. An diesem Beispiel zeigt sich, dass nicht allein auf die Technik als solche abgestellt werden kann, die in bestimmten Fällen durchaus dazu beitragen kann, unbestreitbaren Defiziten bei der Aufgabenerfüllung entgegenzuwirken. Vielmehr führt jenseits eindeutiger Fälle an einer Anwendung des Verhältnismäßigkeitsgrundsatzes kein Weg vorbei. Sofern man es daher prinzipiell akzeptiert, dass sich die Mitarbeiter von Call-Centern bis zu einem gewissen Grade an den Kundenerwartungen und damit an Dritten auszurichten haben und hierfür auch entsprechend geschult werden können, sind auch neuartige Verfahren zur Analyse von Sprache und Stimme nicht per se unzulässig, sofern sie lediglich ausnahmsweise zur Anwendung kommen. Intensivere Formen der Kontrolle sind dagegen mit dem Verhältnismäßigkeitsgrundsatz abzuwehren.

---

120 Däubler, Gläserne Belegschaften?, 6. Aufl. (2015), Rn. 378j; Kiesche/Wilke, Neue Überwachungsformen in Call-Centern, CuA 2012, 5-12 (11).

121 Zoebisch, Stimmungsanalyse durch Call-Center, DuD 2011, 394-397 (397).

122 BAG 30.8.1995 – 1 ABR 4/95, BAGE 80, 366 = NZA 1996, 218 (unter II 2 b).

123 In diese Richtung auch Hrach/Nöbel/Richthof/Alt, Datenschutz im Call Center: Aufzeichnung und Verwendung personenbezogener Daten, RDV 2012, 280-285 (282-285), allerdings ohne ausdrückliche Bezugnahme auf „Keyword Spotting" und Stimmungsanalyse.

So sind Daueraufzeichnungen schon deshalb unverhältnismäßig, weil für die Überprüfung eines „Lernfortschritts“ beim Sprachgebrauch genügt, wenn in gewissen Abständen kontrolliert wird, welche Worte die Beschäftigten in ihrer Kommunikation mit Kunden verwenden. Auch können ständig wechselnde Kundenerwartungen keine kontinuierlichen Einflussnahmen mit den beschriebenen Techniken legitimieren.

3.2.4 Auswertung innerbetrieblicher sozialer Netzwerke

In datenschutzrechtlicher Hinsicht empfiehlt es sich, zwischen der Abbildung der innerbetrieblichen Kommunikationsstruktur als solcher (*Enterprise Social Graph*) und ihrer analytischen Auswertung in bestimmten Beziehungen qua Data Mining zu unterscheiden. Schon bei der Herstellung des Graphen werden gewaltige Mengen personenbezogener Beschäftigtendaten verarbeitet. Insoweit kann man schon bezweifeln, ob tatsächlich jeder innerbetriebliche Kommunikationsvorgang als Datum für eine kontinuierliche Weiterentwicklung des Graphen mit dem Ziel verwendet werden muss, um alle künftigen unternehmensinternen Interaktionen permanent zu effektivieren. So ist eine reine Vorratsdatenspeicherung nach allgemeiner Ansicht unzulässig. Vielmehr bedarf es stets eines hinreichend bestimmten Zwecks, um personenbezogene Beschäftigtendaten zu erheben und zu speichern, wobei nicht bzw. nicht mehr benötigte Daten zu löschen sind (§ 35 Abs. 2 S. 2 Nr. 1 BDSG). Immerhin lässt sich begründen, dass es im Ausgangspunkt „nur“ um eine Optimierung der innerbetrieblichen Kommunikation geht und zahlreiche Kooperationen von Beschäftigten gerade bei räumlich nicht verbundenen möglichst Arbeitszusammenhängen nur dann funktionieren, wenn die Arbeitnehmer ohne Zeitverlust an diejenigen Informationen herankommen, die sie für die Bewältigung ihrer Arbeitsaufgaben benötigen, auch wenn es sich hierbei vielfach um personenbezogene Daten handelt.

Problematisch ist aber die Auswertung aller dieser Daten zu den unterschiedlichsten Zwecken. Insoweit bedarf es für jedes Data Mining, durch das aus dem Datenpool bislang unbekannte Zusammenhänge und Muster zutage gefördert werden sollen, einer klaren Bestimmung des damit im Einzelfall verfolgten Zwecks. Pauschale Zielsetzungen, nach denen die Analyse von personenbezogenen Beschäftigtendaten gleichsam einen Selbstzweck bilden, sind nach geltendem Recht nicht zulässig.[124] Darüber hinaus muss der Einsatz des konkreten Tools für die Durchführung des Arbeitsverhältnisses erforderlich sein, wobei es an dieser Voraussetzung bei einer Analyse des Datenbestandes anhand der unterschiedlichsten Kriterien häufig fehlen wird. Zulässig wäre es dagegen beispielsweise, für ein herausforderndes Entwicklungsprojekt ein Team von hierfür besonders geeigneten Mitarbeitern aus unterschiedlichen Standorten zusammenzustellen und sich dabei auf eine Auswertung des Graphen zu stützen, die zutage fördert, welche Beschäftigten sich in den letzten Monaten intensiv mit bestimmten technischen Neuerungen auseinandergesetzt haben und deshalb am ehesten in der Lage sind, die Arbeitsaufgabe sachgerecht zu erledigen. Aus der Perspektive des Beschäftigtendatenschutzes geht es also keineswegs darum, Effizienzgewinne durch ein Data Mining in personenbezogenen Mitarbeiterdaten generell zu verhindern. Wohl aber fordert das Datenschutzrecht, dass sich der Arbeitgeber

---

[124] Wedde, Der analysierte Arbeitnehmer, CuA 2016, 14-16. Zum Verstoß von pauschalen Big Data-Analysen gegen den Grundsatz der Zweckbindung generell Weichert, Big Data und Datenschutz, ZD 2013, 251-259 (256).

zum einen vor dem Umgang mit diesen Daten klare Rechenschaft darüber ablegt, welches konkrete Ziel damit verfolgt werden soll, und dass zum anderen dieses Ziel so datensparsam (§ 3a BDSG) wie möglich erreicht wird.

3.2.5 Auswertung von Fitnessdaten

Allgemeine Fitnessdaten, wie sie von Fitness-Trackern permanent gemessen werden, stehen regelmäßig in keinem konkreten Zusammenhang zur Aufgabenerfüllung und damit zur Durchführung des Beschäftigungsverhältnisses gemäß § 32 Abs. 1 S. 1 BDSG. Deshalb können sie von Arbeitgebern nicht kraft gesetzlicher Erlaubnis erhoben und/oder verarbeitet werden. Denkbar sind lediglich Freiwilligenprogramme im Rahmen des betrieblichen Gesundheitsmanagements, die vom Arbeitgeber aufgelegt und mithilfe digitaler Technologien durchgeführt werden.[125]

Grundlage des Umgangs mit den personenbezogenen Fitnessdaten ist in diesen Gestaltungen die Einwilligung des betroffenen Mitarbeiters, die den Anforderungen von § 4a BDSG genügen muss, was nur dann der Fall ist, wenn der der Arbeitnehmer ohne jeden Druck seitens des Arbeitgebers oder auch Kollegen darüber entscheiden kann, ob er an einem solchen Programm teilnimmt oder nicht. Außerdem ist in Rechnung zu stellen, dass es sich häufig um Gesundheitsdaten und damit um besonders sensible Daten handelt (§ 3 Abs. 9 BDSG).[126] Für diese Art von Daten gelten erhöhte Anforderungen an die Wirksamkeit der Einwilligung (§ 4a Abs. 3 BDSG) sowie gegebenenfalls besondere Voraussetzungen für deren Erhebung oder Verwendung (§ 28 Abs. 6 bis 8 BDSG).

Eine Zusatzfrage besteht darin, Gesundheitsdaten von Beschäftigten dann unter erleichterten Voraussetzungen erhoben bzw. verwendet werden dürfen, wenn eine Anonymisierung im Sinne von § 3 Abs. 6 BDSG erfolgt. Hierdurch wäre es unter Umständen möglich, besonders gesundheitsbelastende betriebliche Arbeitsbedingungen zu identifizieren, um entsprechende Abhilfemaßnahmen (technische Veränderungen der Arbeitsplätze, Fortbildungen) zu organisieren. Rechtlicher Ausgangspunkt ist insoweit, dass anonymisierte Daten keine personenbezogenen Daten (mehr) sind und damit auch nicht (mehr) dem Datenschutzrecht unterfallen.[127] Dies gilt freilich nur für solche Gestaltungen, bei denen die fraglichen Gesundheitsdaten einer bestimmten oder bestimmbaren natürlichen Person tatsächlich nicht oder nur mit einem unverhältnismäßig großen Aufwand zugeordnet werden können.[128]

---

[125] Kopp/Sokoll, Wearables am Arbeitsplatz – Einfallstor für Alltagsüberwachung ?, NZA 2015, 1352-1359.

[126] Dazu im Zusammenhang mit Wearables näher Wilmer, Wearables und Datenschutz – Gesetze von gestern für die Technik von morgen?, K&R 2016, 382-389 (388).

[127] Taeger/Gabel/Buchner, BDSG, 2. Aufl. (2013), § 3 Rn. 44; DKWW/Weichert, BDSG, 5. Aufl. (2016), § 3 Rn. 49. Siehe auch Erwägungsgrund 26 a.E. DS-GVO.

[128] Zur Unklarheit der gesetzlichen Definition Kühling/Klar, Unsicherheitsfaktor Datenschutzrecht – das Beispiel des Personenbezugs und der Anonymität, NJW 2013, 3611-3617.
Taeger/Gabel/Buchner, BDSG, 2. Aufl. (2013), § 3 Rn. 44; DKWW/Weichert, BDSG, 5. Aufl. (2016), § 3 Rn. 49. Siehe auch Erwägungsgrund 26 a.E. DS-GVO.

Das schlichte Weglassen von Identifizierungsdaten stellt dagegen noch keine Anonymisierung im strengen Sinne des § 3 Abs. 6 BDSG dar.[129] Darüber hinaus kommt es darauf an, in welchem Stadium die Anonymisierung der Gesundheitsdaten vorgenommen wird. Sofern der Umgang mit den Gesundheitsdaten der Beschäftigten so ausgestaltet ist, dass die Anonymisierung erst im Anschluss an die Erhebung erfolgen soll, bleibt es im Hinblick auf die Phase der Erhebung bei der Anwendbarkeit des Datenschutzrechts einschließlich der besonderen Vorschriften des § 28 Abs. 6 bis 8 BDSG. Schließlich lassen Big Data sowie der damit verbundene technische Fortschritt die Grenzen zwischen Anonymität und Personenbezug zunehmend verschwimmen,[130] sodass mittlerweile mit einigem Recht die Forderung erhoben wird, die Anonymität von Daten nicht als gesicherten Zustand anzusehen, sondern ihren Fortbestand einer regelmäßigen Kontrolle zu unterziehen.[131] Sofern neuere Techniken eine Re-Identifizierung von ursprünglich anonymen Beschäftigtengesundheitsdaten ermöglichen sollten, würde das Datenschutzregime somit wieder zum Tragen kommen.

3.2.6 Durchleuchtung der Persönlichkeit qua Sprachanalyseverfahren

Einen in datenschutzrechtlicher Hinsicht besonders heiklen Fall stellen Sprachanalyseverfahren dar, mit denen nicht das Arbeitsverhalten von Beschäftigten insbesondere Call-Centern punktuell beeinflusst werden soll, sondern die in Bewerbungssituationen oder bei Entscheidungen über einen innerbetrieblichen Aufstieg auf eine Durchleuchtung der Persönlichkeit hinauslaufen. Bei diesen Verfahren ist sehr schnell der Punkt erreicht, an dem es um eine „Registrierung“ und „Katalogisierung“ der individuellen Persönlichkeit des Betroffenen geht, die jedenfalls gegen seinen Willen nicht durchgeführt werden darf, weil hierdurch das Persönlichkeitsrecht definitiv verletzt würde. Insoweit bildet der Menschenwürdegehalt des Persönlichkeitsrechts von vornherein einen nicht relativierbaren Schutz vor Zugriffen von außen.

Fraglich kann allenfalls sein, ob sich Bewerber oder Arbeitnehmer einem solchen Analyseverfahren „freiwillig“ aussetzen dürfen, wenn sie sich hiervon unter Umständen Vorteile versprechen. Würde es an jeglicher Abhängigkeitssituation fehlen, wäre letztlich nichts dagegen einzuwenden, wenn eine Person in ein derartiges Sprachanalyseverfahren einwilligt. Hiervon kann in der Bewerbungssituation, aber regelmäßig auch innerhalb des Arbeitsverhältnisses indes keine Rede sein, zumal es um eine Maßnahme mit hoher Eingriffstiefe geht, bei der die individuelle Entscheidung des Arbeitgebers über eine den Werdegang des Bewerbers bzw. Arbeitnehmers erheblich berührende Angelegenheit durch eine auf Algorithmen beruhende Ähnlichkeitsbetrachtung zumindest präjudiziert wird.

Dass bestimmte Erkenntnismethoden auch im Falle unbestreitbarer Wissenschaftlichkeit im Beschäftigungskontext aus Gründen des Persönlichkeitsschutzes nicht genutzt werden dürfen, macht § 19 GenDG deutlich. Insoweit hat der Gesetzgeber zur Begründung des an den Arbeitgeber adressierten generellen Verbots, die Vornahme genetischer Untersuchungen oder Analysen zu verlangen oder deren Ergebnisse entgegenzunehmen,

---

[129] Vgl. DKWW/Weichert, BDSG, 5. Aufl. (2016), § 3 Rn. 49.

[130] Vgl. Dammann, Erfolge und Defizite der EU-Datenschutzgrundverordnung, ZD 2016, 307-314 (313).

[131] Siehe Marnau, Anonymisierung, Pseudonymisierung und Transparenz für Big Data, DuD 2016, 428-433 429), in diesem Sinne auch Roßnagel, Big Data – Small Privacy?, ZD 2013, 562-567 (563).

damit begründet, dass der Schutz der Persönlichkeitsrechte der Beschäftigten die Erhebung eines umfassenden Persönlichkeits- oder Gesundheitsprofils verbiete. Damit solle zugleich verhindert werden, dass sich die Arbeitsmarktchancen der Betroffenen aufgrund bestimmter genetischer Eigenschaften verringerten.[132] Die Analyse des über Jahrzehnte durch Sozialisation und Bildung entwickelten individuellen Sprachgebrauchs als ein nicht nur äußeres Attribut, sondern als ein Kernelement der menschlichen Persönlichkeit geht in eine vergleichbare Richtung und sieht sich daher denselben Bedenken ausgesetzt.

3.3 Individualrechtliche Konsequenzen und präventiver kollektivrechtlicher Schutz

3.3.1 Individualrechtliche Reaktionsmöglichkeiten und sonstige Folgen

Das BDSG sieht verschiedene Rechtsbehelfe des einzelnen Beschäftigten vor, der in seinem Recht auf informationelle Selbstbestimmung durch einen unzulässigen Umgang mit seinen personenbezogenen Daten verletzt wird.

Sofern personenbezogene Daten unrichtig sind, muss die verantwortliche Stelle diese Daten gemäß § 35 Abs. 1 S. 1 BDSG grundsätzlich von sich berichtigen. Darüber hinaus hat der betroffene Arbeitnehmer gemäß § 35 Abs. 1 S. 1 BDSG einen Anspruch auf Berichtigung, der je nach dem konkreten Fall auf Korrektur, Vervollständigung oder Löschung hinauslaufen kann.[133] Lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten mit der Folge zu sperren (§ 35 Abs. 4 BDSG), dass sie grundsätzlich nicht mehr übermittelt oder genutzt werden dürfen (§ 35 Abs. 8 BDSG).

Praktisch wichtiger ist die Löschungspflicht bzw. der Löschungsanspruch aus § 35 Abs. 2 S. 2 BDSG. Dabei stehen im vorliegenden Zusammenhang zwei Fallgruppen im Vordergrund, zum einen die unzulässige Speicherung und zum anderen der Wegfall des Speicherungszwecks. Eine unzulässige Speicherung personenbezogener Daten (§ 35 Abs. 2 S. 2 Nr. 1 BDSG) liegt im Anschluss an § 4 Abs. 1 BDSG grundsätzlich immer dann vor, wenn diese weder durch eine Rechtsvorschrift noch durch eine wirksame Einwilligung des Betroffenen gedeckt ist. Dies betrifft in erster Linie die Situationen, in denen bereits die Datenerhebung unzulässig war. Dasselbe gilt aber auch für die Konstellation, dass lediglich die Auswertung und damit die Nutzung eines vorhandenen Datenbestandes gegen Datenschutzrecht verstößt. Damit ist die Speicherung von personenbezogenen Beschäftigtendaten, die durch ein unzulässiges Data Mining generiert worden sind, für sich genommen unzulässig, sodass diese Daten zu löschen sind, auch wenn der ursprüngliche Datenbestand in rechtmäßiger Art und Weise erhoben worden ist und gegebenenfalls auch weiter gespeichert werden kann. Anders gesagt führen Verstöße gegen das Verbot der Zweckentfremdung von Daten dazu, dass die hierdurch gewonnenen Daten nicht gespeichert werden dürfen bzw. gelöscht werden müssen.

Als eine Form der unzulässigen Speicherung von personenbezogenen Daten wird es gemeinhin auch angesehen, wenn eine Datenerhebung unter Verstoß gegen

---

[132] BT-Drucks. 16/10532, S. 37.

[133] Däubler, Gläserne Belegschaften?, 6. Aufl. (2015), Rn. 552.

betriebsverfassungsrechtliche Vorschriften vorgenommen wurde.[134] In diesem Fall besteht daher ebenfalls eine Löschungspflicht bzw. ein Löschungsanspruch, selbst wenn die Datenerhebung im Übrigen datenschutzrechtlich zulässig gewesen ist.[135] Infolge der Gesetzesfassung („ist") kommt es freilich in allen Gestaltungen auf die gegenwärtige Sach- und Rechtslage an.[136]

Von einem Wegfall des Speicherungszwecks (§ 35 Abs. 2 S. 2 Nr. 3 BDSG) ist dann zu sprechen, wenn die Datenverarbeitung für eigene Zwecke vorgenommen wurde und die weitere Kenntnis der personenbezogenen Daten zur Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Mit dieser Vorschrift wird das vom EuGH aus dem Grundrecht auf Datenschutz aus Art. 8 GRC entwickelte[137] und nunmehr auch in Art. 17 DS-GVO ausdrücklich geregelte „Recht auf Vergessenwerden" vorweggenommen bzw. umgesetzt. Diese Fallgruppe betrifft im Bereich des Arbeitsrechts in erster Linie abgelehnte Bewerber und ehemalige Beschäftigte, dürfte angesichts der zunehmenden Sammlung von Arbeitnehmerdaten aber auch im laufenden Arbeitsverhältnis an Bedeutung gewinnen. Wenn beispielsweise personenbezogene Mitarbeiterdaten nur deshalb erhoben und gespeichert werden, um eine reibungslose Kooperation in einem virtuellen Team zu ermöglichen, bedarf es nach dem erfolgreichen Abschluss des Projekts grundsätzlich keiner dauerhaften Speicherung dieser Daten, sodass sie zu löschen sind. Dass eine rechtlich gebotene Löschung personenbezogener Daten effektiv vollzogen werden muss und nicht durch Anfertigung von Sicherungskopien und Schattendateien hintertrieben werden darf, versteht sich von selbst.[138] Für Gesundheitsdaten schließlich gelten von vornherein noch strengere Regeln (§ 35 Abs. 2 S. 2 Nr. 2 BDSG).

Daneben kennt das BDSG das Widerspruchsrecht, das selbst bei einer rechtmäßigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten greift, sofern der Betroffene wegen seiner besonderen persönlichen Situation in einem erhöhten Maße schutzwürdig ist (§ 35 Abs. 5 BDSG).

Soweit es um Schadensersatz geht, enthält das Datenschutzrecht mit § 7 BDSG eine spezielle Anspruchsgrundlage für jede unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung personenbezogener Daten. Hierbei handelt es sich ausweislich § 7 S. 2 BDSG um eine Haftung aus vermuteten Verschulden. Die große Schwachstelle dieser Regelung besteht allerdings darin, dass auf ihrer Basis nach herrschender Ansicht lediglich der materielle Schaden ersetzt werden kann, den der Betroffene durch einen rechtswidrigen Umgang mit seinen Daten erleidet. Dies ergibt sich nicht zuletzt durch einen Umkehrschluss aus § 8 Abs. 2 BDSG, der einen Anspruch auf Ersatz des immateriellen Schadens nur bei einer automatisierten Datenverarbeitung durch öffentliche Stellen vorsieht.[139] Allerdings sind materielle Schäden von Arbeitnehmern nicht leicht vorstellbar.

---

[134] Däubler, Gläserne Belegschaften?, 6. Aufl. (2015), Rn. 556; Taeger/Gabel/Meents/Hinzpeter, BDSG, 2. Aufl. (2013), § 35 Rn. 19.

[135] Vgl. BAG 22.10.1986 – 5 AZR 660/85, BAGE 53, 226 = NZA 1987, 415 (unter B I 1 a), zu Personalfragebogen im Sinne von § 94 BetrVG.

[136] Simitis/Dix, BDSG, 8. Aufl. (2014), § 35 Rn. 26.

[137] EuGH 13.5.2014 – C-131/12, NJW 2014, 2257 – Google Spain.

[138] Dazu Däubler, Gläserne Belegschaften?, 6. Aufl. (2015), Rn. 561.

[139] Gola/Schomerus, BDSG, 11. Aufl. (2012), § 7 Rn. 12 f.; Taeger/Gabel/Gabel, BDSG, 2. Aufl. (2013), § 7 Rn. 10.

Theoretisch denkbar ist etwa die Konstellation, dass der Arbeitgeber in rechtswidriger Weise das Arbeitsverhalten des Arbeitnehmers überwacht, die hierdurch gewonnenen Daten als Grundlage für eine Versetzung auf eine niedriger dotierte Stelle verwendet und der Arbeitnehmer hierdurch eine Entgelteinbuße erfährt. Tatsächlich enthält die Datenbank „Juris“ aber keinen einzigen Rechtsprechungsnachweis zur Zuerkennung eines auf § 7 BDSG gestützten Schadensersatzanspruchs eines Beschäftigten.

Wichtiger ist stattdessen der Ersatz immaterieller Schäden, der nach allgemeinen bürgerlichrechtlichen Grundsätzen bei einem schwerwiegenden Eingriff in das Allgemeine Persönlichkeitsrecht auf der Grundlage von § 823 Abs. 1 BGB in Verbindung mit Art. 1 Abs. 1 und Art. 2 Abs. 1 GG verlangt werden kann. Dieser Anspruch wird durch § 7 BDSG nach allgemeiner Ansicht nicht ausgeschlossen.[140] Vielmehr wird der durch Art. 23 DSRL geforderte umfassende Schutz im deutschen Recht gerade dadurch gewährleistet, dass die Lücke im BDSG im Hinblick auf die Ersatzfähigkeit immaterieller Schäden und damit im Hinblick auf einen wichtigen Baustein für die effektive Durchsetzung des Datenschutzrechts durch einen Rückgriff auf allgemeine zivilrechtliche Grundsätze geschlossen werden kann.[141] Dass diese Grundsätze in der arbeitsrechtlichen Praxis auch vereinzelt genutzt werden, belegen verschiedene Urteile, die sich überwiegend auf unzulässige Videoaufnahmen beziehen.[142] Entscheidungen über die Zuerkennung von Schmerzensgeld an Beschäftigte bei sonstigen Formen des unzulässigen Umgangs mit personenbezogenen Daten, etwa bei einem Verstoß gegen das Verbot der Zweckentfremdung, sind dagegen nicht bekannt geworden.

Schließlich kommt bei einem Datenschutzrechtsverstoß auch die Ausübung eines auf § 273 BGB gestützten Zurückbehaltungsrechts an der Arbeitsleistung bei gleichzeitiger Aufrechterhaltung des Entgeltanspruchs gemäß § 615 S. 1 BGB in Betracht.[143]

Trotz einer insgesamt durchaus respektablen Anzahl von unterschiedlichen Rechtsbehelfen, die dem einzelnen Arbeitnehmer bei Verletzungen seines Rechts auf informationelle Selbstbestimmung zustehen, weist der Schutz durch individuelle Rechte faktisch doch gewisse Schwächen auf, was auf verschiedenen Gründen beruhen dürfte: Zum einen auf einem Informationsdefizit der Betroffenen, sei es über den Datenschutzverstoß, sei es über die zur Verfügung stehenden Rechtsbehelfe; zum zweiten aus der Scheu, das eigene Arbeitsverhältnis durch einen Rechtsstreit zu belasten; zum dritten ein rationales Desinteresse, kleinere Rechtsverletzungen nicht zum Anlass für eine aufwändige Rechtsverfolgung zu nehmen, zumal ein Obsiegen häufig unsicher ist und je nach Fallgestaltung nicht nur dem Kläger selbst, sondern auch anderen betroffenen Arbeitnehmern zugutekommt, ohne dass diese die Mühen einer rechtlichen Auseinandersetzung auf sich genommen haben (Free-Rider-Problem).

---

[140] Siehe nur BAG 19.2.2015 – 8 AZR 1007/13, NZA 2015, 994.

[141] DKWW/Däubler, BDSG, 5. Aufl. (2016), § 7 Rn. 5, 20; Taeger/Gabel/Gabel, BDSG, 2. Aufl. (2013), § 7 Rn. 10.

[142] LAG Hamm 30.10.2012 – 9 Sa 158/12, ZD 2013, 355; LAG Rheinland-Pfalz 23.5.2013 – 2 Sa 540/12, ZD 2014, 41. Zur unerlaubten Observation durch einen Privatdetektiv jüngst BAG 19.2.2015 – 8 AZR 1007/13, NZA 2015, 994.

[143] Forst, Die Rechte des Arbeitnehmers infolge einer rechtswidrigen Datenverarbeitung durch den Arbeitgeber, AuR 2010, 106-112 (107).

Die praktisch größte Bedeutung kommt dem Datenschutz in individualrechtlichen Streitigkeiten offenbar in Kündigungsschutzverfahren zu, wenn sich die Frage stellt, ob Umstände, auf die der Arbeitgeber eine Kündigung stützt, verwertet bzw. als Beweismittel verwendet werden dürfen, obwohl sie unter Verstoß gegen datenschutzrechtliche Vorschriften ermittelt worden sind. Das BAG bewältigt dieses Problem in ständiger Judikatur mit einer Abwägung zwischen dem Schutz des informationellen Selbstbestimmungsrechts als Ausfluss des allgemeinen Persönlichkeitsrechts des Arbeitnehmers auf der einen Seite und dem Interesse an einer funktionstüchtigen Rechtspflege auf der anderen Seite. Dabei überwiegt das Verwertungsinteresse des Arbeitgebers (nur) dann, wenn zu seinem Beweisinteresse weitere Aspekte hinzutreten, die sein Interesse an der Beweiserhebung als schutzbedürftig erscheinen lassen.[144] Insoweit führt die Judikatur in Fortführung einer älteren Entscheidung des BGH zur rein materiellrechtlichen Reichweite des Persönlichkeitsrechts[145] als Beispiel insbesondere das Bestehen einer Notwehrsituation oder einer notwehrähnlichen Lage des Beweisführers an.[146] Diese im Grundansatz auch vom BVerfG[147] ebenso wie vom BGH[148] geteilte Sichtweise[149] hat zur Folge, dass sich die Existenz eines Verwertungsverbots letztlich erst aus einer umfassenden Interessenabwägung ergibt.[150] Dies dient der Einzelfallgerechtigkeit, bewirkt dafür im Gegenzug aber eine gewisse Rechtsunsicherheit[151] und verringert im Vergleich zu einem generellen Verwertungsverbot zudem den Anreiz für den Arbeitgeber, sich bei der Überwachung der Beschäftigten um eine Einhaltung der rechtlichen Grenzen zu bemühen.

---

144 Vgl. BAG 29.10.1997 – 5 AZR 508/96, BAGE 87, 31 = NZA 1998, 307; BAG 13.12.2007 – 2 AZR 537/06, NZA 2008, 1008; BAG 23.4.2009 – 6 AZR 189/08, BAGE 130, 347 = NZA 2009, 374; BAG 16.12.2010 – 2 AZR 485/08, NZA 2011, 571; BAG 21.6.2012 – 2 AZR 153/11, BAGE 142, 176 = NZA 2012, 1025; BAG 20.6.2013 – 2 AZR 546/12, BAGE 145, 278 = NZA 2014, 143; BAG 21.11.2013 – 2 AZR 797/11, BAGE 146, 303 = NZA 2014, 243.

145 BGH 20.5.1958 – VI ZR 104/57, BGHZ 27, 284, 289 f.

146 Siehe BAG 13.12.2007 – 2 AZR 537/06, NZA 2008, 1008 Rn. 36; BAG 20.6.2013 – 2 AZR 546/12, BAGE 145, 278 = NZA 2014, 143 Rn. 29.

147 Vgl. BVerfG 9.10.2002 – 1 BvR 1611/96 u.a., BVerfGE 106, 28 (48-50); BVerfG 13.2.2007 – 1 BvR 421/05, BVerfGE 117, 202 (240-241).

148 BGH 18.2.2003 – XI ZR 163/02, NJW 2003, 1727; BGH 12.1.2005 – XII ZR 227/03, BGHZ 162, 1, 5, jeweils m.w.N.

149 Vergleichbar auch VGH Baden-Württemberg 28.12.2000 – PL 15 S 2838/99, NJW 2001, 1082; großzügiger dagegen offenbar der EGMR 27.5.2014 – 10764/09, NJW 2015, 1079 Rn. 35 u. 38 – De la Flor Cabrera.

150 Dazu aus der Sicht des BAG Eylert, Kündigung nach heimlicher Arbeitnehmerüberwachung, NZA Beilage 3/2015, S. 100-107 (106); aus der Judikatur vgl. bejahend BAG 29.10.1997 – 5 AZR 508/96, BAGE 87, 31 = NZA 1998, 307; BAG 20.6.2013 – 2 AZR 546/12, BAGE 145, 278 = NZA 2014, 143; BAG 21.11.2013 – 2 AZR 797/11, BAGE 146, 303 = NZA 2014, 243; verneinend BAG 21.6.2012 – 2 AZR 153/11, BAGE 142, 176 = NZA 2012, 1025 (zu § 6b Abs. 2 BDSG); im Erg. auch BVerfG 31.7.2001 – 1 BvR 304/01, NZA 2002, 284; ferner etwa LAG Hamm 10.7.2012 – 14 Sa 1711/10, ZD 2013, 135 (Verstöße gegen § 206 StGB, § 88 TKG, § 32 BDSG); jüngst LAG Rheinland-Pfalz 26.2.2016 – 1 Sa 164/15, Juris.

151 Zur gegenwärtigen Rechtsunsicherheit in dieser Frage eindringlich Becker, FS 100 Jahre Rechtswissenschaft in Frankfurt (2014), S. 421-451 (448-450). Zum Versuch einer Steuerung der Interessenabwägung durch gestufte Regel-Ausnahme-Verhältnisse siehe Morgenroth, Verfassungsrechtliche Überlegungen zu Verwertungsverboten im Arbeitsrecht, NZA 2014, 408-414 (409).

3.3.2 Präventiver kollektivrechtlicher Schutz durch Mitbestimmung

Auf der Ebene des Betriebsverfassungsrechts hat der präventive Schutz durch den Betriebsrat durch Ausübung des Mitbestimmungsrechts bei technischen Einrichtungen gemäß § 87 Abs. 1 Nr. 6 BetrVG die größte Durchschlagskraft, während andere Beteiligungsrechte einschließlich des Kontrolle des Arbeitgeberverhaltens auf Einhaltung der Vorschriften des BDSG im Hinblick auf Beschäftigtendaten nach § 80 Abs. 1 Nr. 1 BetrVG eine geringere Relevanz haben.

Das für § 87 Abs. 1 Nr. 6 BetrVG erforderliche Merkmal der „technischen Einrichtung" wird von der Rechtsprechung seit jeher weit ausgelegt. Schon an dieser Stelle ausgegrenzt werden nur solche Überwachungen, die von Vorgesetzten etc. auf „natürlichem" Wege vorgenommen werden oder bei denen lediglich einfachste Hilfsmittel wie ein Kugelschreiber verwendet werden.[152] Dagegen wurde selbst eine Stoppuhr als technisches Gerät eingestuft und erst auf einer weiteren Prüfungsstufe (dazu sogleich) das Mitbestimmungsrecht verneint.[153]

Damit unterfallen alle hier in Rede stehenden neueren technischen Entwicklungen im Ausgangspunkt problemlos dem Begriff der „technischen Einrichtung". Wenn das BAG in jüngerer Zeit das System SAP-ERP und damit offenbar die Software als solche hierher gerechnet hat, sollen offenbar auch immaterielle Phänomene einbezogen werden.[154] Eine nähere Auseinandersetzung mit dieser Frage ist indes nicht erforderlich, weil jedenfalls die Einheit aus Rechner und Programm als technische Einrichtung betrachten werden kann bzw. sämtliche digitalen Anwendungen irgendeine gegenständliche Grundlage haben, selbst wenn diese noch so einfach und miniaturisiert ist. Demnach handelt es sich etwa bei Lokalisierungssystemen auf GPS- oder RFID-Basis ohne weiteres um technische Einrichtungen.[155] Dasselbe gilt für biometrische Verfahren (z. B. ein Fingerprint-Scanner-System).[156] Ferner ist auch eine vom Arbeitgeber betriebene Facebook-Seite unter den Begriff der technischen Einrichtung zu fassen,[157] wobei für ein rein innerbetriebliches Kommunikationssystem selbstverständlich nichts anderes gelten kann. Die eigentlich entscheidenden Fragen betreffen andere Aspekte, nämlich der Begriff und der Gegenstand der Überwachung sowie die Anforderungen, die erfüllt sein müssen, damit von einer Überwachung gerade durch die technische Einrichtung gesprochen werden kann.

Soweit es um den Begriff der Überwachung geht, hat sich mittlerweile ein weites Verständnis herauskristallisiert, nach dem alle Phasen der Kontrolle einbezogen sind, von der Datenerhebung über die Auswertung von erhobenen Daten bis hin zur Beurteilung im Wege eines Soll-Ist-Vergleichs.[158] Überwachen heißt nach ständiger Rechtsprechung des

---

[152] Vgl. BAG 24.11.1981 – 1 ABR 108/79, BAGE 37, 112 = DB 1982, 1116.

[153] BAG 8.11.1994 – 1 ABR 20/94, NZA 1995, 313.

[154] BAG 25.9.2012 – 1 ABR 45/11, NZA 2013, 275 Rn. 22; vergleichbar bereits BAG 14.11.2006 – 1 ABR 4/06, BAGE 120, 146 = NZA 2007, 399 (BSR = Brokerage System Redesign).

[155] Vgl. ArbG Kaiserlautern 27.8.2008 – 1 BVGa 5/08, Juris (GPS); ArbG Dortmund 12.3.2013 – 2 BV 196/12, NZA-RR 2013, 474 (GPS-gestütztes Fleetboard-Management).

[156] BAG 27.1.2004 – 1 ABR 7/03, BAGE 109, 235 = NZA 2004, 556 (unter II 1 c bb).

[157] ArbG Düsseldorf 21.6.2013 – 14 BVGa 16/13, NZA-RR 2013, 470; in diesem Sinne auch LAG Düsseldorf 12.1.2015 – 9 TaBV 51/14, NZA-RR 2015, 355.

[158] Vgl. Fitting, BetrVG, 28. Aufl. (2016), § 87 Rn. 217.

BAG sowohl das Sammeln von Informationen als auch das Auswerten bereits vorliegender Informationen.[159] Nach einer anderen Wendung müssen die Informationen auf technische Weise ermittelt und dokumentiert werden, sodass sie zumindest für eine gewisse Dauer verfügbar bleiben und vom Arbeitgeber herangezogen werden können.[160] Zugleich hat das BAG aber wiederholt betont, dass es genügt, wenn ein Teil des Überwachungsvorgangs mittels einer technischen Einrichtung erfolgt.[161] Letztlich kann kein Zweifel daran bestehen, dass sich das Mitbestimmungsrecht grundsätzlich auf alle Phasen des Umgangs mit personenbezogenen Daten erstrecken kann, wenn hierdurch eine Kontrolle ausgeübt wird.

Weiter müssen sich die Daten auf die Leistung oder auf das Verhalten von Arbeitnehmern beziehen. Diese Voraussetzung liegt bei allen geschilderten Kontrollmaßnahmen, mit denen die Beschäftigten gezielt überwacht werden sollen, von vornherein unproblematisch vor. Anders ist es dagegen bei den Anwendungen, bei denen es zunächst nur um eine reine Erfassung und Auswertung von Betriebsdaten geht, also um solche Daten, die etwa die bloße Steuerung von Produktionsabläufen, die Logistik und den Ressourcenverbrauch betreffen, wie dies bei zahlreichen Industrie 4.0-Prozessen der Fall sein kann. Sobald freilich aus diesen Betriebsdaten durch die Verknüpfung mit weiteren Informationen, die im System vorhanden sind oder sich zumindest mit einem vertretbaren Aufwand gewinnen lassen, auf die individuelle Leistung bzw. das individuelle Verhalten von Arbeitnehmern geschlossen werden kann, wird man aus Schutzzweckgesichtspunkten das Mitbestimmungsrecht entsprechend einer in der Literatur vertretenen Sichtweise[162] schon nach geltendem Recht eingreifen lassen müssen. Hierfür kann man sich allerdings soweit ersichtlich nicht auf eine gefestigte Rechtsprechung des BAG berufen. Die PAISY-Entscheidung betraf den Fall, dass aus einem nicht nur aus Leistung- oder Verhaltensdaten bestehenden Datenbestand Aussagen über die Leistung oder das Verhalten von Arbeitnehmern gewonnen wurden, während die bloße Verknüpfungsmöglichkeit nicht Gegenstand des Rechtsstreits war.[163]

Schließlich muss die technische Einrichtung aus sich selbst heraus die Überwachung bewirken. Insoweit genügt es auf der einen Seite, dass sie dazu objektiv geeignet ist, während eine subjektive Überwachungsabsicht seitens des Arbeitgebers hierfür nicht erforderlich ist. Auf der anderen Seite verlangt das BAG aber nach wie vor eine Unmittelbarkeit der Kontrolle.[164] Die technische Einrichtung muss also zumindest einen Teil der Überwachung automatisch bewerkstelligen, weil nur dann der

---

[159] BAG 14.9.1984 – 1 ABR 23/82, BAGE 46, 367 = NZA 1985, 28 (Technikerberichtssystem); BAG 14.11.2006 – 1 ABR 4/06, BAGE 120, 146 = NZA 2007, 399.

[160] BAG 10.12.2013 – 1 ABR 43/12, NZA 2014, 439; ähnlich BAG 27.1.2004 – 1 ABR 7/03, BAGE 109, 235 = NZA 2004, 556.

[161] BAG 15.12.1992 – 1 ABR 24/92, CR 1994, 111; BAG 10.12.2013 – 1 ABR 43/12, NZA 2014, 439.

[162] Fitting, BetrVG, 28. Aufl. (2016), § 87 Rn. 226; DKKW/Klebe, BetrVG, 15. Aufl. (2016), § 87 Rn. 182 f.

[163] Vgl. BAG 11.3.1986 – 1 ABR 12/84, BAGE 51, 217 = NZA 1986, 526.

[164] Grdl. BAG 9.9.1975 – 1 ABR 20/74, BAGE 27, 256 = DB 1975, 2233; BAG 10.12.2013 – 1 ABR 43/12, NZA 2014, 439. Beim Einsatz von Rechnern kommt es hierfür auf die jeweils verwendeten (System- oder Anwendungs-)Programme an: BAGE 44, 285 = DB 1984, 775. Die im Schrifttum vertretene These von der Aufgabe des Unmittelbarkeitskriteriums durch das BAG (so Fitting, BetrVG, 28. Aufl. (2016), § 87 Rn. 226; DKKW/Klebe, BetrVG, 15. Aufl. (2016), § 87 Rn. 186) erscheint vor dem Hintergrund des Urteils vom 10.12.2013, a.a.O. (Rn. 20) voreilig.

Überwachungsdruck besteht, der durch das Mitbestimmungsrecht präventiv abgemildert werden soll. Aus diesem Grunde hat das BAG etwa den Einsatz des Routenplaners *Google Maps* als nicht mitbestimmungspflichtig angesehen, weil eine etwaige Kontrolle von Reisekostenabrechnungen im konkreten Fall nicht durch die technische Einrichtung erfolgt, sondern die Entfernungsdaten lediglich die individuelle Kontrolle der Abrechnung durch den zuständigen Mitarbeiter unterstützen.[165] Diese – nicht unumstrittene – Einschränkung steht einem Mitbestimmungsrecht in den hier fraglichen Fallgruppen allerdings regelmäßig nicht entgegen.

Sofern ein Mitbestimmungsrecht gemäß § 87 Abs. 1 Nr. 6 BetrVG besteht, kann der Betriebsrat der Einführung und Anwendung technischer Einrichtungen mithilfe des von der Rechtsprechung anerkannten allgemeinen Unterlassungsanspruchs bis zu einer ordnungsgemäßen Beteiligung entgegentreten und diesen Anspruch gegebenenfalls mit einer einstweiligen Verfügung durchsetzen.[166] Darüber hinaus besteht nach allgemeiner Ansicht sogar ein Zurückbehaltungsrecht der betroffenen Arbeitnehmer bei gleichzeitiger Aufrechterhaltung des Entgeltanspruchs.[167]

Dagegen wird ein Sachvortrags- und Beweisverwertungsverbot im Hinblick auf Erkenntnisse, die ein Arbeitgeber infolge einer Maßnahme unter Verletzung des Mitbestimmungsrechts des Betriebsrats gewonnen hat, vom BAG mittlerweile klar abgelehnt.[168]

4. Legislativer Fortentwicklungsbedarf

4.1 Neue europarechtliche Rahmenbedingungen

Mit der Europäischen Datenschutz-Grundverordnung vom 27. April 2016, die ab dem 25. Mai 2018 gilt, sind die Koordinaten des Rechtsrahmens neu justiert worden.

Im Hinblick auf den Beschäftigtendatenschutz zunächst sind zwei Eckpunkte festzuhalten: Auf der einen Seite enthält die DS-GVO eine Reihe von grundlegenden Prinzipien und Regeln, die aufgrund ihres Charakters als Verordnung in den Mitgliedstaaten der EU als unmittelbar geltendes Recht anwendbar sind (Art. 288 Abs. 2 AEUV) und damit grundsätzlich auch für Arbeitsverhältnisse gelten. Auf der anderen Seite sieht Art. 88 DS-GVO für die „Datenverarbeitung im Beschäftigungskontext“ zwar keine umfassende Bereichsausnahme vor, wohl aber eine – hart umkämpfte – Öffnungsklausel für die Mitgliedstaaten zugunsten „spezifischerer Vorschriften“ vor.

Soweit es um die allgemeinen Regeln der DS-GVO geht, soll an dieser Stelle nur darauf hingewiesen werden, dass die Verordnung am Grundsatz des Verbots der Verarbeitung

---

165 BAG 10.12.2013 – 1 ABR 43/12, NZA 2014, 439.

166 Exemplarisch ArbG Kaiserslautern 27.8.2008 – 1 BVGa 5/08, Juris (Einbau von GPS-Geräten).

167 Fitting, BetrVG, 28. Aufl. (2016), § 87 Rn. 256.

168 BAG 13.12.2007 – 2 AZR 537/06, NZA 2008, 1008 (für § 87 Abs. 1 Nr. 1 BetrVG); andere Tendenz aber noch in BAG 12.1.1988 – 1 AZR 352/86, NZA 1988, 621 (622): Keine Datenverwertung durch Arbeitgeber, wenn Mitbestimmungsrecht des Personalrats nicht beachtet.

personenbezogener Daten mit Erlaubnisvorbehalt festhält und als Erlaubnistatbestände u.a. die Einwilligung der betroffenen Person und die Erfüllung eines Vertrags vorsieht (Art. 6 Abs. 1 UAbs. 1 Buchst. a und b DS-GVO). Auch wird der Grundsatz der Zweckbindung festgeschrieben, wobei dieser Grundsatz zunächst dahin konkretisiert wird, dass personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden müssen und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen (Art. 5 Abs. 1 Buchst. b DS-GVO). Hieran anschließend ist eine sehr vielschichtige Prüfung der Rechtmäßigkeit der Umwidmung vorgesehen (Art. 6 Abs. 4 DS-GVO). Im Übrigen ist hervorzuheben, dass mit Art. 82 DS-GVO nunmehr eine unmittelbar anwendbare Anspruchsgrundlage für den Ersatz materieller oder immaterieller Schäden durch den Verantwortlichen oder den Auftragsverarbeiter vorhanden ist, wenn eine Person wegen eines Verstoßes gegen die Verordnung einen entsprechenden Schaden erlitten hat.

Die Öffnungsklausel für mitgliedstaatliche Regelungen (Rechtsvorschriften und Kollektivvereinbarungen) soll nach dem Wortlaut von Art. 88 DS-GVO „spezifischere Vorschriften“ ermöglichen. Dies wirft die Frage auf, welche Konkretisierungskompetenz die Mitgliedstaaten dabei haben. Insoweit sind im gegenwärtigen Stadium nur erste Eckpunkte auszumachen. Auf der einen Seite fällt auf, dass die Öffnungsklausel nicht pauschal von der Zulässigkeit „günstigerer Vorschriften“ spricht bzw. die Regelungen der DS-GVO nicht mehr – wie im Vorschlag des Europäischen Parlaments[169] – als „Mindestnormen“ und „Mindeststandards“ bezeichnet werden. Auf der anderen Seite ist aber auch nicht mehr – wie im ursprünglichen Vorschlag der Europäischen Kommission[170] – ausdrücklich davon die Rede, dass sich diese spezifischen Vorschriften „in den Grenzen dieser Verordnung“ halten müssen.

Vor diesem Hintergrund wird man zunächst festhalten können, dass die Konkretisierungskompetenz keine Abweichung nach unten erlaubt, das Niveau des Beschäftigtendatenschutzes also nicht nach unten abgesenkt werden darf. In diesem Sinne äußern sich auch die ersten Stellungnahmen im Schrifttum.[171] Für diese Sichtweise spricht, dass die Öffnungsklausel als Zweck der mitgliedstaatlichen Regelung die Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigungsdaten nennt (Art. 88 Abs. 1 DS-GVO) und darüber hinaus anordnet, dass diese Vorschriften angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde und der berechtigten Interessen der Grundrechte der betroffenen Person umfassen (müssen) (Art. 88 Abs. 2 DS-GVO). Mit diesen Vorgaben würde sich eine Absenkung des Schutzniveaus nicht vereinbaren lassen.

Schwieriger ist die Frage zu beantworten, ob und in welcher Weise das Schutzniveau angehoben werden darf. Erste Stellungnahmen vermitteln den Eindruck, als ob die DS-GVO letztlich nur eine Art Mindestniveau darstellt, das zu Gunsten der Beschäftigten

---

169 Vgl. Legislative Entschließung des Europäischen Parlaments vom 12.3.2014 (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (zu Art. 82 DS-GVO-E).

170 Vgl. KOM(2012) 11 endg. vom 25.1.2012 (zu Art. 82 DS-GVO-E).

171 Kort, Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung, DB 2016, 711-716; Wybitul, Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte?, ZD 2016, 203-208 (207).

beliebig heraufgesetzt werden kann.[172] Diese Sichtweise dürfte mit der Grundkonzeption der DS-GVO indes nicht vereinbar sein. Gemäß Art. 1 DS-GVO geht es der Verordnung nämlich nicht nur um den Schutz personenbezogener Daten, sondern auch um den freien Verkehr solcher Daten innerhalb der Europäischen Union. Auch ist in Art. 88 DS-GVO selber von Zwecken „des Managements", vom „Schutz des Eigentums der Arbeitgeber oder der Kunden" (Abs. 1) sowie von der „Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe" (Abs. 2) die Rede. Diese Formulierungen würden keinen Sinn machen, wenn es den Mitgliedstaaten europarechtlich freistehen würde, jeden Umgang mit personenbezogenen Daten von Beschäftigten pauschal zu untersagen, um das Auslegungsproblem hierdurch bewusst zuzuspitzen. Hinzu kommt das entstehungsgeschichtliche Argument, dass sich der Parlamentsentwurf gerade nicht durchgesetzt hat.

Am meisten überzeugt daher eine Konzeption, nach der den Mitgliedstaaten zwar eine Ausfüllungskompetenz zusteht, die mitgliedstaatlichen Vorschriften aber nicht so ausgestaltet sein dürfen, dass den Unternehmen ein Umgang mit personenbezogenen Daten von Beschäftigten in einer über das Schutzniveau der DS-GVO hinausgehenden Weise deutlich erschwert und insbesondere der Datenverkehr innerhalb einer Unternehmensgruppe weitgehend zum Erliegen gebracht wird, weil auch dies nicht „angemessen" im Sinne von Art. 88 Abs. 2 DS-GVO wäre. So wäre es vor dem Hintergrund der Regelungen über die Einwilligung (Art. 7 DS-GVO) sowie insbesondere auch Erwägungsgrund 155 zwar nicht statthaft, die Einwilligung von Beschäftigten als Erlaubnistatbestand kategorisch auszuschließen.

Als zulässig wäre es aber beispielsweise anzusehen, im Hinblick auf den Grundsatz der Zweckbindung genauer festzulegen, unter welchen Voraussetzungen Daten auch für einen ursprünglich nicht vorgesehenen und dokumentierten Zweck verwendet werden dürfen. Letzteres spielt im Arbeitsverhältnis eine nicht unerhebliche Rolle, weil es nicht selten darum gehen kann, ob personenbezogene Daten, die zunächst lediglich zur besseren Steuerung von Arbeitsabläufen und zur Qualitätssicherung erhoben und verarbeitet worden sind, umfassend auch für die individuelle Leistungs- und Verhaltenskontrolle und dabei insbesondere für arbeitsrechtliche Sanktionen von der Abmahnung bis hin zur Kündigung genutzt werden dürfen.

Soweit es schließlich um biometrische Daten geht, können die Mitgliedstaaten gemäß Art. 9 Abs. 4 DS-GVO (ebenso wie für genetische und Gesundheitsdaten) Beschränkungen einführen.

4.2 Konkrete Regelungsvorschläge

Vor dem Hintergrund der rechtstatsächlichen Veränderungen und der gegenwärtigen rechtlichen Rahmenbedingungen einerseits sowie der (künftigen) europarechtlichen Vorgaben andererseits empfehlen sich folgende Vorschläge.

---

[172] Düwell/Brink, Die EU-Datenschutz-Grundverordnung und der Beschäftigtendatenschutz, NZA 2016, 665-668 (666); Kort, Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung, DB 2016, 711-716; Wytibul/Pötters, Der neue Datenschutz am Arbeitsplatz, RDV 10-16 (15).

Zunächst sollte ein eigenständiges Beschäftigtendatenschutzgesetz erarbeitet werden. Die DS-GVO schreibt dies zwar nicht vor. Aus der Perspektive des Unionsrechts könnte der deutsche Gesetzgeber sogar von jeder auf den Beschäftigtendatenschutz bezogenen speziellen Regelung absehen.[173] Ebenso steht es dem deutschen Gesetzgeber frei, die bisherige Vorschrift des § 32 BDSG aufrechtzuerhalten[174] oder neue Sondervorschriften zum Beschäftigtendatenschutz in ein novelliertes BDSG zu integrieren. Insoweit handelt es sich letztlich um eine Frage der gesetzgeberischen Zweckmäßigkeit. Gegen eine völlige Regelungsabstinenz spricht indes, dass die DS-GVO zwar grundsätzlich angemessene Prinzipien und Regeln für den Ausgleich der Interessen von Arbeitgeber und Arbeitnehmern bereithält. Allerdings bewegen sich diese teilweise auf einem sehr hohen Abstraktionsniveau und bieten der Praxis daher nur in eingeschränktem Maße eine Orientierungshilfe. Im Übrigen sollte sich ein gesetzgeberisches Handeln davon leiten lassen, der arbeitsrechtlichen Praxis ein möglichst klares und übersichtliches („benutzerfreundliches“) Regelungswerk an die Hand zu geben, um mit dem Massenphänomen des Umgangs mit personenbezogenen Daten von Beschäftigten umgehen zu können. Hiervon ist die gegenwärtige Ausgestaltung des BDSG insbesondere im Hinblick auf den Arbeitnehmerdatenschutz indes weit entfernt.

Dem Ziel einer praxisnahen und handhabbaren Regelung ohne eine komplizierte Verweisungstechnik kommt ein eigenständiges Beschäftigtendatenschutzgesetz am nächsten, was für eine derartige Lösung spricht. Als zweitbeste Lösung erscheint ein eigenständiger Abschnitt innerhalb eines neuen BDSG, der in einem möglichst geringen Maße mit den allgemeinen Vorschriften verzahnt wird, um Streitigkeiten über das Verhältnis verschiedener Vorschriften zueinander von vornherein entgegenzuwirken.

Regelungstechnisch empfiehlt sich im Hinblick auf neuere technologische Entwicklungen als Gegenstand dieser Expertise keine zu stark an einzelnen technologischen Entwicklungen orientierte Regelungstechnik, die durch Innovationen rasch überholt würde. Stattdessen empfiehlt sich die Festschreibung bestimmter Grundsätze. Hierzu sollten gehören:

- 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 Persönlichkeit)

Dagegen finden sich die erforderlichen Einschränkungen im Hinblick auf die anderweitige Verwendung erhobener Beschäftigtendaten bereits in Art. 6 Abs. 4 DS-GVO. Darüber hinaus enthält Art. 82 DS-GVO die aus Gründen der Klarheit notwendige Anspruchsgrundlage für einen Ersatz auch immaterieller Schäden.

---

[173] Ebenso aktuell Kühling/Martini et al., Die DSGVO und das nationale Recht (2016), S. 20, 298.

[174] In diesem Sinne auch Wybitul, Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte?, ZD 2016, 203-208 (206).

Ein Sonderproblem stellt die Frage eines Beweisverbots bei Verstößen gegen das Datenschutzrecht dar. Ausgangspunkt ist insoweit, dass die Gerichte wie dargelegt eine umfassende Güter- und Interessenabwägung zwischen dem Persönlichkeitsrecht des betroffenen Arbeitnehmers auf der einen Seite und dem Beweisführungsinteresse des Arbeitgebers auf der anderen Seite vornehmen. Damit erfolgt streng genommen gegebenenfalls auf zwei Stufen eine Interessenabwägung: Nämlich zum einen bei der Frage, ob eine Kontrollmaßnahme des Arbeitgebers materiellrechtlich zulässig gewesen ist, zum anderen – und zwar nur bei einer Verneinung dieser ersten Frage – bei der Folgefrage, ob sich der Arbeitgeber in einem Rechtsstreit mit dem Arbeitnehmer etwa über die Berechtigung einer Kündigung eines Beweismittels bedienen darf, das er auf rechtswidrige Art und Weise gewonnen hat. Allerdings werden beide Prüfungsstufen in der Rechtsprechung nicht immer klar voneinander getrennt. Zudem kann die erste Frage aus prozessökonomischen Gründen offen gelassen werden, wenn das Gericht bei einer Interessenabwägung zu dem Ergebnis gelangt, dass ein angebotenes Beweismittel auch dann zulasten des Arbeitnehmers verwertet werden kann, wenn es auf eine rechtswidrige Art und Weise gewonnen worden ist.

Für eine abstrakt-generelle Regelung, nach der jeder Verstoß gegen eine dem Persönlichkeitsschutz des Arbeitnehmers dienende datenschutzrechtliche Vorschrift zu einem Beweisverwertungsverbot führt, spricht die Rechtssicherheit, weil das Ergebnis einer gerichtlichen Interessenabwägung nur schwer prognostizierbar ist. Zudem würde ein Beweisverwertungsverbot die Präventionswirkung des Beschäftigtendatenschutzes erhöhen, weil Arbeitgeber in diesem Fall nicht mehr damit rechnen könnten, trotz eines gezielten Verstoßes gegen datenschutzrechtliche Bestimmungen die hierdurch gewonnenen Ergebnisse gleichwohl in einem anschließenden gerichtlichen Prozess erfolgreich vorbringen zu können. Ferner könnte auf diese Weise der möglichen Friktion von vornherein aus dem Weg gegangen werden, dass ein Arbeitnehmer wirksam gekündigt wird, der hierdurch eintretende Verlust des Arbeitsplatzes aber ein materieller Schaden ist, der unter Umständen nach Art. 82 DS-GVO ersetzt werden muss.

Allerdings sprechen auch gewichtige Gründe gegen die Einführung eines generellen Beweisverwertungsverbots bei Verstößen gegen beschäftigtendatenschutzrechtliche Vorschriften. Zum einen gibt es verschiedene andere wichtige gesellschaftliche Felder wie etwa familiäre Konflikte, in denen es nicht selten zu persönlichkeitsrechtsverletzenden Datenerhebungen kommt und bei denen sich ebenfalls die Frage stellt, ob und unter welchen Voraussetzungen ein Beweis verwertet werden darf. Eine auf das Arbeitsrecht beschränkte Regelung müsse sich daher dem Einwand stellen, dass es sich bei der Frage eines Beweisverwertungsverbotes letztlich um eine übergreifende zivilprozessuale bzw. verfassungsrechtliche Problematik handelt, für die sich isolierte Lösungen verbieten. Zwar stehen mit dem Bestand des Arbeitsverhältnisses für den Arbeitnehmer besonders wichtige Interessen auf dem Spiel.[175] Entsprechend gewichtige Interessen können aber auch in anderen Situationen betroffen sein, so etwa dann, wenn durch eine rechtswidrige Kameraüberwachung einem Unfallbeteiligten Verstöße gegen Verkehrsvorschriften nachgewiesen werden und dadurch eine Gefängnisstrafe droht. Zudem kann es in diesem Zusammenhang streng genommen nur darauf ankommen, wie intensiv die rechtswidrige Datenerhebung als solche in das Persönlichkeitsrecht des Arbeitnehmers eingreift, nicht

[175] Vgl. BVerfG 27.1.1998 – 1 BvL 15/87, BVerfGE 97, 169 (177).

aber darauf, ob der Arbeitgeber die auf diese Weise gewonnenen Daten anschließend für eine Kündigung nutzt, weil das Interesse des Arbeitnehmers am Fortbestand seines Arbeitsverhältnisses systemkonform durch das Kündigungsschutzrecht und nur reflexartig durch Beweisverwertungsverbote geschützt wird.

Wenn das allgemeine Persönlichkeitsrecht des Beschäftigten aber in unterschiedlich intensiver Weise tangiert werden kann, würde ein pauschales Beweisverwertungsverbot, bei dem es nicht mehr auf eine Abwägung mit den gegenläufigen Interessen des Arbeitgebers ankommt, über das Ziel hinausschießen. Man denke an einen vergleichsweise geringfügigen rechtswidrigen Eingriff in die Persönlichkeitsinteressen eines Arbeitnehmers, bei dem der Arbeitgeber einer schweren Verfehlung des Arbeitnehmers auf die Spur kommt. Schließlich sollte bei der rechtspolitischen Bewertung nicht außer Acht gelassen werden, dass die arbeitsgerichtliche Rechtsprechung mittels der von ihr vorgenommenen Interessenabwägung im Grundsatz bereits für einen vergleichsweise hohen Arbeitnehmerschutz sorgt, indem sie das einfache Beweisinteresse des Arbeitgebers gerade nicht ausreichen lässt, um das gegenläufige Persönlichkeitsinteresse des Arbeitnehmers zu überwinden. Auch wenn es immer einzelne Entscheidungen geben mag, die sich im Hinblick auf die Annahme eines solchen besonderen Beweisinteresses des Arbeitgebers großzügig zeigen, wird damit doch ein grundsätzlich angemessener Arbeitnehmerschutz etabliert, dessen Stärke vor allem darin liegt, den Umständen des Einzelfalls hinreichend Rechnung tragen zu können. Vor diesem Hintergrund erscheint es nicht ratsam, jedenfalls aber nicht geboten, in ein Beschäftigtendatenschutzgesetz zusätzlich eine Vorschrift über ein pauschales Beweisverwertungsverbot aufzunehmen.

Für den Bereich des kollektiven Arbeitsrechts empfiehlt sich:

- Klarstellung bzw. Regelung in § 87 Abs. 1 Nr. 6 BetrVG, dass der Umgang mit personenbezogenen bzw. personenbeziehbaren Daten von Beschäftigten der Mitbestimmung des Betriebsrats unterliegt.

Ob ein solcher Regelungsbedarf zu bejahen ist, hängt davon ab, ob es Gestaltungen gibt, die zum einen nach geltendem Recht zumindest nicht eindeutig von § 87 Abs. 1 Nr. 6 BetrVG erfasst werden, zum anderen aber sinnvollerweise einbezogen werden sollten. Die Frage stellt sich konkret im Hinblick auf die Erhebung und Speicherung von Statusdaten sowie von Betriebsdaten, die sich durch Verknüpfungen mit anderen Daten zu Aussagen über das Verhalten oder die Leistung von Arbeitnehmern verdichten lassen. Insoweit wird der seit 1972 unveränderte Gesetzestext noch recht stark von den damaligen Vorstellungen geprägt, die konzeptionell von der technischen Einrichtung und nicht vom seinerzeit noch nicht entwickelten Recht auf informationelle Selbstbestimmung ausgingen.[176] Es ist daher nicht völlig geklärt, wie weit die betriebliche Mitbestimmung bei der Datenverarbeitung im Einzelnen reicht, sofern diese sich nicht explizit auf Verhaltens- oder Leistungsdaten bezieht. Legt man demgegenüber die neuere verfassungsrechtliche Sichtweise zugrunde, dass es kein „belangloses“ personenbezogenes Datum gibt[177] und

---

[176] Vgl. BT-Drucks. VI/1786, S. 49 „da derartige Kontrolleinrichtungen stark in den persönlichen Bereich des Arbeitnehmers eingreifen“.

[177] Grdl. BVerfG 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 (45); bestätigt etwa in BVerfG 24.1.2012 – 1 BvR 1299/05, BVerfGE 130, 151 (183-184); ebenso BAG 25.9.2013 – 10 AZR 270/12, BAGE 146, 109 = NZA 2014, 41 Rn. 45.

Persönlichkeitsbeeinträchtigungen heutzutage eher von den Verarbeitungs- und Verknüpfungsmöglichkeiten ausgehen, die „Big Data“ eröffnet, spricht einiges dafür, den Umgang mit personenbezogenen bzw. personenbeziehbaren Daten von Beschäftigten in den Mittelpunkt des Mitbestimmungstatbestands zu stellen.

Die Regelung eines Beweisverwertungsverbots bei Verstößen gegen das Mitbestimmungsrecht würde trotz der gegenläufigen verfassungsrechtlichen Positionen (u.a. rechtliches Gehör des Arbeitgebers, Allgemeininteresse an funktionsfähiger Rechtspflege) noch innerhalb des einfachrechtlichen Spielraums liegen. Der Gesetzgeber wäre also nicht von vornherein daran gehindert, denjenigen Stimmen, die sich schon nach geltendem Recht für ein solches Beweisverwertungsverbot aussprechen,[178] zum Durchbruch zu verhelfen. Allerdings erscheint eine dahingehende Regelung nicht geboten. Auch wenn ein Beweisverwertungsverbot das Mitbestimmungsrecht effektivieren würde, erfordert es der spezifische Zweck des § 87 Abs. 1 Nr. 6 BetrVG (Schutz und Teilhabe) gleichwohl nicht zwingend, dass ein Verstoß gegen die betriebliche Mitbestimmung als solcher selbst dann zur Unverwertbarkeit der erhobenen Daten führt, wenn das Persönlichkeitsrecht des betroffenen Arbeitnehmers nicht verletzt wird.[179]

Zudem ist eine Verwertung von Beschäftigtendaten in einem Prozess keine Handlung, die materiellrechtliche Positionen schmälert und die deshalb aufgrund der Theorie von der Wirksamkeitsvoraussetzung der betrieblichen Mitbestimmung als individualrechtlich unwirksam einzustufen ist. Darüber hinaus sieht die Arbeitsrechtsordnung sowohl auf der kollektivrechtlichen als auch auf der individualrechtlichen Ebene verschiedene andere Rechtsbehelfe und Rechtsfolgen für den Fall eines Verstoßes gegen § 87 Abs. 1 Nr. 6 BetrVG vor,[180]sodass schon der gegenwärtige Rechtszustand das Mitbestimmungsrecht in einem nicht unbeträchtlichen Maße absichert.[181]

Letztlich hängt die Entscheidung über die Einführung eines Beweisverwertungsverbot davon ab, ob man der Feststellung des materiellen Rechts in einem gerichtlichen Verfahren einen eigenständigen Wert beimisst oder das prozessuale Handeln des Arbeitgebers nur als einen unselbstständigen Annex seines betrieblichen Handelns begreift und deshalb das Telos der Mitbestimmung auch auf einen Arbeitsgerichtsprozess durchschlagen lässt.

---

[178] Vgl. LAG Bremen 28.7.2005 – 3 Sa 98/05, RDV 2006, 24; Fischer, BB 1999, 154-157 (155-157); DKKW/Klebe, BetrVG, 15. Aufl. (2016), § 87 Rn. 6.

[179] Eingehend Schlewing, Prozessuales Verwertungsverbot für mitbestimmungswidrig erlangte Erkenntnisse aus einer heimlichen Videoüberwachung?, NZA 2004, 1071-1077 (1074-1077).

[180] Vgl. BAG 13.12.2007 – 2 AZR 537/06, NZA 2008, 1008 (für § 87 Abs. 1 Nr. 1 BetrVG).

[181] Aus diesem Grund gegen ein Beweisverwertungsverbot de lege lata Fitting, BetrVG, 28. Aufl. (2016), § 87 Rn. 607, anders noch Fitting, BetrVG, 25. Aufl. (2010), § 87 Rn. 256.

5. Zusammenfassung

5.1 Problemstellung

Die Digitalisierung des Wirtschafts- und Arbeitslebens führt dazu, dass im Zusammenhang mit betrieblichen Prozessen eine immer größere Menge an Daten entsteht und verarbeitet wird. Dies gilt sowohl für den industriellen Bereich („Industrie 4.0“) als auch für den Dienstleistungssektor. Hierbei werden häufig nicht lediglich reine Betriebsdaten erhoben und ausgewertet, sondern in einem erheblichen und ständig zunehmenden Maße auch personenbezogene Daten von Beschäftigten erfasst und verarbeitet. Insoweit können phänomenologisch drei Grundformen des Umgangs mit solchen Daten unterschieden werden: Zum einen kann die Erhebung von Beschäftigtendaten bloße Begleiterscheinung der Optimierung von betrieblichen Prozessen sein, deren eigentliches Ziel in der Steigerung der Effektivität technischer oder logistischer Abläufe liegt. Zum anderen können die technischen Möglichkeiten aber auch gezielt dazu genutzt werden, die Leistung und das Verhalten von Beschäftigten zu steuern und zu überwachen. Gleichsam dazwischen liegt die Fallgruppe, in denen die Daten von Beschäftigten, die zunächst zur Prozessoptimierung generiert worden sind, anschließend bewusst zur Leistungs- bzw. Verhaltenskontrolle verwendet werden.

Das Datenschutzrecht sollte von dem Grundgedanken geprägt werden, einen angemessenen Ausgleich herbeizuführen zwischen dem berechtigten Interesse des Arbeitgebers, betriebliche Prozesse zu verbessern und die Leistung der Beschäftigten zu kontrollieren, und dem gegenläufigen Interesse der Arbeitnehmer an einem Schutz ihrer Persönlichkeit im Zusammenhang mit der von ihnen ausgeübten Beschäftigung. Hierzu bedarf es einer realistischen Einschätzung der technischen Möglichkeiten zur Überwachung von Beschäftigten als Regulierungskontext, um auf dieser Basis eine tragfähige rechtliche Architektur zu entwickeln, wobei es aus datenschutzrechtlicher Perspektive letztlich darauf ankommt, welche konkreten Aspekte der Persönlichkeit der Arbeitnehmer in welcher Intensität von einer Kontrolltechnik betroffen werden. Zudem müssen sich alle existierenden und neu zu schaffenden Regulierungen auf der Ebene des deutschen Rechts in den Grenzen des Unionsrechts halten und damit konkret vor allem der – ab dem 25. Mai 2018 geltenden – Europäischen Datenschutz-Grundverordnung.

5.2 Ergebnisse

5.2.1 Neuere technische Entwicklungen mit Kontrollpotenzial

Folgende neuere technische Entwicklungen bzw. Anwendungen können im Beschäftigungskontext identifiziert werden, die mit einem datenschutzrechtlich relevanten Kontrollpotenzial verbunden sind:

- *Lokalisierungssysteme*
  Zur Lokalisierung von Beschäftigten innerhalb von Betriebsstätten kommen vorwiegend RFID-Systeme zum Einsatz. Verwendungszweck sind z.B. Zeiterfassungen und Zugangskontrollen. Außerhalb von Betriebsstätten stehen die Mobilfunkendgerät-Ortung (Handy-Ortung) sowie die Übermittlung von GPS-Positionsdaten im Vordergrund. Verwendungszweck sind vielfach das

Flottenmanagement von Speditionen o.ä. sowie das Tracking spezifischer Transporte.

- *Biometrische Verfahren*
  Biometrische Verfahren knüpften an physiologische oder verhaltensbezogene Merkmale von Beschäftigten an. Durch den Vergleich von aktuell erhobenen und hinterlegten Datensätzen wird die Frage einer Personenidentität festgestellt. Verwendungszweck sind die Authentifizierung und die Autorisierung insbesondere beim Zugang zu besonders geschützten Bereichen.

- *Mobile Arbeitszeit- und Projektzeiterfassung*
  Bei diesen Systemen geht es regelmäßig um die zunächst manuelle Eingabe entsprechender Daten durch die Beschäftigten in mobile Endgeräte und die anschließende Übermittlung dieser Daten – gegebenenfalls in Echtzeit per mobilem Internet – an eine betriebliche Datenbank zur weiteren Verarbeitung. Verwendungszwecke sind im Außenverhältnis gegenüber Kunden die Auftragsabrechnung sowie im Verhältnis zu den Mitarbeitern die Arbeitskontenführung, die Entgeltabrechnung und die Reisekostenabrechnung.

- *Nutzeraktivitäten an stationären und mobilen Endgeräten*
  Am Markt frei verfügbare Programme können heutzutage das gesamte Nutzerverhalten an stationären und mobilen Endgeräten (Dateneingabe, Kommunikationsverhalten per E-Mail, Internetverlauf, Zeiten der Inaktivität etc.) permanent in Echtzeit überwachen („Spionageprogramme“). Als Verwendungszweck kommen die punktuelle wie auch die umfassende Kontrolle des Mitarbeiterverhaltens in Betracht, soweit es in irgendeiner Beziehung zu einem stationären oder mobilen Endgerät steht und der Arbeitgeber ein entsprechendes Programm auf dem Gerät installiert hat.

- *Industrie 4.0-Anwendungen*
  Die Digitalisierung von betrieblichen Abläufen im industriellen Bereich („Industrie 4.0“) zielt auf eine umfassende digitale Vernetzung der gesamten Wertschöpfungskette. Zu den Kernelementen gehört zum einen die autonome Kommunikation zwischen Maschinen bzw. Werkstücken, um hierdurch den gesamten Wertschöpfungsvorgang zu optimieren (Ersparnis unproduktiver Wartezeiten, Vermeidung bzw. Verkürzung von Produktionsstörungen, Schonung von Ressourcen etc.). Zum anderen wird die Mensch-Maschine-Interaktion in einem immer stärkeren Maße durch digitale Technologien geprägt. Dies betrifft mobile Assistenzsysteme (*Wearables*) wie etwa der Einsatz digitaler Werkzeuge (Datenbrille, intelligenter Handschuh), aber auch der zunehmende Einsatz von Industrierobotern. Bei diesen Vorgängen fallen häufig in hohem Maße personenbezogene Daten an, zumal manche Systeme zur Optimierung betrieblicher Produktionsabläufe auf individualisierten Nutzerkonten aufbauen. Zu den weiteren Anwendungsbereichen zählt die vorausschauende Wartung (*Predictive Maintenance*).

- *Sonstige inner-und außerbetriebliche Assistenzsysteme*
  Mit Hilfe von Handscannern können auch außerhalb des industriellen Bereichs Verfahrensabläufe optimiert werden, wobei sich im Falle eines kontinuierlichen

Einsatzes dieser Geräte für zahlreiche einzelne Arbeitsschritte bei einer entsprechenden Programmierung zugleich das gesamte Arbeitsverhalten von Beschäftigten aufzeichnen, auswerten und dadurch kontrollieren lässt.

- *Sprachgebrauchs- und Stimmungsanalyseverfahren*
  Durch Sprachgebrauchs- und Stimmungsanalyseverfahren können und sollen insbesondere bei Mitarbeitern in Call-Centern die Verwendung bestimmter Worte (*Keyword Spotting*) sowie Mentalitätszustände überwacht bzw. beeinflusst werden.

- *Auswertung innerbetrieblicher sozialer Netzwerke*
  Die innerbetriebliche Kommunikation erfolgt in vielen Unternehmen bzw. Konzernen zunehmend über organisationsinterne soziale Netzwerke. Diese sozialen Netzwerke erlauben es, die in einer Organisation vorhandene und sich ständig verändernde Kommunikationsstruktur grafisch abzubilden (*Enterprise Social Graph*) und nach verschiedenen Kriterien zu analysieren. Hierdurch können die innerhalb der Belegschaft bestehenden informellen Kommunikationskanäle zum Vorschein gebracht werden.

- *Fitnessdaten*
  Tragbare Fitness-Tracker erlauben es Mitarbeitern, ihre Gesundheits- und Fitnessdaten zu erheben und das eigene Verhalten daran zu orientieren. Zugleich ist nicht ausgeschlossen, dass diese Daten gegebenenfalls für betriebliche Zwecke (Gesundheitsmanagement, personalpolitische Entscheidungen) genutzt werden.

- *Durchleuchtung der Persönlichkeit mittels Sprachanalyseverfahren*
  Zu den neuesten Trends gehören Sprachanalyseverfahren. Mit diesen digital unterstützten Anwendungen wird der Gebrauch der Sprache in Wort und Schrift zahlreiche digitale Bausteine zerlegt und mit den in einer hinterlegten Referenzdatensätzen verglichen, um daraus auf die Persönlichkeitsstruktur bzw. einzelne Persönlichkeitsmerkmale der betroffenen Person zu schließen. Diese Verfahren können in Bewerbungssituationen oder im Vorfeld sonstiger personalpolitischer Maßnahmen zum Einsatz gebracht werden.

5.2.2 Gegenwärtiger Rechtsrahmen

Die zahlreichen rechtlichen Regelungen auf europäischer Ebene (Datenschutzgrundrecht gemäß Art. 8 GRC und Datenschutzrichtlinie 95/46/EG), deutscher Ebene (Grundrecht auf informationelle Selbstbestimmung gemäß Art. 1 Abs. 1 und Art. 2 Abs. 1 GG sowie BDSG) und internationaler Ebene (Art. 8 EMRK) laufen letztlich darauf hinaus, dass der Arbeitgeber nur dann mit personenbezogenen Daten von Beschäftigten umgehen (d. h. sie erheben, verarbeiten oder nutzen) darf, wenn dies für die Zwecke des Beschäftigungsverhältnisses erforderlich und angemessen ist. Dabei muss grundsätzlich Transparenz gewahrt und der Zweck des jeweiligen Umgangs mit den Beschäftigtendaten vorab klar festgelegt werden.

Auf dieser Grundlage können folgende Aussagen getroffen werden:

- *Lokalisierungssysteme*
  Innerbetriebliche und außerbetriebliche Lokalisierungssysteme sind dann statthaft, sofern sie für die Gewährleistung der persönlichen Sicherheit des Mitarbeiters im Einzelfall erforderlich sind. Geht es (nur) um den Schutz von Vermögenswerten des Arbeitgebers, ist es dagegen regelmäßig nicht erforderlich, über die Ortung der Betriebsmittel hinaus den Standort von Beschäftigten festzustellen. Jedenfalls dürfen entsprechende Daten nicht zu einer allgemeinen Leistungs- bzw. Verhaltenskontrolle genutzt werden. Lokalisierungssysteme können grundsätzlich zur Effektivierung betriebliche Abläufe eingesetzt werden. Regelmäßig zulässig ist auch die Einrichtung von Zugangskontrollsystemen. Bei alledem ist die Erstellung umfassender Bewegungsprofile aber als unzulässig anzusehen. Lokalisierungen haben grundsätzlich in einer für den betroffenen Arbeitnehmer erkennbaren Weise stattzufinden. Eine heimliche Ortung ist in Anlehnung an die vom BAG aufgestellten Grundsätzen zur heimlichen Videoüberwachung eines Beschäftigten (allenfalls) zulässig, wenn der konkrete Verdacht einer strafbaren Handlung zulasten des Arbeitgebers vorliegt, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind und die verdeckte Lokalisierung insgesamt nicht unverhältnismäßig ist.

- *Biometrische Verfahren*
  Biometrische Verfahren können grundsätzlich nur zum Zwecke der Authentifizierung und der Autorisierung als zulässig angesehen werden. Hinzukommen muss, dass es einen hinreichend gewichtigen Grund für eine solche Zwecksetzung gibt (z.B. Zugang zu besonders geschützten Bereichen) und die verwendeten Merkmale eine möglichst geringe Eingriffstiefe aufweisen.

- *Mobile Arbeitszeit- und Projektzeiterfassung*
  Mobile Arbeitszeits- und Projektzeiterfassung begegnen bei manueller Dateneingabe durch die Beschäftigten und hinreichender Transparenz über die Verwendung der erhobenen Daten keinen Bedenken.

- *Nutzeraktivitäten an stationären und mobilen Endgeräten*
  Eine umfassende Dauerkontrolle aller Nutzeraktivitäten an stationären und mobilen Endgeräten für Zwecke der Leistungs- und Verhaltenskontrolle von Beschäftigten ist auch bei voller Transparenz stets unverhältnismäßig. Als zulässig sind grundsätzlich nur punktuelle Kontrollen bestimmter Anwendungen mit einem klar definierten Zweck (z.B. einer Qualitätskontrolle) anzusehen. Eine heimliche Kontrolle ist wiederum von vornherein nur unter den genannten strengen Voraussetzungen statthaft und muss sich zudem auf einzelne Aktivitäten beschränken.

- *Industrie 4.0-Anwendungen*
  Zwecks Effektivierung von betrieblichen Produktionsabläufen („Industrie 4.0“) kann es im Einzelfall erforderlich sein, nicht nur Betriebsdaten, sondern auch personenbezogene Daten von Beschäftigten zu erheben und zu verarbeiten. Hierfür können Nutzerkonten angelegt werden. Die hierbei gewonnenen und gespeicherten Datenmengen dürfen aber grundsätzlich nur dazu verwendet werden, die betrieblichen Prozesse zu verbessern oder auch einen individuellen Qualifizierungsbedarf zu ermitteln werden, nicht aber die Leistung und das

Verhalten der Beschäftigten zu kontrollieren. Eine Überwachung des kompletten Arbeitsverhaltens als Konsequenz einer umfassenden Digitalisierung sämtlicher Arbeitsschritte wäre in jedem Fall unzulässig.

- *Sonstige inner-und außerbetriebliche Assistenzsysteme*
  Der Einsatz von digitalen Assistenzsystemen ist zur Optimierung von Verfahrensabläufen einschließlich der Vorgabe einzelner Arbeitsschritte an Beschäftigten zulässig. Die hierdurch gewonnenen Daten dürfen aber wiederum nicht zur Leistungs- bzw. Verhaltenskontrolle genutzt werden.

- *Sprachgebrauchs- und Stimmungsanalyseverfahren*
  Sprachgebrauchs- und Stimmungsanalyseverfahren dürfen nur sporadisch und nicht dauerhaft eingesetzt werden. Insbesondere legitimieren es sich ständig ändernde Kundenanforderungen nicht, die Mitarbeiter in Call-Centern kontinuierlich derartigen Verfahren auszusetzen.

- *Auswertung innerbetrieblicher sozialer Netzwerke*
  Die pauschale Auswertung innerbetrieblicher sozialer Netzwerke ohne eine an konkreten Arbeitsaufgaben und Projekten orientierte Zwecksetzung ist unzulässig. Insbesondere ist es dem Arbeitgeber verwehrt, die innerbetriebliche Kommunikation konsequent darauf hin zu analysieren, in welchen sozialen und privaten Beziehungen die Mitarbeiter zueinander stehen.

- *Fitnessdaten*
  Die Nutzung von Gesundheitsdaten im engeren Sinne ist (außerhalb der hier nicht behandelten traditionellen Fallgruppen wie die Entgeltfortzahlung im Krankheitsfall und die krankheitsbedingte Kündigung) regelmäßig nur auf der Grundlage einer ausdrücklichen Einwilligung zulässig. Auch für allgemeine Fitnessdaten kommt letztlich nur der Erlaubnistatbestand der Einwilligung in Betracht, weil die entsprechenden Daten im Allgemeinen weder für die Begründung noch für die Durchführung oder die Beendigung des Beschäftigungsverhältnisses erforderlich sind.

- *Durchleuchtung der Persönlichkeit mittels Sprachanalyseverfahren*
  Eine umfassende Ermittlung der Persönlichkeitsstruktur durch Sprachanalyseverfahren muss als unzulässig angesehen werden. Die hohe Eingriffstiefe einer derartigen Durchleuchtung der eigenen Persönlichkeit spricht dagegen, in Bewerbungssituationen bzw. innerhalb von Arbeitsverhältnissen von einer freien Entscheidung des Betroffenen auszugehen.

  Der Arbeitnehmer hat nach dem BDSG beim unzulässigen Umgang mit seinen personenbezogenen Daten eine Reihe von Rechten (u. a. Löschungsanspruch und Anspruch auf Ersatz materieller Schäden), die praktisch aber nur eine untergeordnete Rolle spielen. Effektivere Rechte bzw. Rechtsfolgen auf der einzelvertraglichen Ebene, nämlich ein Anspruch auf Ersatz des immateriellen Schadens bzw. ein Beweisverwertungsverbot, finden sich außerhalb des Datenschutzrechts (aufgrund ungeschriebener allgemeiner bürgerlichrechtlicher Grundsätze) oder sind in der Rechtsprechung nur aufgrund einer allgemeinen und daher nicht vollständig prognostizierbaren Interessenabwägung anerkannt.

Die größte Effektivität entfaltet der präventive Schutz durch das Mitbestimmungsrecht des Betriebsrats gemäß § 87 Abs. 1 Nr. 6 BetrVG bei technischen Einrichtungen, die zu Überwachung von Leistung und Verhalten der Arbeitnehmer bestimmt sind. Die Rechtsprechung hat diesen Beteiligungstatbestand auf die automatisierte Auswertung von personenbezogenen Daten von Beschäftigten ausgedehnt. Wieweit das Mitbestimmungsrecht im Hinblick auf Betriebsdaten reicht, die mit Beschäftigtendaten lediglich verknüpft werden können, ist bislang allerdings nicht völlig geklärt.

5.2.3 Legislativer Fortentwicklungsbedarf

Soweit es um konkrete Regelungsvorschläge geht, ist zunächst als Ausgangspunkt festzuhalten, dass die neue Europäische Datenschutz-Grundverordnung (DS-GVO) eine Öffnung für „spezifischere Vorschriften“ auf der mitgliedstaatlichen Ebene enthält (Art. 88 DS-GVO). Bei der Schaffung solcher Vorschriften steht den Mitgliedstaaten eine Konkretisierungskompetenz zu, wobei sie aber auf der einen Seite das Schutzniveau der DS-GVO nicht unterbieten und auf der anderen Seite die Datenerhebung und den freien Datenverkehr nicht in einem Maße beeinträchtigen dürfen, die das Schutzniveau der DS-GVO erheblich (unangemessen) überschreitet.

Im Einzelnen empfiehlt sich die Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes, das sich weniger an einzelnen technologischen Entwicklungen orientiert, sondern vornehmlich auf die Festschreibung bestimmter Grundsätze hinausläuft. Hierzu sollten gehören:

- 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 Persönlichkeit).

Für den Bereich des kollektiven Arbeitsrechts empfiehlt sich eine Klarstellung bzw. Regelung in § 87 Abs. 1 Nr. 6 BetrVG, dass der Umgang mit personenbezogenen bzw. personenbeziehbaren Daten von Beschäftigten der Mitbestimmung des Betriebsrats unterliegt.

Erstellt im Auftrag des Bundesministeriums für Arbeit und Soziales.

Die Durchführung der Untersuchungen sowie die Schlussfolgerungen aus den Untersuchungen sind von den Auftragnehmern in eigener wissenschaftliche Verantwortung vorgenommen worden. Das Bundesministerium für Arbeit und Soziales übernimmt insbesondere keine Gewähr für die Richtigkeit, Genauigkeit und Vollständigkeit der Untersuchungen.