Daten- und Persönlichkeitsschutz im Arbeitsverhältnis

Praxishandbuch zum Arbeitnehmerdatenschutz

Bearbeitet von
Herausgegeben von Prof. Dr. Stephan Weth, Prof. Dr. Maximilian Herberger, Dr. Michael Wächter, Unternehmensjurist, und Prof. Dr. Christoph Sorge, Bearbeitet von Dr. Ulrich Baumgartner, Rechtsanwalt, Thomas Breyer, Rechtsanwalt, Dr. Dominic Broy, Dipl.-Jur., Assessor, Dr. Philipp Byers, Rechtsanwalt, Prof. Franz Josef Düwell, Vorsitzender Richter am BAG a.D., Dr. Jan Fritz Geiger, Rechtsanwalt, Ines M. Hassemer, Rechtsanwältin, Dennis Heinson, LL.M. (UCLA), Attorney at Law, Dr. Stefan Kramer, Rechtsanwalt, Dr. Sebastian Overkamp, Rechtsanwalt, Yvonne Overkamp, Richterin, Dr. Bernd Schmidt, LL.M., Rechtsanwalt, Dr. Hendrik Schöttle, Rechtsanwalt, Katharina Sicking, Dipl.-Jur., Assessorin, und Christian Willert, Rechtsanwalt

2. Auflage 2019. Buch. XXX, 769 S. Hardcover (In Leinen)
ISBN 978 3 406 71186 2
Format (B x L): 16,0 x 24,0 cm

zubeziehen, die als **Ware** verwertet und vermarktet werden. Denn dadurch kann die Autonomie des Einzelnen reduziert werden. Dies deshalb, weil neben dem Verhalten eines Arbeitnehmers und seinen Arbeitsergebnissen auch **Aspekte seiner Persönlichkeit** miterfasst werden, die als Wissen in Maschinen bzw. in IT-Systeme übertragen werden. Hierbei ist vom Verantwortlichen eine entsprechende **Data Responsibility** wahrzunehmen. Denn es stellt sich die Frage des **Profiling.**[32] Zielsetzung einer solchen Vorgehensweise ist dabei eine intensive Datennutzung, um bessere Entscheidungen treffen zu können und die Arbeitsorganisation im Unternehmen insgesamt in eine **lernende Organisation** umzugestalten. Dadurch soll der Prozentsatz der erfassbaren Daten (Searchable Data) erhöht werden.

Die systemischen Risiken für den Datenschutz liegen hierbei weniger in der Technologienutzung per se als in der Festlegung von **Zweckbestimmungen** (Purposes) und Zweckbindungen der Daten. Denn das Arbeitsverhältnis wird zur Plattform für Business. Die Datennutzung wird damit vertikal und tief. Insofern wirkt **Technologieeinsatz** für den Einzelnen nur vordergründig entlastend, weil dieser durch eine Erweiterung der Aufgaben des Einzelnen und durch eine höhere **Arbeitslast** (Workload) begleitet wird. Die Unternehmens-Performance wird durch die Erhöhung der Performance des Einzelnen durch **Arbeitsvernetzung** und -verdichtung erhöht. Damit ergeben sich Effizienzsteigerungen im Verhältnis Mensch-Maschine und durch Vernetzung von Arbeitsschritten im Rahmen von Unternehmensabläufen und -prozessen. 27

Damit wird die Arbeit auch zu hundert Prozent messbar. Das Arbeitsverhältnis nähert sich einem **Lizenzmodell** an.[33] Der Arbeitnehmer erledigt damit nur diejenigen Handgriffe, zu denen er im Detail befugt ist. In Matrix-Organisationen ergeben sich solche **Meta-Steuerungsprozesse,** die für die Durchführung einer Tätigkeit einen hohen Aufwand für die Beantragung der Umsetzung jeder einzelnen Tätigkeit erfordern. Menschen werden wie Maschinen mit **festgelegten Vorgehensweisen** eingesetzt. Dies ergibt für den einzelnen einen zusätzlichen Druck durch eine enge Prozess- und Finanzsteuerung, die sich allein an Finanzfreigaben des Unternehmens und nicht an geschäftlichen Erfordernissen orientiert. 28

Diese Veränderung der **Steuerung von Arbeitsverhältnissen** führt auch dazu, dass von Arbeitnehmern erwartet wird, dass sie ihre eigenen Arbeitsmittel (Bring Your Own Device) und auch ihre Persönlichkeit (Personal Brand) in das Unternehmen einbringen sollen. Dadurch sollen Defizite des Unternehmens und seiner **Leistungsreduzierung** gegenüber Kunden ausgeglichen werden. Das verändert das Selbstverständnis der Abgrenzung der **Risikosphären** von Arbeitgeber und Arbeitnehmer. Die Subjektivität der Privatsphäre des Einzelnen steht in diesem Kontext einer **Erwartungshaltung des Unternehmens** gegenüber, die zu einer Auflösung der Privatsphäre führt, um für das Unternehmen neue Impulse zu gewinnen, die im Rahmen starrer Hierarchien nicht möglich sind. Die Demokratisierung der Arbeitsverhältnisse und das **Driften der Organisationsstrukturen** führen dazu, dass Grenzziehungen für den Arbeitnehmer zwischen betriebsöffentlich und privat immer schwieriger werden. 29

Unternehmen messen heute zunehmend den Wert eines Mitarbeiters am Umfang seiner Zustimmung für das Unternehmen und seiner Partizipation an den Tools und Medien des Unternehmens. Es geht um **Engagement,** Skills und Performance, die nach den Vorgaben des Unternehmens gemessen werden. Und es geht hier auch um ein **Employee Scoring,** welches für jeden einzelnen Mitarbeiter sein **soziales Ranking** im Unternehmen bestimmt. Und hierzu werden zunehmend auch Informationen aus dem Internet herangezogen. Die IT-Systeme im Unternehmen messen, in welchem Umfang sich ein Arbeitnehmer an internen Diskussionen beteiligt und wie häufig er Aussagen der Geschäftsleitung **liked.** Unternehmenserfolg wird heute nicht nur auf Unternehmensebene 30

[32] Paal/Pauly/*Ernst* DSGVO Art. 4 Rn. 36 ff.
[33] *Wächter,* Datenschutz Rn. 168, 199.

betrachtet, sondern auch **personalisiert** bis auf die Ebene des einzelnen Mitarbeiters und seines persönlichen Beitrags zur Legitimation von Entscheidungen der Unternehmensleitung. Auch bei einer zunehmenden Betrachtung von Aktivitäten der Arbeitnehmer ist der **Schutzstandard der DSGVO** einzuhalten

31 Es ist darauf zu achten, dass für Zwecke des Beschäftigungsverhältnisses erhobene Daten – nicht im Rahmen einer **Zweckänderung** – nach Art. 7 IV DSGVO anderen nicht kompatiblen Zwecken zugeführt und weiterverarbeitet werden.[34] Dieser Punkt ist deshalb so wichtig, weil die geschäftliche Aktivitäten-Erfassung im Arbeitsverhältnis unter Nutzung von **Business Analytics** technisch zu weitgehenden Verwendungsmöglichkeiten und zum intensiven Einsatz von Informationen zur aktiven Geschäftssteuerung genutzt werden kann. Dies sind neuartige **Wertschöpfungsquellen,** die einen wirtschaftlichen Wert per se darstellen. Beispiele sind integrierte Auswertungen unter Nutzung von Echtzeitdaten sowie die Portionierung von Daten für unterschiedliche Entscheidungserfordernisse und wirtschaftliche Zwecke. Der neue Weg ist hierbei, mit dem **Internet of People,** nicht nur Geschäfte oder Dinge, sondern auch Menschen durch Informationen zu steuern.

32 Angesichts dieses Befunds geht es im Datenschutz zunehmend um die Handhabung der Verknüpfung und **Verkettung von Daten.** Bei der Frage der Rechtmäßigkeit der Datenerhebung ist hierbei zu beachten, dass die strengen Maßstäbe der Datenverarbeitung nach § 26 I BDSG für **Zwecke des Beschäftigungsverhältnisses** nach § 26 VII BDSG auch dann anzuwenden sind, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, **ohne** dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden. Dabei ist die Vorschrift des § 26 VII BDSG so zu verstehen, dass sie auch zur Anwendung kommt, **wenn § 1 I 2 BDSG nicht erfüllt ist.**[35] Der Umfang der Möglichkeiten der Datenerhebung, die dann zu einer rechtmäßigen Datenverarbeitung führt, ist insofern erheblich eingeschränkt. Dies ist bei der Handhabung von Datenkonzepten in Unternehmen in besonderer Weise zu berücksichtigen. Reduziert sich der **Umfang der rechtmäßigen Datenerhebung** (zB beim Fragerecht des Arbeitgebers), so reduziert sich auch der Umfang der Möglichkeiten der beschäftigtenbezogenen Datenverarbeitung insgesamt.

33 Dieser Punkt der eingeschränkten Datenerhebung ist auch in besonderer Weise bei der **Aktivitäten-Erfassung von Mitarbeitern** zu berücksichtigen. Eine Einschränkung der Erhebung von Daten ist im Besonderen dann zu beachten, wenn Daten in der Unternehmensorganisation **visibel** sind. Gerade bei global integrierten Unternehmen erfordert die Implementierung **weltweiter Systemplattformen** für die Beschäftigtendaten eine enge Zweckbindung, die sich am Zweck der Datenerfassung orientiert. Kritisch wird dies, wenn Geschäftsdaten (Business Data) und transaktionale Daten (Transactional Data), aber auch Arbeitsergebnisse (Work Results) sowie Daten über Mitarbeiteraktivitäten **(Behavior)** gemeinsam erfasst werden. Es ist hierbei nicht ausreichend, den **Zugriff von Personen** zu beschränken, die im Rahmen ihrer Tätigkeit Kenntnis davon haben müssen. Die Aktivitäten-Erfassung und die Nutzung des Internet of People zur **Verhaltensteuerung** von Menschen ist eine sensible Thematik. Insofern sollte der Zugriff bzw. die Speicherung von Beschäftigtendaten auf das erforderliche Maß beschränkt werden.

c) Application Sharing und Networking bei Arbeiten 4.0

34 Die Idee, Daten zu teilen, um vom Wissen und der Erfahrung anderer zu profitieren, ist in **arbeitsteiligen Unternehmen** ein wesentliches Wertschöpfungspotential. Allerdings sind im Arbeitnehmerdatenschutz Application Sharing und Networking auch unter dem

[34] Gola/*Schulz* DSGVO Art. 6 Rn. 177 ff.
[35] *Schantz/Wolff,* Neues DatenschutzR, Rn. 1344.

Aspekt zu betrachten, ob dadurch Informationen über die Mitarbeiter, die diese Daten generieren, wiederum Informationen gesammelt werden. Dies können sowohl **Metadaten** über die Intensität ihrer Kommunikation sein als auch Bewertungen ihrer Beiträge durch andere. Eine indirekte Beeinflussung der – regelmäßig als freiwillig bezeichneten – Beiträge ist die Messung der Anzahl der Aktivitäten durch einen **Social Score,** der ein Ranking der Mitarbeiter beinhaltet.

Die andere Seite dieser Betrachtung ist es, dass es beim vernetzten Arbeiten 4.0 zu den 35
arbeitsvertraglichen Verpflichtungen gehört, Arbeitsergebnisse und auch den Stand von Bearbeitungen in eine **Datenbank** einzugeben. Dadurch wird es für Unternehmen möglich, komplexe geschäftliche Vorgänge zu handhaben und Erfahrungswerte im Umgang mit fachlichen Fragestellungen zu verwerten. Die Grenze zwischen der arbeitsrechtlichen Verpflichtung und der **Sozialsphäre** im Arbeitsverhältnis gegenüber berechtigten Privatsphäre-Anliegen von Mitarbeitern wird danach fließend.

Für **People Analytics** nutzbar ist auch ein **soziales Intranet,** über das die Zusam- 36
menarbeit im Unternehmen koordiniert und Kommunikation sowie Wissenstransfer gefördert werden. Zudem kann anhand der Metadaten untersucht werden, wie stark Unternehmensbereiche miteinander vernetzt sind, wie hoch der **Wissenstransfer** tatsächlich ist (zB durch Dateiuploads), wie die Stimmung im Unternehmen ist und wer die **Meinungsmacher** (Influencer) oder Experten im Unternehmen sind. Bei der Einführung von People Analytics im Zusammenhang mit dem sozialen Intranet setzen Unternehmen auf flächendeckende Information und **Transparenz der Daten.** Dazu sind Regelungen zur **Visibilität der Daten** erforderlich. Jeder User, der Zugriff hat, sollte alle eigenen Daten auch löschen können. Auch sollte jeder User entscheiden können, welche Informationen er teilen möchte. Das Management sollte für die weitere Nutzung nur **aggregierte Daten** verwenden.

Zielsetzung muss es bei der heutigen **Standardisierung von Arbeitsprozessen** in In- 37
dustrie 4.0 und im Besonderen beim vernetzten Arbeiten 4.0 sein, bei einer Sicherstellung der rechtlichen Zulässigkeit der Verarbeitung personenbezogener Daten auch die Individualität und persönliche Entfaltung der Arbeitnehmer nach **§ 75 BetrVG** zuzulassen. Menschen sind auf Kooperation angelegt. Ebenso Unternehmensorganisationen. Dies betrifft den positiven Aspekt. Die Nutzung arbeitsteiliger IT-Systeme betrifft aber ebenso den klassischen Überwachungsdruck durch den Arbeitgeber bei der Erbringung der Arbeitsleistung. Und bei neuen Formen **arbeitsteiliger Einzelvorgänge** mit unterschiedlichen Bearbeitungsaspekten erfolgt zunehmend auch eine **soziale Kontrolle** durch direkte und indirekte Vorgesetzte (Personal- und Fachvorgesetzte) und Kollegen. Dem muss entgegengewirkt werden.

So kann es sein, dass an einem einzigen Personalvorgang bei einem **Country-to-** 38
Country-Transfer eines Mitarbeiters einer deutschen Konzerngesellschaft in eine andere europäische Konzerngesellschaft mit Headcountfreigaben und unterschiedlichen Management-Approvals eine **Vielzahl von Mitarbeitern** arbeiten, die bei unterschiedlichen Interessenlagen zu diesem Vorgang und auch verschiedenen Berichtslinien den Vorgang mit unterschiedlichen Zielsetzungen eskalieren, ohne dass ein Unternehmensbereich – Personalbereich, Managementlinie oder Finanzbereich – eine **Entscheidungskompetenz** hat. Jeder verfolgt insofern bei einer Vernetzung nur seine eigenen Bereichsinteressen. Best Practice könnte sein, für solche Fragestellungen eine Person als **Focal Point** zu legitimieren, die sowohl zentraler Ansprechpartner als auch Letztentscheider ist.

Ein anderes Beispiel ist, wenn ein deutscher Mitarbeiter eine **internationale Aufga-** 39
benstellung im europäischen oder internationalen Konzernverbund ohne Veränderung seines Arbeitsvertrags mit der deutschen Konzerngesellschaft übernehmen soll. Dies bedeutet in einer solchen **Matrix-Organisation,** dass ein Mitarbeiter für einen anderen Unternehmensbereich oder für eine andere Landesgesellschaft so eingesetzt wird, dass der Personalvorgesetzte nur noch der **Card-Holder** (Personalakten-Verantwortlicher) ist. Die Zuweisung von Arbeit sowie die Kontrolle der Erledigung von Arbeit werden dann

durch beliebige Fachfunktionen ausgeübt, die an der jeweiligen arbeitsteiligen Aufgabenstellung beteiligt sind. Diese Aufteilung von Verantwortung und Herstellung einer **Transparenz** über einen Mitarbeiter, der von den unterschiedlichsten Funktionen bewertet wird, entspricht nicht mehr dem tradierten Wert auf Privatheit einer einfachen **Arbeitgeber-Arbeitnehmer-Beziehung,** zB eines Angestellten, der 30 Jahre dieselbe Aufgabe am selben Arbeitsort beim selben Arbeitgeber ausübt. Die Bewertung angemessener Privatheit im Arbeitsverhältnis ist heute komplizierter.

40 **Privatheit** als bürgerlicher Wert diente zunächst der Abgrenzung von der Allgemeinheit und hatte seinen Ausgangspunkt im Schutz vor übergeordneter Herrschaft. Dies trifft auf moderne Sachverhalte der Arbeitsorganisation wie dem **Application Sharing** nicht mehr zu. Damit haben sich die Schutzerfordernisse für Arbeitnehmer verändert. Gruppenbezogenes **Teilen von Informationen** wird deshalb häufig anders wahrgenommen. Dies auch deshalb, weil die Wahrung von Privatheit bei der Durchführung von Arbeit im internationalen Kontext unterschiedlich bewertet wird. So wird in manchen Kulturen das **Tracking von Mitarbeitern** als wertvollerer Wertbeitrag für den Unternehmenserfolg betrachtet als die Erledigung der Arbeit. Das deutsche Bild des eigenverantwortlichen Mitarbeiters steht dem internationalen Modell der **Manager-Worker-Beziehung** entgegen. Der Manager hat nach dem amerikanischen Konzept kein Fachwissen, entscheidet aber und legt Zielvorgaben und Prioritäten fest. Der Worker hat zwar die Fachkenntnis, er soll aber nur die Vorgaben des Managers ohne Abweichung ausführen.

41 Auf die beschriebene Weise werden nach Vorgaben des Managements Tools und Anwendungen in der jeweiligen Rolle genutzt. **Worker reporten,** Manager tracken. Dies verdeutlicht die intensive Nutzung von Application Sharing, die Nutzung von Knowledge Warehouses sowie von Response Datenbanken. Denn diese Erfassung und Nutzung von Informationen dient dem Aufbau von **Management-Systemen,** die nach der Analyse der Informationen im Rahmen unterschiedlicher Reports zur Festlegung der weiteren Vorgehensweise dienen. In der Regel werden Prioritäten dann so festgelegt, dass die Quartalszahlen kongruent zu den Zielvorgaben sind. Datenschutz steht in diesem Kontext mit betriebswirtschaftlichen Handlungsvorgaben in Konflikt.

42 Für den Einzelnen bedeutet dies, dass er viele Informationen teilen muss. Datenschutzrechtlich sollte beim Teilen von Informationen das Prinzip der **diligentia quam in suis** gelten. Dieses Prinzip beinhaltet die Anwendung der eigenüblichen Sorgfalt nach § 277 BGB, die man in seinen eigenen Angelegenheiten als **subjektiv-individuellen Maßstab** anwendet.[36] Auf die DSGVO bezogen bedeutet dies, dass ein solches Niveau an Datenschutz umgesetzt wird wie es ein Betroffener im Hinblick auf **den eigenen Schutz** an Privatsphäre in einer bestimmten Situation für sich selbst erwartet. Der Maßstab an Schutz für sich selbst wird so auch auf andere übertragen. Arbeitnehmerdatenschutz wird damit in den Kontext des gegenseitigen **Vertrauensschutzes** gesetzt.

43 Mitarbeiter erhalten heute aus **Data Warehouses** Informationen und stellen ihre Arbeitsergebnisse in Datenbanken ein. **File Sharing Tools** dienen dem Austausch von Dokumenten, Meinungen und Links. Daten- und Persönlichkeitsschutz für Arbeitnehmer muss einem solchen komplexen Feld der Zusammenarbeit und Wertschöpfung nicht nur vertikal in der Berichtslinie des Mitarbeiters nach oben (Report to Chain) und gegenüber den eigenen Mitarbeitern (People Managed) gewährleistet werden, sondern auch **horizontal gegenüber Kollegen** auf derselben Hierarchiebene (Same Manager). Hinzu kommt die arbeitsteilige Zusammenarbeit mit externen Partnern und Akteuren auf gemeinsamen Kommunikationsplattformen. Durch die Tätigkeiten und die Nutzung des Internet erfolgt hierbei eine **Globalisierung in Mikroprozessen,** dh durch einzelne E-Mails und Kommunikationsvorgänge, die eine nationale Begrenzung der rechtlichen Sichtweise erschweren und letztlich auch zu einer Unsicherheit des **Schutzstandards** für den einzelnen Arbeitnehmer führen.

[36] Jauernig/*Stadler* BGB, 16. Aufl. 2015, § 277 Rn. 3.

Technisch erfolgt diese Art der Erledigung von Aufgabenstellungen im Rahmen vereinfachter Geschäftsprozesse auf standardisierten **System-Plattformen,** welche den erhöhten Anforderungen an den Austausch von Informationen gerecht werden müssen. Arbeitnehmer greifen hierbei innerhalb der **Systemapplikationen** in ihrer prozessbezogenen Rolle auf Informationen zu. **Industrielle Wertschöpfung** im Arbeitsverhältnis wird transformiert in Werkzeuge, arbeitsorganisatorische Abläufe und vernetzte Organisationsstrukturen.[37] Dies führt zu **sozialer Interaktion** der Mitarbeiter unabhängig von ihrem Arbeitsort mit persönlichkeitsrechtlichen Implikationen. Durch entsprechende Zugriffskonzepte sind Informationen im Rahmen ihrer Zweckbestimmung zu schützen. Jede Zweckbestimmung mit Beschäftigtendaten muss hierbei dem Maßstab der Erforderlichkeit nach § 26 I BDSG genügen. Ferner erfordert dies eine lückenlose **Datengeheimnisverpflichtung** aller Mitarbeiter.[38] Nur so kann ein **Vertrauenstatbestand** der Zusammenarbeit geschaffen werden, bei welcher die Privatsphäre geschützt wird. 44

Bei der heute großen **Fragmentierung von Vorgängen und Geschäftsbereichen** in Unternehmen und den sich daraus ergebenden Abstimmungserfordernissen stellt sich die Frage, ob Nachfragen im Bereich der **Privatsphäre** des Einzelnen – als eine Überschreitung des arbeitgeberseitigen Fragerechts entsprechend § 134 BGB – als unwirksame Einwilligung zu betrachten sind oder ob solche Fragen als **geschäftsüblich** anzuerkennen sind. Die Privatautonomie, private Lebensverhältnisse frei zu gestalten, erfährt hier ihre Grenze. Tatsächliche Phänomene, die einem **Verbot** zuwiderlaufen, sind insofern jeweils aus dem durch Auslegung ermittelnden Sinn des spezifischen Regelungszusammenhangs zu ermitteln.[39] Die Einwilligung nach Art. 6 Ia DSGVO iVm Art. 7 DSGVO sowie die **Abwägungsformel** des § 26 II 1, 2 BDSG ergeben, dass eine Einwilligung bei Überschreitung des Fragerechts regelmäßig verboten ist. Allerdings ist jeweils eine **Schwelle der Rechtsanwendung** anzulegen, die Abgrenzungen zu sozial- und geschäftsüblichen Vorgehensweisen vornimmt. Die Kernfrage ist hierbei nach Art. 24 DSGVO, ob die Anerkennung von Vorgehensweisen Nachteile oder **Risiken für Arbeitnehmer** nach sich zieht. 45

Die Einwilligung erfolgt in beschriebenem Fall jedenfalls konkludent und wird trotz Nichteinhaltung von Formalien letztlich im Unternehmen **sozial wirksam** sein. Auch wenn eine solche Vorgehensweise einer Fragestellung an eine Gruppe von Mitarbeitern, die coram publico antworten muss, grundsätzlich auch nicht dem **Erforderlichkeitskriterium** der Datenerhebung nach § 26 I 1 BDSG entspricht. Das Arbeitsverhältnis wird zur **Medieninszenierung,** bei welcher von jedem Mitarbeiter sein **Commitment** für das Unternehmen eingeholt wird. Die Kollegen „sollen zusehen" und sich vergewissern, dass jeder Kollege „für das Unternehmen ist". 46

Das Gefühl, Belangloses zu sagen, sowie das Gefühl, nur etwas **unverbindliches Privates** situativ unternehmensöffentlich zu machen, bringt die Beteiligten dazu, von sich etwas preis zu geben. Allerdings ist bei den Inhalten von Fragen im Datenschutzrecht das **Prinzip der Sozialadäquanz** im Wortlaut des § 26 BDSG sowie in der Konzeption der DSGVO grundsätzlich nicht berücksichtigt. Insofern unterliegt im Grunde jede Frage einer Zulässigkeitsprüfung. Sind Mitarbeiter bereit, eine iSd § 26 BDSG nicht wirklich erforderliche Frage zu beantworten, erfordert eine Eingabe ins System insofern eine **Anonymität** der Daten. Die **Freiwilligkeit** unterliegt hier jedenfalls einem sozialen Gruppenzwang. Allerdings setzt die Art der Fragestellung eine transparente Beantwortung der Frage durch alle Teilnehmer voraus. 47

Anonymität und Freiwilligkeit wird in einer solchen Arbeitsrealität ersetzt durch Gruppengefühl und gegenseitige **soziale Anerkennung.**[40] Identität mit einer Gruppe bedeutet 48

[37] *Reichwald/Piller,* S. 96.
[38] *Wächter,* Datenschutz, Rn. 381 ff.
[39] *Musielak* JuS 2017, 949 ff. (951).
[40] *Reichwald/Piller,* S. 169.

damit, dass andere ausgeschlossen sind. Imitation, dh Nachahmung von Verhalten ist hierbei ein soziales Muster, sich in der Gruppe zu behaupten. Die **soziale Ordnung** erlaubt nur bedingt die Abgrenzung des Einzelnen als Individuum. Nach der DSGVO wird man fragen müssen, ob die Gesamtsituation für alle Beteiligten noch als **fair** anzusehen ist. In jedem Fall ist nach Art. 5 I e DSGVO die **Speicherdauer** – zB auf einen Monat – zu begrenzen und es sind **Datenspuren** zu beseitigen.

49 In diesen Zusammenhang gehört auch die **Nutzung von Groupware.** Der Einzelne soll sich damit für Anliegen und Fragen anderer verfügbar zeigen. Macht er beim „Spiel von Geben und Nehmen" von Informationen nicht mit, so hat dies für ihn regelmäßig zur Konsequenz, dass er mit der Zeit vom **Informationskreislauf** ausgeschlossen wird. Ist ein Mitarbeiter über eine Sametime-Anwendung oder ein Smartphone/Handy – im Rahmen der **betriebsüblichen Nutzung** im Betrieb – nicht erreichbar, so hat dies für ihn den Nachteil, dass er weniger häufig angesprochen und damit in die gemeinsame Kommunikation von Kollegen nicht mehr einbezogen wird. E-Mails und Telefonate nehmen durch ihren zeitlichen Aufwand in der Unternehmenskommunikation in Unternehmen ab und werden durch schnellere und einfachere Medien wie SMS (Short Message Service) ersetzt.

50 Die **sofortige Verfügbarkeit** und **schnelle Reaktion** des Angesprochenen ist dabei das Kriterium des Teilens von Informationen. Hierbei spielt es für den Beteiligten keine Rolle, ob er arbeitsvertraglich in gerechtfertigter Weise nicht verfügbar ist, weil er zB seine **tägliche Arbeitszeit** bereits abgeleistet hat. Er muss immer verfügbar sein. Denn ist ein Arbeitnehmer nicht erreichbar, so wird er der **Erwartungshaltung** von Kollegen nicht gerecht, die zB sofort eine Hilfestellung bzw. Aussage benötigen. Dies in besonderer Weise dann, wenn der Arbeitnehmer keine Vertretung für seine Aufgabenstellung hat.

51 Es kommt heute hinzu, dass sich bei Telefonkonferenzen Beteiligte während der Konferenz – unbemerkt für andere – mit Sametime-Tools abstimmen, wie sie sich gegenüber einem anderen oder einer Gruppe verhalten sollen. **Verdeckte Kommunikation** zur besseren Erreichung von Zielsetzungen spiegelt sich auch im E-Mail-Verkehr wider, indem den auf Kopie (Carbon Copy – cc.) genannten Personen, zusätzliche solche mit Blindkopie (Blind Carbon Copy – bcc.) hinzugefügt werden. Der ursprüngliche Sinn einer Blindkopie, den Kreis der E-Mail-Adressaten **vertraulich** zu behandeln, enthält heute eine neue Zielsetzung der Gruppenbildung und strategischen Kommunikation zum Nachteil des offiziellen Adressaten, der nicht weiß, wer Teil der Kommunikation ist **(Negatives Networking).** Im Hinblick auf das Persönlichkeitsrecht des Empfängers ist dies dann problematisch, wenn der Verfasser für den Empfänger vertrauliche Inhalte scheinbar ohne Kopie an Dritte übermittelt, allerdings bestimmte Personen, auch außerhalb des Unternehmens, auf Blindkopie setzt. Der Empfänger kann heute insofern nicht mehr vertrauen, dass eine an ihn gerichtete E-Mail ohne cc.) einen **bilateralen Briefcharakter** hat.

52 Zur Gewährleistung des Persönlichkeitsschutzes sollte deshalb eine Kommunikation im Unternehmen mit bcc.) untersagt werden. Best Practice könnte sein, für unternehmensrelevante Kommunikationen durch eine **Sekretariats-Kopie** eine transparente Aktenlage herzustellen.[41] Ein anderer Weg könnte sein, die Kommunikation durch E-Mails durch **Response-Datenbanken** zu ersetzen, in welchen sowohl die Dokumentation der Mitarbeiter als die Speicherung von Unternehmensdokumenten **zentralisiert** wird. Dies führt zu einem höheren Persönlichkeitsschutz, einer besseren Datensicherheit und einer besseren Handhabung des Datenschutzes im Hinblick auf Speicher- und Löschungserfordernisse.

53 Zu beachten ist bei dieser Themenstellung auch der **Schutz von Unternehmensdaten.** Haben Arbeitnehmer Zugriff auf Informationen, die für das Unternehmen schützenswert sind, zB auf Management- bzw. Organisationsstrukturen und **Unternehmens-**

[41] Koreng/Lachenmann DatenschutzR-FormHdB/*Bergt* S. 342 f.

prozesse, so ist eine nicht autorisierte Offenlegung zu vermeiden. Dies ungeachtet, ob es sich um ein Gespräch, einen Blog oder eine Aktivität in einem sozialen Netzwerk handelt. Insofern spielt hierbei auch der Gesichtspunkt eine Rolle, dass Arbeitnehmer darauf achten sollten, dass sie beim **Umgang mit Unternehmensinformationen** bei Nutzung von sozialen und beruflichen Netzwerken Plattformbetreibern nur soweit Rechte einräumen wie dies ihr Arbeitgeber zulässt, und die auch auf dem Übertragungszweck nach § 31 V UrhG entsprechen.[42] In der Regel sind die Eigentums- und Nutzungsrechte (einschließlich **Copyright**) des Unternehmens geschützt. Dazu gehören auch Materialien (Arbeitsergebnisse) sowie andere urheberrechtlich geschützte Werke.

Datenschutzrechtlich kritisch ist die **geteilte Nutzung** von Applikationen, wenn ein 54
Mitarbeiter eines Unternehmens auf die technische Infrastruktur eines Kunden, dh auf dessen **Produktions- bzw. Echtdaten** zugreifen muss. Eine Möglichkeit, Datenschutzrecht zu gewährleisten und sozial wirksam zu machen, sind Verpflichtungserklärungen der Mitarbeiter. Erforderlich ist bei besonderen Fallkonstellationen auch das Mittel der **Arbeitnehmerüberlassung** zum datenschutzgemäßen Mitarbeitereinsatz. Dies betrifft zB den Einsatz von Beratern eines Softwareunternehmens bei Kunden, um **Vorgaben des § 203 StGB** zur Einhaltung von Datengeheimnissen nachzukommen. So unterliegt zB ein Unternehmen, welches als Wirtschaftsprüfungsgesellschaft Daten zur Rechnungslegung und Bilanzierung verarbeitet, der Vorschrift des § 203 I Nr. 3 StGB, welche die Verletzung von Privatgeheimnissen unter Strafe stellt. Die Strafvorschrift schützt in diesem Zusammenhang neben der **Geheimsphäre** des Einzelnen auch das Allgemeininteresse an der Verschwiegenheit.[43]

d) Cognitive Computing und Nutzung von People Analytics

Es ist heute ein wesentlicher Faktor, eine Wertschöpfung aus der Vermessung von Men- 55
schen zu erzielen. Im Rahmen eines **Human Factors Engineering** wird erfasst, wie Menschen sich verhalten, sich bewegen und welche Vorlieben sie haben. Aus dieser Erhebung physischer und psychischer Eigenschaften werden Schlussfolgerungen für die Entwicklung von Produkten für Konsumenten und für die **Führung von Mitarbeitern** gezogen. Dies mit Blick auf die Zukunft. Das bedeutet für den Datenschutz, dass eine detaillierte **Folgenprognose** für die Wahl von Entscheidungsalternativen im Datenschutzrecht zu treffen ist. Gerade in einem Rechtsgebiet wie dem Arbeitnehmerdatenschutz ist die Einbeziehung individueller und kollektiver Folgen für Betroffene deshalb so wichtig, weil eine durchgeführte IT **Fakten schafft,** die regelmäßig nur teilweise oder nicht mehr korrigierbar sind.

Investitionen werden heute auf Basis neuer Geschäftsmodelle angesichts konkreter Ge- 56
schäftschancen getroffen. Zur Verbesserung der Profitmargen werden hierbei, soweit möglich, Tätigkeiten von Mitarbeitern durch **Repetitive Solutions** ersetzt, die zunehmend Technologielösungen sind. Innovationen sollen **Non-labor based Profit** ermöglichen. Damit werden Tätigkeiten von Mitarbeitern und der Einsatz von Technologie zur Schaffung einer optimierten Kostenstruktur immer enger verknüpft. Geschäftsprozesse werden **digitalisiert.** Mitarbeiter sollen nicht mehr primär durch ihre Arbeit einen Wertbeitrag leisten, sondern die Information über die Mitarbeiter sollen als **Asset** genutzt werden. People Analytics bezeichnet in diesem Zusammenhang die **Datenanalyse** von Arbeitnehmerdaten. Hierbei werden bestimmte persönliche Aspekte genutzt, um diese zu bewerten und wirtschaftlich **multifunktional** zu verwenden und zu verwerten.

Die Menge der über Mitarbeiter erfassten Informationen wird erhöht. Eine Metrik 57
überführt dann die Informationen über **Eigenschaften von Mitarbeitern** im Rahmen von Analyseverfahren in einen Zahlenwert, der einen automatisierten Vergleich von Ge-

[42] *Rehbinder/Peukert,* UrhR, Rn. 874.
[43] LPK-StGB/*Kindhäuser* StGB § 203 Rn. 1.

sichtspunkten sowie eine inhaltliche Bewertung ermöglicht. Datenschutzrechtlich ist ein solches **Profiling** nach Art. 4 Nr. 4 DSGVO ein Unterfall der automatisierten Einzelentscheidung nach Art. 22 DSGVO. Hierbei ist von Bedeutung, dass Art. 22 DSGVO die Nutzung von Profilen entsprechenden Beschränkungen unterwirft.[44] Wesentlich für den Arbeitnehmerdatenschutz ist es, **Transparenz** zu solchen Sachverhalten im Unternehmen herzustellen.

58 Informationspflichten nach Art. 13 II f DSGVO bzw. Art. 14 II g DSGVO sowie auch der **Auskunftsanspruch** von Betroffenen nach Art. 15 DSGVO dienen dazu, dass Betroffene die wesentlichen Umstände des Profiling erkennen und der **Profilbildung** nach Art. 21 I S. 1 DSGVO widersprechen können. Dies ist angesichts neuer Entwicklungen von Cognitive Computing und **People Analytics** von Bedeutung. Denn diese neuen Sachverhalte führen zu einer umfassenden Bildung von Persönlichkeitsprofilen und können beim einzelnen Arbeitnehmer einen erheblichen psychischen **Überwachungsdruck** auslösen.[45] Anders als bei einer Videoüberwachung erfolgt dies nicht durch optische Erfassung, sondern durch die Erfassung von **Charakterzügen** eines Menschen, deren Vorhersage für den Einzelnen dessen **personelle Autonomie** einschränkt. Es ergibt sich für ihn ein Druck bzw. Rechtfertigungszwang, mit seinen künftigen Handlungen negativen Annahmen entgegenzuwirken, was einen erheblichen Anpassungsdruck für den Einzelnen erzeugen kann.

59 Solche Datenanalysen als Gegenstand der Personalführung verändern die traditionelle Personalarbeit in einem Unternehmen radikal. Analog dem **Internet of Things** werden bei einem **Internet of People** entsprechende Pools von Mitarbeitern verknüpft. Das Arbeitsverhältnis wird dabei durch den **Zugang zur Arbeit** definiert. Statt der Schaffung einer Dauerbeschäftigung geht es um die Schaffung von Räumen der Zusammenarbeit (Coworking Spaces), für welche entsprechende **Plattformen** geschaffen werden (Collaboration Platforms). Die neuen Formen der Arbeit entfernen sich damit zunehmend von den klassischen Formen der Arbeitsorganisation in Unternehmen. Damit geht es beim Arbeiten um die Organisation von **veränderbaren Teams** (Agile Teams). Dazu werden immer wieder neue Formen der Zusammenarbeit gebildet. **Crowdsourcing-Aufgaben** ergeben sich für abgrenzbare Aufgabenstellungen. Komplexere Themen müssen anders organisiert werden. Hierzu gehören in der Industrie 4.0 auch neue Formen der Zusammenarbeit von **Mensch und Maschine** (Man-Machine-Partnership).

60 In Unternehmen werden **Assets** verarbeitet. Das können Lösungsvorschläge von Mitarbeitern oder auch Outputs von Maschinen sein. Insofern ist bei der Analyse und Bewertung solcher Arbeitsergebnisse danach zu unterscheiden, ob Vorgänge des Unternehmens oder die **Handlung von Personen** analysiert und bewertet werden. Werden Daten für Vorgänge der Personaladministration oder der Personalführung genutzt und erfolgt Personalführung durch Analyse-Verfahren, spricht man von **HR Analytics** oder Workforce Analytics. Hierbei geht es um **Mixed Data,** weil die Analyse von Daten aus dem Personalwesen in Verbindung mit anderen Unternehmensdaten erfolgt. Diese Zielsetzung der Integration von IT-Systemen und Daten in Unternehmen ist datenschutzrechtlich mit **Trennungs-** und **Visibilitäts-Konzepten** für Daten zu begleiten.

61 **People Analytics** soll dazu dienen, künftig ohne das Erfordernis einer Personalabteilung individuelle und kollektive Personalentscheidungen durch **Systemanalyse** zu treffen. Damit sollen Personalentwicklung und Gehaltserhöhung nur noch **granular** für jeden einzelnen Mitarbeiter erfolgen, bei dem das Unternehmen dafür eine Notwendigkeit sieht. Gehaltserhöhungen sollen danach zB nur noch diejenigen Mitarbeiter erhalten, die das Unternehmen verlassen wollen und dem das Unternehmen als **Retention Maßnahme** entgegensteuern möchte. Der früher als negativ bewertete **Abkehrwillen** eines Mitarbeiters vom Unternehmen wird in der heutigen agilen Kultur zum strategischen Vorteil

[44] Gola/*Schulz* DSGVO Art. 22 Rn. 3.
[45] *Schantz/Wolff,* Neues DatenschutzR, Rn. 727 ff., 730 ff. (732).