A. Einleitung

§ 1 Überblick

Die Menschheit ist auf dem Weg zur digitalen Evolution. Die Technisierung und Digitalisierung des Alltags schreiten unaufhörlich voran – und dies mit einer rasanten Geschwindigkeit. In den letzten Jahrzehnten wurde der Fortschritt durch die erhöhte Rechenkapazität und den nahezu unbegrenzten Speicherplatz nochmals exponentiell beschleunigt. Big Data, Machine Learning und Künstliche Intelligenz[1] sind Begriffe, die inzwischen jedermann bekannt und nahezu täglich Gegenstand der medialen Berichterstattung im technischen Bereich sind.[2] Mit der Zunahme von Daten und deren Verarbeitung hat auch der Schutz dieser Daten, vor allem der personenbezogenen Daten, eine ganz andere Bedeutung erlangt.[3] Die Gesellschaft muss vor den Risiken des digitalen Umfelds geschützt werden, sodass der Einzelne nicht zu einem bloßen Datenobjekt degradiert[4] und die Privatsphäre ein Relikt aus alten Zeiten wird.

Auch vor der Arbeitswelt macht der digitale Fortschritt keinen Halt. Vielmehr ist diese die „zentrale Schnittstelle der Veränderung"[5]. Jeder Unternehmer[6] strebt dem Ziel der Gewinnmaximierung nach. Dieses Ziel kann auf verschiedenste Wege erreicht werden. Einer davon ist die Kostensenkung durch Rationalisierung von Arbeitsprozessen, also der Minimierung des erforderlichen Arbeits- und Kostenaufwandes durch effizientere Ausgestaltung von Arbeitsprozessen. In diesem Zusammenhang werden sog. *Business-Intelligence*-Systeme (BI-Systeme) relevant.[7] Der Begriff der *Business Intelligence* selbst ist schon alt und wurde wohl das erste Mal in

1 Kurz: KI, englisch: Artificial Intelligence (AI).
2 Siehe beispielsweise das größte technische Newsportal Deutschlands: www.heise.de.
3 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 37 Rn. 5.
4 So bereits das Bundesverfassungsgericht im Jahr 1983, vgl. BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 – Volkszählungsurteil.
5 *BMAS*, Grünbuch Arbeiten 4.0, S. 6.
6 Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt eine adäquate weibliche oder diverse Form gleichberechtigt ein.
7 *Grothe/Gentsch*, Business intelligence, S. 69.

der „*Cyclopaedia of Commercial and Business Anectotes*“ aus dem Jahre 1868 verwendet: Hier wird beschrieben, wie ein Bankier Informationen nutzt, um Profit daraus zu schlagen, indem er diese Informationen als Erster besitzt.[8] Im Kontext der Informationstechnik dürfte *Luhn* erstmals 1958[9] den Begriff verwendet haben[10] und zwar in dem Zusammenhang, wie Informationen automatisch auf die Zielperson abgestimmt und entsprechend im Unternehmen verteilt werden können, um die Entscheidungsfindung zu unterstützen und zu optimieren. So wird im Kern der Begriff auch heute noch verstanden.[11] BI-Systeme sind Systeme, die computerbasiert unternehmerische Entscheidungen unterstützen – mit Hilfe von Algorithmen. Kombiniert mit neueren Technologien, die diese Business Intelligence nutzen (z.B. *People Analytics*), können inzwischen automatisiert Entscheidungen gefällt werden.[12]

Solch automatisierte Entscheidungen sind selbstverständlich auch im HR-Management denkbar und werden vor allem außerhalb Europas bereits weitgehend angewandt.[13] So können beispielsweise ungeeignete Bewerber auf eine Stelle durch einen Computer aussortiert oder die gesamte Bewerberliste nach Eignung sortiert werden. Ein Beispiel wäre, dass diese mit einem Punktewert, einem sog. „Score“ versehen werden, damit der Verantwortliche[14] sofort einen Überblick über die Geeignetheit eines Kandidaten hat. In den Vereinigten Staaten und teilweise sogar in Großbritannien wenden bereits 70 % der Unternehmen solche Systeme an.[15] Manche Unternehmen gehen sogar so weit, dass sie die Bewerber überhaupt nicht mehr persönlich interviewen, sondern den Computer die Entscheidung

8 *Kirkland*, Cyclopaedia of Commercial and Business Anecdotes, S. 210.
9 *Luhn*, IBM Journal 1958, 314.
10 *Dorschel*, Praxishandbuch Big Data, S. 256.
11 *Gola*, Datenschutz am Arbeitsplatz, S. 12 Rn. 27 f.
12 WHWS/*Broy/Heinson*, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis, Rn. 1: „*Immer häufiger werden IT-Systeme auch über Beschäftigte entscheiden, ohne dass ein Mensch beteiligt ist.*“
13 Vgl. *Peck*, The Atlantic 2013 (Dezember 2013); *O'Neil*, Weapons of math destruction, S. 108: 60-70 % der Unternehmen wenden solche Technologien an, im Vergleich zu 30-40 % im Jahr 2014.
14 Es sind stets Personen männlichen und weiblichen Geschlechts gleichermaßen gemeint; zur besseren Leserlichkeit und ohne Diskriminierungsabsicht wird im Folgenden nur die männliche Form verwendet.
15 *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, <www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/BSt_DSGVOundADM_dt.pdf>, S. 7; so auch *O'Neil*, Weapons of math destruction, S. 108.

treffen lassen. Es findet also keinerlei menschliche Interaktion mehr statt.[16] Dieses Szenario ist jedoch nicht lediglich im Bewerbungsverfahren, sondern auch während eines intakten Arbeitsverhältnisses denkbar, wenn es darum geht, welche Arbeitnehmer auf Schulungen geschickt, befördert oder gar entlassen werden sollen. Für die Entscheidung des Computers können in den Entscheidungsalgorithmus unzählige Daten einfließen, die von der fachlichen Qualifikation des Arbeitnehmers bis hin zu Persönlichkeits- und Gesundheitsaspekten reichen können. Das gesamte HR-Management wird also immer datenlastiger bzw. datengetriebener (auch *evidenzbasiertes* Management genannt; die zugrundeliegenden Ansätze werden unter dem Stichwort *People Analytics* zusammengefasst).

Aufgrund immer leistungsfähigerer Computer und der Möglichkeit nahezu unbegrenzt Daten zu speichern, sind allumfassende „Auswertungen von Menschen" binnen Bruchteilen von Sekunden möglich. Bereits früh hat das Bundesverfassungsgericht daher festgestellt, dass es kein „belangloses Datum" (mehr) gibt.[17] Der Grundstein für das heutige Datenschutzrecht wurde gelegt. Seit dem 25.05.2018 gibt es nunmehr in Europa eine neue Regelung des Datenschutzes, die sog. Datenschutz-Grundverordnung[18]. Sie soll den heutigen Anforderungen, die durch die rasche technologische Entwicklung entstanden sind, gerecht werden.[19]

In Art. 22 DSGVO findet sich eine Regelung über automatisierte Entscheidungen im Einzelfall einschließlich Profiling. Es ist umstritten, ob es sich hierbei um ein Verbot mit Erlaubnisvorbehalt[20] oder lediglich um ein Betroffenenrecht handelt, welches dieser geltend machen muss, wenn er nicht Betroffener einer automatisierten Entscheidung sein will[21]. Ausnahmen sind nur im Rahmen der Ausnahmetatbestände von Art. 22 Abs. 2 DSGVO möglich. Das Profiling wird in Art. 4 Nr. 4 DSGVO defi-

16 Vgl. *Peck*, The Atlantic 2013 (Dezember 2013).

17 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 (44) – Volkszählungsurteil Rn. 158.

18 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU L 119/1.

19 Vgl. Erwägungsgrund 6 der DS-GVO.

20 *Eichler*, RDV 2017, 10 (11); *Taeger*, RDV 2017, 3; wohl auch *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 78 Rn. 61; *Sörup/Marquardt*, ArbRAktuell 2016, 103 (106); Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 29b; Sydow/*Helfrich*, Art. 22 DSGVO Rn. 39 f.

21 Dafür EuArbRK/*Franzen*, Art. 22 DSGVO Rn. 3 m.w.N.; zweifelnd an einem Verbot Plath/*Kamlah*, Art. 22 DSGVO Rn. 4.

niert als *jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogene Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.* Zumindest nach dem Wortlaut des Erwägungsgrunds 71 der Verordnung könnte man davon ausgehen, dass das Profiling auch eine automatisierte Entscheidung darstellt und daher unter das Verbot fällt. So würde das im Erwägungsgrund explizit aufgeführte Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen als modernes Tool im Personalmanagement jedenfalls erheblichen datenschutzrechtlichen Bedenken unterliegen.

Doch auch auf bereits eingesetzte Systeme, die wegen der etwas anderen Formulierung des § 6a BDSG a.F. aufgrund mangelnder automatisierter Entscheidung im Einzelfall zulässig waren, könnte ein weitergehendes Verbot durch Art. 22 DSGVO Auswirkungen dergestalt haben, dass diese nunmehr umgestaltet bzw. abgeschafft werden müssen. Aktuelle Personalbedarfsplanungssysteme basieren beispielsweise darauf, dass zukünftiger quantitativer, zeitlicher und örtlicher Personalbedarf automatisiert durch Algorithmen bestimmt wird.[22] Hierbei werden sog. *Data Mining*-Systeme eingesetzt, welche bislang unbekannte Zusammenhänge in Personaldaten entdecken sollen, wobei wohl häufig auf anonymisierte Daten zurückgegriffen werden kann.[23] *Data Mining*-Systeme sind Anwendungen, die bislang unbekannte und potenziell nützliche Muster in Daten erkennen können.[24] Eine Vielzahl der Daten sind im Unternehmen in aller Regel bereits vorhanden und in den Datenbanken der Personalmanagementsysteme[25] gespeichert. Diese müssen nur noch zusammengeführt bzw. verknüpft und mit den eingangs genannten BI-Systemen ausgewertet werden.

Nach einer repräsentativen Studie von LinkedIn und Bitkom Research sammeln bereits 78 % der befragten Unternehmen Daten der Beschäftig-

22 *Strohmeyer*, Informationssysteme im Personalmanagement, S. 95.
23 *Strohmeyer*, Informationssysteme im Personalmanagement, S. 165.
24 *Strohmeyer*, Informationssysteme im Personalmanagement, S. 157.
25 Ein Personalmanagementsystem ist ein System zur umfassenden Verwaltung von Personaldaten. Je nach Ausgestaltung des Systems kann ein solches System die Personalbedarfsplanung, Personaleinsatzplanung, Personalentwicklungsplanung, Personalkostenplanung sowie die Personalabrechnung und -verwaltung (Personalakte) in einem Softwarepaket bündeln und den erforderlichen Aufwand der HR-Manager deutlich reduzieren.

ten und analysieren diese IT-basiert. 36 % der Unternehmen planen die Nutzung von *Big Data* zur Optimierung der HR-Prozesse, während 9 % diese Technologie sogar schon einsetzen. Allerdings haben auch 52 % der Unternehmen noch generelle Datenschutz- und Sicherheitsbedenken und verzichten daher auf einen weitergehenden Einsatz.[26]

Bereits aus diesen Zahlen ist ersichtlich, dass die rechtliche Lage zum (Beschäftigten-)Datenschutz noch weitestgehend ungeklärt ist, weshalb Unternehmen – vor allem in Anbetracht der hohen Sanktionen nach dem neuen Datenschutzrecht, die nach Art. 83 Abs. 5 DSGVO auf bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresgesamtumsatzes festgesetzt werden können – schlichtweg darauf verzichten. Sollten mit der Anwendbarkeit der DSGVO nunmehr jegliche Analysen und Prognosen im HR-Management verboten sein, so wäre dies das Aus für das moderne Personalmanagement. Dies bedeutete enorme Wettbewerbsnachteile gegenüber Wettbewerbern außerhalb der Europäischen Union, die ihr Humankapital effektiver einsetzen können.

Da Entscheidungen immer häufiger datenbasiert gefällt werden, soll im Rahmen dieser Dissertation untersucht werden, auf Basis welcher Daten Entscheidungen im HRM nach neuem Datenschutzrecht wie gefällt werden dürfen, insbesondere inwieweit eine Automatisierung bzw. Computerunterstützung im Hinblick auf Personalentscheidungen zulässig ist.

§ 2 *Interessenskonflikt im Arbeitsverhältnis*

Bevor jedoch mit der rechtlichen Analyse dieser Technologien begonnen werden kann, sollen für das bessere Verständnis der Materie zunächst die Interessen der jeweiligen Parteien an der Nutzung bzw. dem Schutz der Daten dargestellt werden, um in Abwägungsfällen diese besser einordnen und bewerten zu können. Im Arbeitsverhältnis besteht grundsätzlich ein Interessenskonflikt: Der Arbeitgeber hat vor Beginn des Arbeitsverhältnisses kaum bis gar keine Informationen über den Arbeitnehmer und umgekehrt. Lediglich die von der jeweiligen Partei zur Verfügung gestellten Informationen können im Vorfeld ausgewertet werden, wobei auch hier moderne Plattformen und Tools helfen, weitere Informationen zu beschaffen. So nutzen Arbeitgeber inzwischen soziale Netzwerke, um mehr über die Bewerber herauszufinden, während sich Arbeitnehmer auf Arbeitge-

26 Vgl. *Bitkom Research GmbH/LinkedIn Deutschland, Österreich, Schweiz*, "Big Data" verändert das Personalwesen nachhaltig.

berbewertungsportalen wie *kununu*[27] informieren können. Hinzu kommt, dass beiden Seiten daran gelegen ist, nur positive Informationen über sich selbst Preis zu geben, während negative Aspekte möglichst unter den Tisch gekehrt werden sollen. Hierauf soll im Folgenden jedoch nochmals näher eingegangen werden.

I. Asymmetrische Informationsverteilung im Arbeitsverhältnis

Auf dem Arbeitsmarkt sowie im Arbeitsverhältnis besteht grundsätzlich ein Informationsgefälle zwischen Arbeitgeber und (potenziellem) Arbeitnehmer, welches zu einer sog. *Adverse Selection* bei Vertragsschluss bzw. zum Auftreten von *Moral Hazard* nach Vertragsschluss führen kann. Beides sind Begriffe aus der Verhaltensökonomik, einem Teilgebiet der Volkswirtschaftslehre.[28]

1. Prinzipal-Agenten-Theorie

Die Prinzipal-Agenten-Theorie versucht die Probleme, die durch das Informationsgefälle entstehen, zu beschreiben. Der Prinzipal ist dabei eine Person bzw. Organisation (hier: der Arbeitgeber) für die der Agent (hier: der Arbeitnehmer) eine Handlung durchführt. Der Agent hat Informationen, über die der Prinzipal nicht verfügt. Dieser versucht an diese Informationen zu kommen.[29] Diese ungleiche Informationsverteilung führt dazu, dass das optimale Gleichgewicht zwischen Arbeitsangebot und -nachfrage nicht erreicht wird und nur sog. „Second-best-Lösungen" erzielt werden.[30] Beispielsweise wird im Rahmen des Bewerbungsverfahrens ein Bewerber ausgewählt, der nicht die optimale Besetzung für die Stelle ist bzw. erhält der Arbeitnehmer während des Beschäftigungsverhältnisses zu viel Lohn für die verrichtete Arbeitsleistung. Hierbei weiß der Arbeitnehmer besser

27 *kununu* gehört zum beruflichen sozialen Netzwerk XING und ermöglicht es Mitarbeitern und Bewerbern ihre Arbeitgeber anonym zu bewerten, Angaben zum Betriebsklima, Gehalt, zu den Vorgesetzen etc. zu machen. Somit haben potenzielle Kandidaten für eine neue Stelle die Möglichkeit, von dritter Stelle etwas mehr über das Unternehmen im Vorfeld zu erfahren.

28 Vgl. *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 371 ff.

29 *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 371.

30 Vgl. *Hochhold/Rudolph*, Principal-Agent-Theorie, in: Schwaiger/Meyer, Theorien und Methoden der Betriebswirtschaft, S. 135.

als sein Arbeitgeber, wie sehr er sich bei seiner Arbeit anstrengt, welche Fähigkeiten er hat etc.[31] Der Arbeitgeber versucht, an diese Information zu gelangen, um den optimalen Arbeitnehmer auszuwählen bzw. den leistungsäquivalenten Lohn zu bezahlen. Dafür werden immer häufiger Tools eingesetzt, die das Internet (und somit auch soziale Netzwerke) nach Informationen über den Bewerber durchsuchen, um somit ein möglichst umfassendes Bild („Profil") vom Bewerber zu erhalten.

2. Adverse Selection

Ein Begriff aus der Prinzipal-Agenten-Theorie ist die sog. *Adverse Selection*. Diese tritt auf, wenn ein Agent vor Vertragsschluss mehr Information über seine eigene Situation hat als der Prinzipal und dies schlussendlich dazu führt, dass der Prinzipal keinen Vertrag mit dem Agenten abschließen möchte, da der Agent möglicherweise einen höheren Preis als angemessen verlangt.[32] Ohne die Möglichkeit, sich Informationen über den Agenten zu beschaffen, führt dies dazu, dass Arbeitgeber lediglich Lohnangebote abgeben in Höhe der durchschnittlich erwarteten Leistung der Arbeitnehmer; gute Arbeitnehmer sind zu diesem Preis nicht bereit zu arbeiten, weshalb sich nur noch Agenten mit unterdurchschnittlicher Leistung auf dem Markt befinden und der Markt im Worst-Case-Szenario zusammenbricht.[33] Um diese negative Auslese zu verhindern, gibt es verschiedene Möglichkeiten Informationsasymmetrie zu beseitigen. Für die potenziellen Arbeitnehmer besteht ein Anreiz durch *Signaling*, also dem Übermitteln von privaten Informationen mit dem Ziel, dem Arbeitgeber ihre Fähigkeiten zu vermitteln. Umgekehrt führt der Arbeitgeber ein *Screening* durch. Er versucht also möglichst viele Informationen über den Bewerber einzuholen bspw. durch Fragebögen, Tests, Vereinbarung einer Probezeit etc.[34]

In der modernen Arbeitswelt erstellen Arbeitnehmer daher Profile auf beruflichen sozialen Netzwerken, die dann entweder durch Head Hunter oder durch Personalverantwortliche bei den Unternehmen schnell gefunden werden können. So gibt es beispielsweise beim Netzwerk *LinkedIn*

31 *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 372.
32 *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 374.
33 *Hochhold/Rudolph*, Principal-Agent-Theorie, in: Schwaiger/Meyer, Theorien und Methoden der Betriebswirtschaft, S. 137.
34 Vgl. *Hochhold/Rudolph*, Principal-Agent-Theorie, in: Schwaiger/Meyer, Theorien und Methoden der Betriebswirtschaft, S. 138.

die Möglichkeit, Empfehlungen von bisherigen Arbeitskollegen und Vorgesetzten einzuholen und auf seine Seite zu setzen, um durch *Signaling* dem Arbeitgeber positive Informationen über sich selbst, die durch Dritte generiert wurden, zu vermitteln. Dies erfolgt mit dem Ziel, die *Adverse Selection* zu vermeiden und somit die gewünschten Stellen und Gehälter angeboten zu bekommen. Im Rahmen des *Screenings* werden diese Informationen durch die Arbeitgeber genutzt.[35]

3. Moral Hazard

Das Beschäftigungsverhältnis ist ein „klassisches Beispiel für Moral Hazard"[36]. *Moral Hazard* bedeutet „moralische Versuchung" und umschreibt das Problem, dass eine Person, deren Verhalten unzulänglich beobachtbar ist, dazu neigt, sich unehrlich oder auf andere Weise unerwünscht zu verhalten. Gerade bei Arbeitnehmern besteht hier die Versuchung, sich um die arbeitsvertraglichen Pflichten zu drücken.[37] Dieser Moral Hazard kann einerseits dadurch beseitigt werden, dass Arbeitgeber Anreize schaffen, mehr und/oder effizienter zu arbeiten wie beispielsweise durch eine Zahlung eines hohen Lohnes oder durch die Einführung einer variablen bzw. erfolgsabhängigen Vergütung. Andererseits kann der Arbeitgeber durch stärkere Überwachung (sog. *Monitoring*[38]) bei gleichem Lohnniveau dagegenwirken oder die verschiedenen Ansätze kombinieren.

Gerade das *Monitoring* durch Arbeitgeber wird mit der zunehmenden Digitalisierung der Arbeit einfacher: Elektronische Geräte erfassen automatisiert (Nutzungs-)Daten, die von Arbeitgebern ausgewertet werden, um festzustellen, welche Leistung der jeweilige Arbeitnehmer erbringt. Durch den Vergleich mit anderen Arbeitnehmern kann festgestellt werden, ob hier ein „Underperforming" vorliegt und somit auch der *Moral Hazard*, beispielsweise ausgelöst durch *Adverse Selection*, Niederschlag findet. Entgegenwirken können Arbeitgeber dem Problem im laufenden Beschäfti-

35 Die Nutzung von Daten in beruflich orientierten sozialen Netzwerken durch Arbeitgeber ist zulässig, da Arbeitnehmer diese Informationen ja gerade dort veröffentlichen, um von Arbeitgebern gefunden zu werden, vgl. hierzu auch *Göpfert/Dußmann*, NZA-Beilage 2016, 41 (43 f.).

36 *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 373.

37 *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 373.

38 *Hochhold/Rudolph*, Principal-Agent-Theorie, in: Schwaiger/Meyer, Theorien und Methoden der Betriebswirtschaft, S. 139; vgl. auch WHWS/*Geiger*, Teil A. VI. Bedrohung des Persönlichkeitsrechts des Arbeitnehmers, Rn. 16.

gungsverhältnis dadurch, dass sie an das *Monitoring* rechtliche oder tatsächliche Folgen knüpfen. Hier können erfolgsbezogene Boni, variable Vergütung bis hin zu Versetzungen und Kündigungen bei Unterschreitung gewisser Schwellenwerte als Beispiele genannt werden.

II. Die unterschiedlichen Interessen der Parteien

Es wurde bereits herausgearbeitet, dass die Parteien des Arbeitsvertrags das Interesse haben, gewisse Informationen zurückzuhalten und andere wiederum Preis zu geben. Worin das Informationsinteresse des Arbeitgebers und das Geheimhaltungsinteresse des Arbeitnehmers genau liegt und welchen Ursprung diese Interessen haben, soll im Folgenden nochmals detailliert dargestellt werden.

1. Das Informationsinteresse des Arbeitgebers

Das Informationsinteresse des Arbeitgebers ist vielseitig. Einerseits sind Arbeitgeber gezwungen, persönliche Daten zu erheben, um diese an die staatliche Verwaltung weiterzugeben (z.B. für die Erhebung der Lohnsteuer, Sozialversicherung etc.). Bereits 1985 wurde von *Peters* festgestellt, dass sich aus 113 Gesetzen und Verordnungen die Verpflichtung des Arbeitgebers ergibt, insgesamt 75 verschiedenen staatlichen Datenempfängern Arbeitnehmerdaten zukommen zu lassen.[39] Dieser Informationsverpflichtung möchten die Arbeitgeber möglichst kostengünstig nachkommen, indem sie IT-Systeme einsetzen.[40]

Andererseits hat der Arbeitgeber auch ein Interesse, seine Arbeitnehmer möglichst effizient, d.h. nach ihren Fähigkeiten, Kenntnissen sowie ihren (persönlichen) Stärken und Schwächen entsprechend, auf dem optimalen Arbeitsplatz einzusetzen und somit *Moral Hazard* zu vermeiden.[41] Aus Sicht des Arbeitgebers ist der Arbeitnehmer ein Produktionsfaktor, der optimal „verwendet" werden muss. Die Folge ist eine Schematisierung der Anforderungen an den einzelnen Arbeitnehmer, die mithilfe automa-

39 *Peters*, DSWR 1985, 186 (188).
40 *Walz*, Mitbestimmung 1986, 292 (294).
41 Zur Personaloptimierung als Teil des Rechts auf unternehmerische Freiheit, vgl. auch *Götz*, Big Data im Personalmanagement, S. 17.

tisierter Verarbeitung möglichst effizient erfolgen soll.[42] Durch die elektronische Datenverarbeitung sinken die Transaktionskosten des Arbeitgebers im Hinblick auf die Datengewinnung und -verarbeitung enorm, sodass die Begrenzung des Informationsinteresses durch Kosten praktisch weggefallen ist. Bestes Beispiel hierfür ist die Videoüberwachung von Beschäftigten: Der Arbeitgeber kann sehr einfach ohne Personalkosten mit einmaligem Aufwand seine Beschäftigten lückenlos aufzeichnen,[43] mit zunehmender Speicherkapazität und sinkenden Kosten quasi über deren gesamtes „Betriebsleben".

Das Informationspotential durch die Verwendung von IT-basierten Systemen lässt sich gut für Planungszwecke nutzen, damit die Arbeitsleistung, bestmöglich auf den Arbeitsprozess bezogen, bewertet und gesteuert sowie die Arbeitsleistungen verschiedener Arbeitnehmer miteinander verglichen werden können. Hierdurch objektiviert und rationalisiert sich die Personalentscheidung.[44]

2. Das Geheimhaltungsinteresse des Arbeitnehmers

Arbeitnehmer profitieren nicht lediglich von der automatisierten Verarbeitung, da die vom Arbeitgeber gesammelten Informationen sowohl für als auch gegen den Arbeitnehmer verwendet werden können (z.B. kann ein Belastungsprofil des Arbeitnehmers für die Zuweisung eines passenden Arbeitsplatzes genutzt werden, genauso aber auch für einen Selektionsmechanismus beim Stellenabbau[45]).

Der größte Profit des Arbeitnehmers von einem Personalinformationssystem liegt darin, dass die individuelle Situation besser berücksichtigt,[46] sowie mögliche noch unbekannte Störfaktoren (z.B. nicht eine funktionierende oder anders gelebte Hierarchie im Unternehmen[47]) durch Big Data-Auswertungen identifiziert und aus dem Weg geräumt werden können.

Arbeitnehmer haben also ein Interesse, gewisse Informationen über sich Preis zu geben, um die eigene Arbeitssituation zu verbessern. Nicht außer Acht gelassen werden darf allerdings, dass Beschäftigte ein ebenso großes

42 *Simitis*, in: FS Coing 70, S. 495 (500).
43 *Franzen*, ZfA 2012, 172 (174 f.).
44 *Simitis*, in: FS Coing 70, S. 495 (505 f.).
45 *Simitis*, in: FS Coing 70, S. 495 (507).
46 *Simitis*, in: FS Coing 70, S. 495 (506).
47 Siehe unten, **E. § 4.**

Interesse haben, möglichst wenige persönliche Informationen preiszugeben, um ihre Privatsphäre zu schützen.[48] Das Interesse der Arbeitnehmer liegt vornehmlich darin, *selbst* die Entscheidungsgewalt darüber zu haben, welche Informationen der Arbeitgeber erhält bzw. an ihn weitergegeben werden und für welche Zwecke er diese Informationen einsetzen darf.[49] Zudem besteht ein hohes Interesse daran, nicht lückenlos überwacht und dokumentiert zu werden,[50] um nicht jede einzelne Handlung im Arbeitsalltag ggf. rechtfertigen zu müssen.

3. Technikspezifische Risiken

Dieser Interessenskonflikt wird durch den Einsatz moderner IT-Technologie, bei welcher immer mehr Daten durch die Arbeitgeber gesammelt werden, verstärkt: Technologien wie Personalinformationssysteme führen zu einem deutlichen Informationsgefälle zwischen (internen) Arbeitnehmern und externen Bewerbern.[51] Der Arbeitgeber verfügt über deutlich mehr Informationen über die bereits Beschäftigten. Dies resultiert dann darin, dass dieser eher dazu neigt, interne Bewerber zu berücksichtigen als externe. Hierdurch lässt sich sowohl das Risiko der *Adverse Selection* als auch das des *Moral Hazard* verringern. Unternehmen werden daher zu einer Art „closed shops"[52], bei denen es insbesondere für externe Bewerber besonders schwierig ist, eine entsprechende Anstellung zu finden. Da Stellen jedoch vielfach nicht nur intern besetzt werden können bzw. auch „frischer Wind" ins Unternehmen gebracht werden soll, investieren Arbeitgeber in Technologien, die es ihnen ermöglichen, auch von externen Bewerbern möglichst viele Informationen zu bekommen (beispielsweise durch Recherche in sozialen Netzwerken, aber auch durch Eignungs- und Persönlichkeitstests im Rahmen der Einstellung bzw. Assessment Centern).

Weit bedenklicher und gravierender ist es jedoch, dass es durch den technischen Fortschritt möglich wurde, Arbeitnehmer quasi lückenlos zu überwachen, sei es per Videoüberwachung im Betrieb, Überwachung des betrieblichen PCs, GPS-Ortung von Fahrzeugen oder Mobiltelefonen,

48 *Franzen*, ZfA 2012, 172 (175).
49 *Schmitz*, Interessenausgleich im Beschäftigtendatenschutz, S. 32.
50 *Thüsing*, RDV 2009, 1.
51 *Simitis*, in: FS Coing 70, S. 495 (508).
52 *Däubler*, Gläserne Belegschaften, § 2 Rn. 33.

RFID-Ordnung innerhalb Gebäuden, bis hin zur Überwachung der Vitalfunktionen durch Wearables.[53] Die technischen Möglichkeiten von Arbeitgebern ihre Arbeitnehmer zu überwachen, steigen mit zunehmendem Technikfortschritt exponentiell und sind heute – zumindest aus technischer Hinsicht – nahezu grenzenlos.

Auf bestimmte Geräte wie beispielsweise Mobiltelefone, PCs oder Fahrzeuge sind die Arbeitnehmer angewiesen,[54] sodass sie keine Möglichkeit haben, einer etwaigen Überwachung zu entgehen. Da die meisten Arbeitstransaktionen mit Hilfe von entsprechenden Informations- bzw. Kommunikationssystemen digital abgebildet werden, besteht eine noch nie dagewesene Transparenz von Leistung- und Verhalten, denn jede Nutzung eines technischen Geräts hinterlässt personenbezogene Spuren (z.B. bei PCs beispielsweise Cookies, IP-Adressen etc.; bei Mobilgeräten zusätzlich noch die IMEI-Nummer[55]), die zu Verhaltens- und Leistungskontrollen verwendet werden können.[56] Dies führt dazu, dass die Arbeitgeber durch die Verknüpfung der Einzeldaten[57] genaue Persönlichkeitsprofile über ihre Arbeitnehmer erstellen können und dies oftmals – teilweise datenschutzwidrig – auch tun.[58]

Die Sammlung verschiedener Daten zum Zwecke der detaillierten Auswertung und dem Auffinden noch unbekannter Muster wird unter den Überbegriff *Big Data* gefasst.[59] Die seit dem 21. Jahrhundert vorhandene nahezu unbegrenzte Speicher- und Rechenkapazität ermöglicht es Arbeitgebern alle Daten zu erfassen und innerhalb kürzester Zeit auszuwerten – dies dank immer stärkerer Rechenkapazität zu erschwinglichen Preisen. Typische Analysemethoden in diesem Zusammenhang sind beispielsweise Online Analytical Processing (OLAP) sowie Data Mining.

Beim Data-Mining werden systematisch statistische Methoden auf große Datenbestände angewandt, um unbekannte Querverbindungen und

53 In *Gola*, Datenschutz am Arbeitsplatz werden verschiedene Überwachungssituationen aufgezählt und untersucht.
54 *Tinnefeld/Viethen*, NZA 2000, 977 (978).
55 Sog. Internet Mobile Equipment Identity; dies ist eine 15-stellige Seriennummer anhand welcher jedes Mobilgerät, welches einen SIM-Schacht hat, identifiziert werden kann. Die IMEI kann durch Eingabe von *#06# in das Wählfeld abgefragt werden.
56 Zu Datenspuren im Internet, vgl. *Köhntopp/Köhntopp*, CR 2000, 248.
57 Vgl. *Däubler*, Gläserne Belegschaften, § 2 Rn. 36.
58 *Tinnefeld/Viethen*, NZA 2000, 977 (979).
59 Zur Verwendung des Begriffs bei Beschäftigtendaten, vgl. *BMAS*, Weißbuch Arbeiten 4.0, S. 142.

Trends zu erkennen.[60] Bei OLAP hingegen wird dem System „eine Frage gestellt" bzw. eine Hypothese in den Raum gestellt, welche durch Analyse der Daten bestätigt oder widerlegt werden soll.[61]

Ein weiteres Risiko ist die einfache Übermittlung bereits gesammelter und elektronisch erfasster Daten; einmal gespeichert können die Daten unbegrenzt oft vervielfältigt und an verschiedenste Empfänger in Bruchteilen von Sekunden versandt werden.[62] Dies gilt nicht nur innerhalb eines Betriebs, sondern über das Internet auch über Betriebs- und Unternehmensgrenzen hinaus bis hin ins nicht-europäische Ausland bei multinationalen Konzernen. Nicht übersehen werden darf hierbei das Risiko von Datenpannen, bei denen unbefugte Dritte Zugriff auf die gespeicherten Informationen über die Arbeitnehmer erhalten.[63]

So bleibt festzustellen, dass die Möglichkeit der Informationsgewinnung aus Daten zwar enorme Vorteile vor allem für die Arbeitgeber, aber auch für die Arbeitnehmer bringen kann, ebenso groß jedoch auch die Risiken sind. Typisches Beispiel hierfür ist die Einführung einer Totalüberwachung als Datenmissbrauch.

III. Datenschutz als Instrument zum Interessensausgleich

Hier setzt das (Beschäftigten-)Datenschutzrecht an, welches die Zulässigkeit der Erhebung und Verarbeitung von personenbezogenen Daten regelt, und vor allem eine maßlose Datensammlung beschränkt[64] sowie Missbräuche mit Strafen belegt. Im Endeffekt stellt das Datenschutzrecht eine Kodifizierung der erforderlichen Grundrechtsabwägung zwischen den Rechten des Verarbeiters (zumeist der Arbeitgeber) sowie des Betroffenen (Arbeitnehmer) im Wege der praktischen Konkordanz dar. So bestimmt Erwägungsgrund 2 der DSGVO, dass *„die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten […] gewährleisten [sollten], dass ihre Grundrechte und Grundfrei-*

60 *Heinson/Schmidt*, CR 2010, 540 (542).
61 *Heinson/Schmidt*, CR 2010, 540 (542).
62 *Roßnagel et al.*, Datenschutz bei Wearable Computing, S. 29.
63 Vgl. jüngst eine der wohl größten Datenpannen weltweit bei welcher 24,5 Mio. hochsensible medizinische Datensätze weltweit ungeschützt zugänglich waren; hierzu *Greenbone Networks GmbH*, Sicherheitsbericht, <www.greenbone.net/wp-content/uploads/CyberResilienceReport_DE.pdf>.
64 *Heinson/Schmidt*, CR 2010, 540 (541 f.).

heiten und insbesondere ihr Recht auf Schutz personenbezogener Daten […] gewahrt bleiben."

Auf nationaler und unionaler Ebene ist das informationelle Selbstbestimmungsrecht des Beschäftigten aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG (bzw. auf unionaler Ebene das Recht auf Privatheit Art. 7 f. EU-GRC) mit dem Eigentumsrecht (Art. 14 Abs. 1 und 2 GG / Art. 17 EU-GRC), der unternehmerischen Freiheit (Art. 12 Abs. 1 GG / Art. 16 EU-GRC) sowie der Vertragsfreiheit des Arbeitgebers (Art. 2 Abs. 1 GG) in einen schonenden Ausgleich (sog. „praktische Konkordanz") zu bringen.[65] Das immer zu berücksichtigende Kriterium der Erforderlichkeit (§ 26 Abs. 1 BDSG) ist letztlich eine Ausprägung der Grundrechtsabwägung um die Verhältnismäßigkeit zu sichern. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten muss geeignet und gleichzeitig das mildeste Mittel darstellen, um die unternehmerischen Interessen und Zwecke bei der Durchführung des Beschäftigtenverhältnisses zu verwirklichen. Wo immer möglich, gilt es, so die Datensammlung auf ein Minimum zu begrenzen.[66] Dies ergibt sich ebenfalls aus Art. 5 Abs. 1 lit. c DSGVO, wonach personenbezogene Daten auf das für Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen (Grundsatz der Datenminimierung).

Gerade im Beschäftigtendatenschutz hat die jahrelange Rechtsprechung des BAG nunmehr ein sehr diffiziles Regelungsregime zur Generalklausel des § 32 BDSG a.F. geschaffen, welches zu einem gerechten Ausgleich der widerstreitenden Interessen führen soll. Diese Rechtsprechungsgrundsätze sollen nach dem Willen des Gesetzgebers auch mit Inkrafttreten der DSGVO weiterhin Anwendung finden.[67] Allerdings bringen neue Technologien – wie beispielsweise *Big Data* – mitunter große (technikspezifische) Risiken, die bislang in der Rechtsprechung kaum behandelt wurden, bereits in naher Zukunft sicherlich zum Alltag der täglichen Judikatur gehören werden.

IV. Zwischenergebnis

Wie die Ausführungen zeigen, herrschen – gerade im Beschäftigungsverhältnis – immer Interessensgegensätze zwischen der verarbeitenden Stelle

65 *Brink/Schwab*, RDV 2017, 170 (172).
66 *Brink/Schwab*, RDV 2017, 170 (172 f.).
67 Vgl. BT-Drs. 18/11325, S. 97.

(Arbeitgeber) und dem Betroffenen (Arbeitnehmer), die durch das (Beschäftigten-)Datenschutzrecht in einen gerechten Ausgleich gebracht werden müssen. Nicht jede Datenerhebung und -verarbeitung führt zwangsweise zu einem Nachteil für den Arbeitnehmer. Die erhobenen Daten können durchaus zum Vorteil des Arbeitnehmers eingesetzt werden. Teilweise ist der Arbeitgeber „als verlängerter Arm des Staates" sogar dazu verpflichtet, Daten zu erheben und an die entsprechenden staatlichen Stellen wie beispielsweise die Finanzverwaltung weiterzuleiten. Das Beschäftigtendatenschutzrecht darf daher nicht als reines Abwehrrecht des Arbeitnehmers gegen die Datenerhebung und -verarbeitung durch den Arbeitgeber gesehen werden, sondern soll vielmehr Missbrauchsfälle verhindern und eine möglichst weitgehende Grundrechtsverwirklichung der einzelnen Parteien ermöglichen.[68] Bei jedem einzelnen Verarbeitungsvorgang müssen daher die Interessen aller Beteiligten und die Gefahren für die Grundrechte genau durchleuchtet werden, bevor pauschal ein Urteil gefällt wird. Bereits aus der Eigenschaft der tangierten Grundrechte als Individualschutzrechte folgt, dass immer Einzelfallgerechtigkeit herzustellen ist.

68 So bestimmt bereits Art. 1 Abs. 3 DSGVO, dass der freie Verkehr personenbezogener Daten aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Union weder eingeschränkt noch verboten werden darf.