Wolfgang Däubler

Gläserne Belegschaften

Das Handbuch zum Beschäftigtendatenschutz

9. Auflage

BUND VERLAG

§ 1 Einleitung

I. Einige praktische Probleme

1. Das verdächtige Personalratsmitglied

In der Kreissparkasse zirkulierte ein anonymes Schreiben, das einen Abteilungsleiter diffamierte. Der Vorstand hegte aus bestimmten Gründen den Verdacht, Verfasser könne das Personalratsmitglied P sein. Anlässlich der Verabschiedung eines Kollegen wurde gerade auch P herzlich zu der Feier eingeladen, wo er Kuchen aß, Kaffee trank und Wein zu sich nahm. Der Vorstand veranlasste daraufhin eine **DNA-Analyse** der Speichelreste, die sich auf dem Falzkleber des bösartigen Briefes befanden. Weiter wurden die Speichelreste auf Kuchengabel, Kaffeetasse und Weinglas des P auf gleiche Weise untersucht. Das Ergebnis war eindeutig: Dieselbe Person, die den Brief zugeklebt hatte, hatte auch den Kuchen gegessen sowie Kaffee und Wein getrunken. Der Vorstand wollte den P fristlos kündigen und beantragte die dafür erforderliche Zustimmung des Personalrats. Dieser lehnte jedoch ab. Der Vorstand rief daraufhin das in solchen Fällen zuständige Verwaltungsgericht an; sein Antrag, die Zustimmung des Personalrats zu ersetzen, wurde in erster Instanz zurückgewiesen. In zweiter Instanz hatte der VGH Mannheim über den Fall zu entscheiden.[1] **1**

Das geschilderte Vorgehen des Sparkassenvorstands ist sicherlich (bislang) eine Ausnahme geblieben. Immerhin ließen sich über das Internet unschwer Firmen ermitteln, die bei Bedarf DNA-Analysen von Gewebeproben machten.[2] Dies erfolgte vorwiegend zu dem Zweck, ungewisse Vaterschaften zu klären[3], doch wer will ausschließen, dass der »betriebliche Speicheltest« irgendwann Schule macht? **2**

2. Lidl, Telekom, Deutsche Bahn u. a.

Seit **Ende März 2008** gibt es in Deutschland **»Datenskandale«.** Die irritierte Öffentlichkeit wurde zunächst im Fernsehen darüber unterrichtet, beim Discounter Lidl habe man Beschäftigte mit versteckten Kameras observiert und Berichte über persönliche Befindlichkeiten geschrieben. Zuvor betrachtete man solche **2a**

1 VGH Baden-Württemberg AuR 2001, 469 (Entscheidung vom 28. 11. 2000 – PL 15 S 2838/99) mit Anmerkung Roos.
2 Nachweise bei Weichert, DuD 2002, 133 Fn. 4.
3 S. etwa die sicherlich nicht selbstironisch gemeinte Internetanschrift *www.papacheck.de.*

Dinge als undenkbar; in fast 60 Jahren Bundesrepublik schien der Datenschutz jedenfalls im privaten Bereich ganz gut zu funktionieren. Die Ende der 1970er Jahre in einer breit angelegten Untersuchung getroffene Feststellung, in über 20 % der untersuchten Fälle hätten sich – in ersichtlich rechtswidriger Weise – medizinische Befund- und Therapiedaten in der Personalakte befunden,[4] war schnell in Vergessenheit geraten.

2b Im September 2008 legten die **Aufsichtsbehörden für den Datenschutz** ihren **Bericht in Sachen Lidl** vor.[5] Danach hatten Detekteien im Auftrag der Firma in rund 30 Lidl-Vertriebsgesellschaften zahlreiche Daten über Beschäftigte gesammelt und zu schriftlichen Berichten zusammengefasst. Die Datenschützer nennen u. a.

- Einschätzung der Arbeitsleistung und Arbeitsmotivation des Mitarbeiters
- Informationen über das Mitarbeiterverhalten gegenüber Kunden
- Informationen zu den Führungsqualitäten von Vorgesetzten
- Informationen über das Pausenverhalten einzelner Mitarbeiter
- Informationen über Zwischenmenschliches und daran anknüpfende Beurteilungen
- Gesundheitszustand und (mögliche) Schwangerschaften
- Finanzielle Situation der Mitarbeiter und ihrer Familien
- Vermutete Stimmungslage und »Wesensart« von Mitarbeitern.

Dies alles wurde durch **versteckte Kameras**, daneben aber auch durch Mithören von Telefonaten und durch **persönliche Gespräche** ermittelt. Letztere kamen zustande, weil offiziell erklärt worden war, die Detektive seien in der jeweiligen Filiale tätig, um Diebstähle durch Kunden aufzuklären; insoweit waren sie **eine Art »verdeckter Ermittler«,** die ihre wahre Rolle nicht zu erkennen gaben. Damit unterschieden sie sich scheinbar nicht grundsätzlich von »Testkäufern«, deren Einsatz bei vielen Einzelhandelsunternehmen gängige Praxis ist,[6] die jedoch nur eine bestimmte »Funktionserfüllung«, nicht aber die ganzen Lebensumstände des Arbeitnehmers erfassen.

2c Die unmittelbar **arbeitsbezogene Observation von Mitarbeitern** stand auch in einigen anderen, weniger bekannt gewordenen Fällen im Mittelpunkt. So wurden etwa in einer Filiale der Firma **Edeka** zwei Detektive als Praktikanten eingeschleust, die heimliche Filmaufnahmen von Beschäftigten machten.[7] Sie dienten anschließend als Mittel, die Betroffenen zu Eigenkündigungen zu veranlassen. In einem Fall wurde auch eine Strafanzeige erstattet, weil ein Beschäftigter während eines vierwöchigen Fahrverbots am Steuer seines Privatwagens gesessen hatte. Auch sollen die Detektive Einzelne zu strafbaren Handlungen wie dem »Mit-Gehen-Lassen« von Waren angestiftet haben.

---

4 Kilian, Personalinformationssysteme, S. 103 ff.

5 Wiedergegeben in RDV 2008, 216, auch zum Folgenden.

6 Aus der Rechtsprechung, die sich in der Regel auf die Mitbestimmungspflichtigkeit bezieht, s. etwa BAG 18. 4. 2000 – 1 ABR 22/99, DB 2000, 2227 = AP Nr. 33 zu § 87 BetrVG 1972 Überwachung; LAG Nürnberg 10. 10. 2006 – 6 TaBV 16/06, NZA-RR 2007, 136, 140.

7 Mitgeteilt bei DANA 2008, 123.

Direkt auf die Arbeit als solche bezogen waren auch die **»Runden Tische« bei Daimler** in Stuttgart und Bremen.[8] Beschäftigte, die einige Zeit krank gewesen waren, wurden nach ihrer Rückkehr von ihrem Vorgesetzten in einem persönlichen Gespräch nach der Natur ihrer Erkrankung sowie danach gefragt, ob sie weiter an Beschwerden leiden würden. Die dabei preisgegebenen Umstände wurden dann am »Runden Tisch« unter voller Namensnennung diskutiert. An diesem waren neben zahlreichen Gruppenleitern auch die Personalabteilung, der werksärztliche Dienst und der Betriebsrat vertreten. Der Inhalt eines persönlichen Gesprächs über den Gesundheitszustand (bis hin zur Einnahme bestimmter Medikamente und zur Fortführung einer psychotherapeutischen Behandlung) wurde so faktisch zum Gegenstand der betriebsinternen Öffentlichkeit. 2d

Die **Firma Tönnies**, Europas größter Fleischverarbeiter, setzte ungefähr 200 Videokameras ein, um die Mitarbeiter zu überwachen. Erfasst wurde zum Teil auch das Verhalten in der Kantine und in Umkleidekabinen.[9] Ähnliches wird in Bezug auf die Firma **Burger King** berichtet.[10] 2e

Bei der **Deutschen Telekom** ging es primär um Aufsichtsratsmitglieder der Arbeitnehmerseite und Mitglieder des Konzernbetriebsrats, deren **Telefonverhalten** im Einzelnen erfasst und ausgewertet wurde. Auf diese Weise sollte ermittelt werden, **wer mit Journalisten** Kontakte hatte und deshalb für das Bekanntwerden von Informationen verantwortlich sein konnte, die für das Unternehmen schädlich waren. Durch Einschaltung einer Detektei wurde überdies die **wirtschaftliche Situation einzelner Mitarbeiter umfassend durchleuchtet**, was sämtliche Kontobewegungen, aber auch Angaben aus der Steuerakte sowie selbst den Zinssatz des Sparbuchs und den Kaufpreis der Eigentumswohnung der Lebensgefährtin erfasste. Wie die Detektei an diese Informationen kam, ist nicht geklärt.[11] In Bezug auf eine Managerin einer kroatischen Tochtergesellschaft wurden eingehende Fakten aus ihrem persönlichen Umfeld bin hin zu vielfältigen Sexkontakten ermittelt und in den Akten festgehalten.[12] Bei der zur Talanx-Gruppe gehörenden **Firma Gerling-Versicherungen** wurden die Verbindungsdaten mehrerer Mitarbeiter und ihre E-Mail-Accounts ausgewertet, um herauszubekommen, wer Interna über den ungewöhnlich brutalen Abbau der betrieblichen Altersversorgung an die Zeitschrift »Capital« gegeben hatte – freilich ohne Erfolg.[13] 2f

Die **Deutsche Bahn AG** schaltete gleichfalls Detekteien ein, um herauszufinden, inwieweit Mitarbeiter oder ihre Ehe- und Lebenspartner Scheinfirmen betrieben oder auf andere Weise an der Auftragsvergabe durch die Bahn profitierten. Zu diesem Zweck wurden die Bankverbindungen und Kontobewegungen von Mitarbeitern und ihren Ehegatten[14] mit denen von Lieferanten und Dienstleistern 2g

8 S. die kurze Notiz in DANA 2009, 26.
9 Mitgeteilt bei DANA 2008, 164.
10 DANA 2008, 122.
11 Darstellung nach Handelsblatt vom 18. 5. 2009, S. 1.
12 Handelsblatt vom 20. 5. 2009, S. 11.
13 Mitgeteilt in DANA 2008, 122.
14 Mitgeteilt bei Ehleben/Schirge/Seipel, AiB 2009, 192.

abgeglichen. Erfasst waren ca. 173 000 Beschäftigte, was zu 300 »Treffern« und zu 125 Fällen von »verschärfter Beobachtung« führte. Ein konkreter Verdacht gegen bestimmte Personen hatte sich nicht ergeben; von positiven Ergebnissen der »verschärften Beobachtung«, insbesondere von strafgerichtlichen Verurteilungen, wird nirgends berichtet.[15] Einbezogen wurden alle Beschäftigten, also damit auch sehr viele Personen, die nichts mit der Vergabe von Aufträgen zu tun hatten. Bei der **Aktion »Uhu«** sollte ermittelt werden, wer von insgesamt 40 Personen, die Zugang zu bestimmten Informationen hatten, die Presse eingeweiht haben konnte. Die E-Mail-Daten, die an die Detektei gegeben worden waren, erbrachten keine Aufschlüsse. Ein »Schriftstilgutachten« verwies auf eine bestimmte Person, die daraufhin gekündigt wurde – freilich im Ergebnis ohne Erfolg, da sich das Arbeitsgericht von dem Gutachten nicht überzeugen ließ.[16] Das persönliche Umfeld einer Reihe von Führungskräften wurde auch bei der **Deutschen Bank** erforscht, obwohl kein konkreter Verdacht strafbarer Handlungen vorlag.[17]

2h In einer Hannoveraner Niederlassung der Firma **Primark** musste der 2014 erstmals gewählte Betriebsrat feststellen, dass dort insgesamt 128 Videokameras installiert waren, die auch Aufenthaltsräume der Beschäftigten und Umkleidekabinen erfassten. Im Büro des Filialleiters befand sich ein Kamerasteuerungsgerät samt Monitor; der »Boss« konnte so immer die Kamera aussuchen und die von dieser aufgenommenen Vorgänge »heranzoomen«, die ihn gerade interessierten. Der Betriebsrat kam in achtmonatigen Verhandlungen zu einem Kompromiss: In allen nicht öffentlich zugänglichen Bereichen wurden die Kameras abgebaut, auch die Kassiererinnen an den Kassen waren außerhalb der Beobachtungszonen. Die aufgezeichneten Bilder wurden nach 72 Stunden automatisch gelöscht. Insgesamt blieben 67 Kameras übrig.[18] In jüngster Zeit erlangte das Textilhandelsunternehmen **Hennes & Mauritz (H&M)** eine wenig schmeichelhafte Bekanntheit: In der Niederlassung Nürnberg hatte die Personalleitung jahrelang Daten aus dem Privatbereich der Mitarbeiter erfasst, die von familiären Konflikten über das religiöse Bekenntnis bis hin zu gesundheitlichen Beeinträchtigungen »von der Blasenschwäche bis zur Krebserkrankung« reichten.[19] Nach eingehenden Untersuchungen verhängte die zuständige Aufsichtsbehörde ein Bußgeld in Höhe von 35,3 Mio. Euro.[20]

3 Im Vergleich zu diesen Vorgängen sind die traditionellen Probleme des betrieblichen Datenschutzes, wie sie etwa in den Berichten der Aufsichtsbehörden zum Ausdruck kommen, von eher undramatischer Natur. Darf beispielsweise eine **Abmahnung** von der Personalabteilung **in einem unverschlossenen Umschlag** an den Betroffenen gesandt werden, obwohl dadurch z. B. die Beschäftigten der Poststelle unschwer den Inhalt des Schreibens zur Kenntnis nehmen können?

15 Auch nicht bei Diller, BB 2009, 438 ff.
16 Sämtliche Mitteilungen nach DANA 2009, 20.
17 Handelsblatt v. 26. 5. 2009, S. 1.
18 Im Einzelnen geschildert bei Däubler, CuA 2/2016, S. 30.
19 Berichtet in CuA 3/2020, S. 7.
20 Berichtet in CuA 11/2020, S. 6.

Darf ein **ärztliches Zeugnis in der Personalakte** bleiben, das sich mit einer inzwischen überwundenen psychischen Erkrankung befasst? Folge wäre, dass jeder Personalsachbearbeiter, der über einen Urlaubsantrag entscheidet, automatisch auch diese sensiblen Inhalte erfahren könnte.[21] Ist es zulässig, dass sich auf einer Wand des Prokuristenzimmers ein großes Plakat befindet, auf dem die **Verkaufserfolge** der einzelnen Außendienstmitarbeiter aufgezeichnet und so für jeden Besucher nachvollziehbar sind?[22]

Probleme traten selbstredend schon bisher im Zusammenhang mit Informationstechniken auf. Ist die **Video-Überwachung**, wie man sie aus dem Supermarkt oder der Bankfiliale kennt, eigentlich den Arbeitnehmern gegenüber beliebig zulässig? Was geschieht, wenn der Betriebsrat – wie häufig – mit dem Arbeitgeber verbindlich vereinbart, dass das Verhalten der Beschäftigten auf diesem Wege nicht kontrolliert werden darf, der Arbeitgeber sich dann aber nicht daran hält? Unzulässig erlangte Beweismittel dürfen an sich nicht verwertet werden,[23] doch gilt dies auch für ein »Geständnis«, das ein Arbeitnehmer nach Konfrontation mit den ihn belastenden Aufnahmen abgelegt hat? Wie ist eine »**versteckte Kamera**« im Betrieb zu behandeln? Kann der Einzelne wegen Verletzung seines allgemeinen Persönlichkeitsrechts vielleicht sogar Schadensersatz verlangen?[24] Die in der Literatur gestellte besorgte Frage, ob die illegale Videoüberwachung nicht für den Arbeitgeber sehr kostspielige Folgen haben könne,[25] legt eine positive Antwort nahe. 4

3. Neuere technische Entwicklungen

Der Schutz der Persönlichkeitssphäre des Arbeitnehmers legitimiert sich nicht in erster Linie durch die Bekämpfung von »Skandalen«. Vielmehr gibt es zahlreiche als ganz »normal« akzeptierte Entwicklungen, die zu »gläsernen Belegschaften« führen könnten. So hat beispielsweise die **Nutzung von E-Mail, Intranet und Internet** neben unbestreitbaren Vorzügen auch den Nachteil, dass das Verhalten des Einzelnen intensiv überwacht werden kann, ohne dass er dies überhaupt bemerkt. Inwieweit kann von solchen technischen Möglichkeiten Gebrauch gemacht werden? Darf der Arbeitgeber – so eine häufig gestellte Frage – offen oder auch heimlich E-Mails lesen, die aus dienstlichem Anlass an einzelne seiner Beschäftigten gerichtet sind? Wie steht es mit E-Mails, die privaten Charakter tragen? Und weiter: Dürfen alle aufgerufenen Internet-Seiten mit Hilfe der Firewall des Arbeitgebers gespeichert und ggf. ausgewertet werden? Das Anlegen 5

21 S. den Fall BAG 15. 7. 1987 – 5 AZR 215/86, NZA 1988, 55.
22 S. die Schilderung in DSB Schleswig-Holstein, 23. TB, unter 6.3.2.
23 So bezüglich unzulässiger Videoaufnahmen im Grundsatz BAG 16. 12. 2010 – 2 AZR 485/08, NZA 2011, 571.
24 Dazu ArbG Frankfurt/Main 20. 3. 2001 – 5 Ca 4459/00, RDV 2001, 190; LAG Hessen 25. 10. 2010 – 7 Sa 1586/09 – wiedergegeben bei Ruhland, CuA 4/2011, S. 13.
25 Klein/Roos, ZD 2016, 65.

einer solchen Protokolldatei ist jedenfalls nicht von vorne herein unzulässig.[26] Muss der Arbeitnehmer nach Ende des Arbeitsverhältnisses die **Festplatte seines PC** auch dann an den Arbeitgeber **herausgeben**, wenn er erlaubterweise private Dokumente dort gespeichert hatte?[27] Auf dem Software-Markt sind zahlreiche Programme erhältlich, die jede Aktivierung des Computers aufzeichnen und die sich in diesem auch unbemerkt installieren lassen.[28] Das ArbG Augsburg hatte sich mit einem Fall zu befassen, in dem eine solche Spyware mit dem Ziel eingesetzt wurde, angebliche Manipulationen des Betriebsratsvorsitzenden bei der Zeiterfassung aufzudecken.[29] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit beklagte schon vor vielen Jahren, dass die Angebote insoweit immer zahlreicher und preisgünstiger würden.[30] Im Einzelfall lässt sich auch eine **Webcam** installieren, die von Zeit zu Zeit (unbemerkt) Aufnahmen macht. Sonderprobleme ergeben sich, wenn Arbeitnehmerdaten in die **»cloud«** ausgelagert werden,[31] da sich dabei die Server häufig in Drittstaaten befinden, die über kein entwickeltes Datenschutzrecht verfügen.

6 Der **Aufenthaltsort des Arbeitnehmers** kann nicht nur bei Fernfahrern mit Hilfe von GPS[32] festgestellt werden. So macht es technisch keine Schwierigkeiten, den jeweiligen **»Standort« eines Handys** ausfindig zu machen, und zwar auch dann, wenn nicht telefoniert wird.[33] Der Ermittlungsrichter beim BGH hat die Nutzung dieser Möglichkeit im Rahmen eines strafrechtlichen Ermittlungsverfahrens ausdrücklich gebilligt,[34] doch gilt dasselbe auch im Arbeitsleben? Kann hier auf eine Einschaltung von Gerichten verzichtet und dieses Mittel allein zum Zweck einer Optimierung der Arbeitsprozesse eingesetzt werden? Die Frage ist Gegenstand einer eingehenden Diskussion.[35] Das **heimliche Anbringen von GPS-Sensoren** ist vom BGH als strafbare Handlung qualifiziert worden.[36]

7 Rechtlich gleichfalls nicht unproblematisch erscheint das immer häufiger angewandte Verfahren, einzelne Personen mit Hilfe **biometrischer Merkmale wie Fingerabdruck** oder äußerer Gestalt der Iris zu identifizieren. Dabei wird meist

---

26 So bereits Köppen, CuA 6/2012, S. 36 unter Bezugnahme auf den Bericht des brandenburgischen Datenschutzbeauftragten. Für Zulässigkeit der Auswertung des Browserverlaufs nur im Ausnahmefall des Verdachts einer Straftat oder einer schweren Pflichtverletzung BAG 27. 7. 2017 – 2 AZR 681/16, NZA 2017, 1327 ff.

27 Vgl. LAG Schleswig-Holstein 20. 1. 2000 – 4 Sa 389/99, RDV 2001, 107. Zur Behandlung solcher »Mischdateien« s. Däubler, Digitalisierung und Arbeitsrecht, § 8 Rn. 90 f. mwN.

28 Einzelheiten schon bei Haverkamp, CF Heft 7/2000, S. 26.

29 ArbG Augsburg, 4. 10. 2012 – 1 BV 36/12, LAGE Art. 2 GG Persönlichkeitsrecht Nr. 16; eingehende Darstellung und Würdigung der Entscheidung bei Däubler, CuA 1/2013, S. 13 ff.

30 Mitgeteilt bei *www.heise.online.de* v. 05. 04. 2001 (Abfrage am 10. 03. 2002).

31 Zum Cloud Computing s. Sinn, CuA 4/2014, S. 4 und das Handbuch von Borges/Meents sowie Rost u. a., RDV 2020, 240.

32 Global Positioning System.

33 Einzelheiten bei Fox, DuD 2002, 212 ff.

34 BGH DSB Heft 4/2001, S. 19.

35 Kiesche/Wilke, CuA 7/2009, S. 5 ff.; Schröder, ZD 2013, 13; Thannheiser, CuA 2/2014, S. 4, zuletzt Gola/Pötters/Wronka, Arbeitnehmerdatenschutz, 7. Aufl., Rn. 1250 ff.

36 BGH 4. 6. 2013 – 1 StR 32/13, ZD 2013, 502 = RDV 2013, 297.

übersehen, dass sich bei dieser Gelegenheit »überschießende Informationen« höchst sensibler Art wie z. B. solche über die aktuelle Stimmung und den Gesundheitszustand ergeben können.[37]

7a Verfahren dieser Art sind nur die sichtbare Spitze eines Eisbergs. Mit Hilfe von **»Cloud Computing«** wird die Speicherung und Verarbeitung von Daten auf solche Dritte ausgelagert, bei denen die nötigen Kapazitäten gerade zur Verfügung stehen.[38] Dabei geht es nicht nur um die Bereitstellung von Speicherkapazitäten (»Infrastructure as a Service – IaaS«), sondern häufig auch um das Angebot von Verarbeitungsmöglichkeiten (»Software as a Service – SaaS«).[39] In der Regel werden solche »Cloud-Dienste« preiswert angeboten; meist werden sie vom Anbieter nicht selbst erbracht, sondern sind Sache von Sub- und Subsubunternehmern. Diese befinden sich irgendwo auf der Welt; der Auftraggeber und eigentliche »Herr« der Daten hat keinerlei wirksame Kontrolle mehr, ja er weiß nicht einmal, auf welchem Server sich seine Daten gerade befinden. Die Einhaltung von Vorschriften zu kontrollieren, ist faktisch nicht mehr möglich; auch ist nicht abschätzbar, inwieweit ausländische Instanzen auf das Gespeicherte zugreifen.

7b Hinter dem Stichwort **»Big Data«** verbirgt sich das Phänomen, dass riesige Datenmengen verfügbar gemacht werden, die mit immer besseren Methoden ausgewertet werden können.[40] Eine Milliarde Facebook-Nutzer generieren automatisch eine unübersehbare Zahl von Daten, jede Minute wird auf YouTube Videomaterial hochgeladen, das für 72 Stunden »Programm« genügt.[41] Viele Geräte sind mit dem Internet verbunden; das mit einem »Navi« ausgerüstete Auto mag als Beispiel stehen.[42] Aus diesem unendlich großen Material lassen sich mit den vorhandenen Analysetools neue Erkenntnisse zu dem Ziel gewinnen, auf der Makroebene menschliches Verhalten mit möglichst hoher Wahrscheinlichkeit vorauszusagen. Auf der Mikroebene ermittelt man bislang unbekannte Präferenzen und Eigenschaften bestimmter Personen, so dass man – so die harmloseste Konsequenz – ihnen gegenüber eine **optimale Werbestrategie** praktizieren kann.[43] Wer ein Buch bei Amazon kauft, wird häufig einen Hinweis darauf erhalten, welche weiteren Bücher andere Käufer desselben Buches angeklickt oder erworben haben. Dies ist alles andere als eine spontane Eingebung; manche sprechen von einem Ende der Anonymität im Netz.[44] Dabei kann man sich keineswegs darauf verlassen, die großen Anbieter wie Facebook und Google hätten immer ein unta-

37 Dazu Hamb. DSB, 18. TB, S. 3, 16 ff.; kritisch auch die nds. Datenschutzbeauftragte, berichtet bei Köppen, CuA 3/2016, S. 36 ff. Gegen Anwesenheitskontrolle und Zeiterfassung durch Fingerabdrücke LAG Berlin-Brandenburg 4. 6. 2020 – 10 Sa 2130/19, RDV 2020, 273.

38 Dazu Baunack, CuA 4/2016, S. 32; Funke/Wittmann, ZD 2013, 221 ff.; Rost u. a., RDV 2020, 240; Sinn, CuA 4/2014 S. 4 ff.; Weichert, DuD 2010, 679 ff.

39 Hamann, in: Arnold/Günther (Hrsg.), Kap. 6 Rn. 93 f.

40 Brandt, CuA 11/2013 S. 11. Zum Begriff s. weiter Rozek, CuA 7–8/2017, S. 38 ff.

41 Weichert, ZD 2013, 252.

42 Man spricht insoweit vom »Internet der Dinge« – dazu Sinn, CuA 12/2013, S. 4; Nürnberger/Bugiel, DuD 2016, 503.

43 Roßnagel, ZD 2013, 562. Dazu auch BITKOM, Big-Data-Technologien, S. 19 ff.

44 Boehme-Neßler, DuD 2016, 419.

deliges Verhältnis zur Rechtsordnung.[45] So hat **Facebook** ohne Einwilligung der Betroffenen die Daten von 87 Mio. Nutzern an die Firma Cambridge Analytica weitergegeben, wobei Aussagen im Rahmen einer Umfrage, aber auch die Kommunikation mit »Freunden« erfasst waren.[46] Weiter wurden zahlreiche Klauseln in den Facebook-Vertragsbedingungen vom LG Berlin für unwirksam erklärt.[47] Auch wurden die »Hinweise« des App-Zentrums von Facebook beanstandet[48] und die Datenweitergabe von WhatsApp an Facebook nach der Übernahme untersagt.[49] Die spanische Datenschutzaufsichtsbehörde verhängte eine Geldstrafe in Höhe von 1,2 Mio. Euro gegen Facebook;[50] wegen falscher Angaben setzte die EU-Kommission eine Strafe von 110 Mio. Euro fest.[51] Wegen Missbrauchs seiner marktbeherrschenden Stellung musste **Google** im Juni 2017 2,42 Milliarden, im August 2018 4,34 Milliarden Euro Bußgeld in den USA bezahlen.[52] In Frankreich waren wegen Datenschutzverstößen 50 Mio. Euro fällig.[53]

7c **Auch Beschäftigtendaten** können betroffen sein.[54] So lässt sich etwa der Arbeitseinsatz dadurch ermitteln, dass man eine Korrelation zwischen dem Wetter, der in der Abteilung bestehenden Arbeitsbelastung und der gleitenden Arbeitszeit herstellt: Wer trotz vieler Arbeit bei schönem Wetter kaum länger als die obligatorische Kernzeit im Betrieb bleibt, hat offensichtlich eine gewisse innere Distanz zu seiner Tätigkeit und/oder seinem Arbeitgeber. Wer Betriebsratsmitglied ist, keine Familie hat und abends häufig Lieder der Arbeiterbewegung auf YouTube hört, wird eher streikbereit sein als ein unauffälliger Kollege ohne Amt, der sich abends um seine Familie kümmert. Auch wenn von solchen Möglichkeiten derzeit (wohl) noch kaum Gebrauch gemacht wird, liegt hier in der Zukunft ein weites Anwendungsfeld für datenschutzrechtliches Gegensteuern.[55] Besonders fällt dabei ins Gewicht, dass die innerbetriebliche Kommunikation immer stärker über (elektronische) Netze erfolgt und dabei so viele Daten liefert, dass sich ein fast vollständiges Abbild des betrieblichen Geschehens herausbildet, das differenzierter Auswertung zugänglich ist.[56] Relevante Daten lassen sich zu **Algorithmen** zusammenfassen, an denen dann Bewerber oder für eine Beförderung in Frage kommende Personen gemessen werden.[57]

45 Exemplarisch OVG Hamburg 26. 2. 2018 – 5 Bs 93/17, ZD 2018, 230 (WhatsApp).
46 Spiegel Online 4. 4. 2018. Die Zahl der in Deutschland betroffenen Nutzer wurde mit über 300 000 veranschlagt. Der Fall ist erwähnt auch bei Dzida, BB 2018, 2677.
47 LG Berlin 16. 1. 2018 – 16 O 341/15, K&R 2018, 269.
48 KG 22. 9. 2017 – 5 U 155/14, ZD 2018, 118 = K&R 2018, 121.
49 OVG Hamburg 26. 2. 2018 – 5 Bs 93/17, K&R 2018, 282.
50 ZD 11/2017 S. XI = ZD-Aktuell 2017, 05780.
51 ZD 8/2017 S. XII = ZD-Aktuell 2017, 0564.
52 Angaben nach Kübler, BB 2018, Heft 34, Erste Seite.
53 Votteler, ZD 2019, 431. Weitere Einzelheiten zur Bußgeldpraxis unten § 12 VI 2 (Rn. 626 ff.).
54 Hierzu und zum Folgenden Brandt, CuA 11/2013, S. 11 ff.
55 Weiterführend Weichert, ZD 2013, 251.
56 Eingehend Höller, CuA 5/2016, S. 9 ff.
57 Nachweise bei Däubler, Digitalisierung und Arbeitsrecht, § 9 Rn. 4 ff., 22 ff.

Große aktuelle Bedeutung hat der Anschluss an **soziale Netzwerke wie Facebook** oder Google+. Sie werden in steigendem Umfang als Mittel auch zur dienstlichen Kommunikation verwendet,[58] wobei der öffentliche Charakter des Mediums einige Probleme aufwerfen kann. Gegenstand heftiger Diskussion war etwa die Frage, ob ein Mitbestimmungsrecht besteht, wenn der Arbeitgeber Kunden das Recht einräumt, auf seiner Facebook-Seite Beschäftigte zu bewerten, mit denen sie in Kontakt gekommen waren.[59] Weiter haben unbedachte und zum Teil auch unqualifizierte Äußerungen von einem privaten Facebook-Account aus zu höchst unangenehmen arbeitsrechtlichen Konsequenzen geführt.[60] Wer Abends über Facebook »postet«, wähnt sich in seiner Privatsphäre, obwohl er sich in Wirklichkeit mitten auf einem viel besuchten Marktplatz befindet, wo nicht nur Freunde zuhören und angreifbare oder beleidigende Äußerungen an andere weiter tragen. **7d**

Je mehr man sich dem **»Internet der Dinge«** nähert, wo sich selbst steuernde Systeme dominieren und der Mensch (fast) nur noch als Konstrukteur und bei »Pannen« gefragt ist, umso mehr fallen Daten an: Jeder Eingriff in elektronisch gesteuerte Systeme wird notwendigerweise erfasst, jeder Handgriff wird zur Datenquelle.[61] Das Arbeitsverhalten wird in allen Details abgebildet;[62] dies gilt beispielsweise auch für den Umgang mit **Robotern**.[63] Schranken sind faktisch weithin auf die Verwendungsebene begrenzt. In der **»Arbeit 4.0«** ist der Datenschutz von noch größerer Bedeutung als heute.[64] Um ihn auf die neuen Herausforderungen vorzubereiten, besteht durchaus zeitlicher Spielraum, da Big Data, Algorithmen und Roboter zwar in aller Munde sind, in der Praxis jedoch noch eine recht geringe Rolle spielen.[65] **7e**

4. Staatlicher Zugriff

Arbeitnehmerdaten können auch für staatliche Instanzen von erheblichem Interesse sein. Dies ist am Beispiel der **Rasterfahndung nach dem 11. September** **8**

58 Bager, CuA 7–8/2013, S. 37; Carstensen, CuA 6/2014, S. 18; Gliewe, AuA 8/2012 S. 464; Bender, K&R 2013, 218.

59 Ablehnend LAG Düsseldorf 12. 1. 2015 – 9 TaBV 51/14, ZD 2015, 282 = NZA-RR 2015, 355, aufgehoben durch BAG 13. 12. 2016 – 1 ABR 7/15, NZA 2017, 657.

60 Däubler, CuA 6/2013, S. 12.

61 S. das Beispiel bei Karthaus, NZA 2017, 558ff.

62 Ebenso Rozek, CuA 7–8/2017, S. 39.

63 Zum Einsatz von Robotern s. Groß/Gressel, NZA 2016, 990, die allerdings der Versuchung erliegen, Entscheidungen eines Roboters (»Was ist als nächstes zu erledigen?«) wie menschliche Entscheidungen zu behandeln. Roboter kann man jederzeit deaktivieren, bei Menschen ist dies nicht in gleicher Weise möglich.

64 S. die Beiträge von Robrecht und Hofmann, in: Taeger (Hrsg.), Internet der Dinge, S. 195ff., 209ff.

65 Tuleweit, CuA 12/2019, S. 28 berichtet über eine Befragung von mehr als 14000 Beschäftigten in über 600 Betrieben der chemischen Industrie: E-Mail und Intranet nutzten die allermeisten, während nur 5% mit Big Data und weniger als 1% mit Künstlicher Intelligenz, 3-D-Druckern, Datenbrillen und Smart Watches zu tun hatten. Dabei geht es um eine Branche, in der sich nicht wenige Weltmarktführer befinden.

2001 besonders deutlich geworden, bei der von einzelnen Firmen der Energieversorgung und der Chemie verlangt wurde, Daten über männliche Arbeitnehmer zwischen 18 und 40 Jahren herauszugeben, um so eventuelle »Schläfer« zu ermitteln. Im Zusammenhang damit wurde sogar die Auffassung vertreten, wenn die Ermittlungsbehörde Vertraulichkeit wünsche, dürfe der Betriebsrat nicht einmal informiert werden.[66] Das Terrorismusbekämpfungsgesetz vom 9. 1. 2002[67] hat durch seinen Art. 5 den Anwendungsbereich des sog. Sicherheitsüberprüfungsgesetzes vom 20. 4. 1994[68] erheblich ausgeweitet. Nach Maßgabe einer Rechtsverordnung können danach auch Beschäftigte in Unternehmen der Energieerzeugung und der Telekommunikation samt ihren Ehe- oder Lebenspartnern einer »**Sicherheitsüberprüfung**« unterzogen werden, die weite Teile des Privatlebens erfasst.[69] Bereits zu früheren Zeiten wurde – wenn auch auf höchst zweifelhafter Rechtsgrundlage – Entsprechendes praktiziert. So erklärte etwa Ende der 70er Jahre der Bundesarbeitsminister die EDV-Abteilung der Bundesversicherungsanstalt für Angestellte für »sicherheitsempfindlich«, was zur Folge hatte, dass alle Beteiligten sicherheitsüberprüft wurden. Das BAG hat dieses Vorgehen gebilligt,[70] obwohl es selbst einräumte, dass die gespeicherten Daten von keinem nachrichtendienstlichen Interesse seien. Entscheidend ist, dass derjenige, der die »Zuverlässigkeitsprüfung« nicht besteht, in dem fraglichen Bereich (der den gesamten Betrieb umfassen kann) nicht mehr beschäftigt werden darf. Dies wird in vielen Fällen Arbeitslosigkeit zur Folge haben.[71]

8a Heute stehen andere Maßnahmen im Vordergrund. Unternehmen erhalten ein im Außenhandel dringend erforderliches AEO-Zertifikat nur dann, wenn die Personalien ihrer Beschäftigten **mit den Antiterrorlisten** regelmäßig **abgeglichen** wurden, die von den USA und der EU-Kommission aufgestellt werden und die Personen aufzählen, die der Unterstützung des Terrorismus verdächtig sind.[72] Umfassender sind verbreiteter Einschätzung nach die Überwachungsmaßnahmen der National Security Agency **(NSA).** Wie weit sie im Einzelnen reichen, ist nicht vollständig bekannt, doch ist es höchst unwahrscheinlich, dass Unternehmen und die dort tätigen Arbeitnehmer ausgeklammert bleiben.[73] Dem Whistle-

66 Rossmann/Gerling, DuD 2001, 750.
67 BGBl. I S. 361.
68 BGBl. I S. 867.
69 Die Ehe mit einer Russin kann »Sicherheitsbedenken« auslösen, wenn deren Bruder in der russischen Armee tätig ist. So BVerwG 9. 11. 1994 – 1 WB 10/94, zitiert bei BVerwG 9. 12. 1999 – 1 WB 60/99, ZBR 2000, 127. Überblick über die Rechtsprechung bei Däubler, SÜG, § 5 Rn. 14 ff.; zum Rechtsschutz s. dort § 14 Rn. 26 ff.
70 BAG 17. 5. 1983 – 1 AZR 1249/79, NJW 1984, 824 ff.
71 Näher zum Menschen als »Sicherheitsrisiko« im Bereich des Arbeitsrechts Däubler, SR 2012, 57 ff.
72 Däubler-Gmelin, DuD 2011, 456; Schlarmann/Spiegel, NJW 2007, 870, 872; Homburg, AuR 2013, 137 f.; Däubler-Gmelin, CuA 4/2014, S. 13; s. auch Gola/Pötters/Wronka, Rn. 1348 ff.
73 Konrad-Klein, CuA 9/2013, S. 24; zum PRISM-Skandal s. Jakobs, CuA 11/2013, S. 26.

blower Eduard Snowden kommt das große Verdienst zu, die Öffentlichkeit auf die Problematik aufmerksam gemacht zu haben.[74]

II. Technische Entwicklung und Recht

Die geschilderten betrieblichen Beispiele und Problemfälle wurden lange Zeit als eher theoretische Möglichkeit gesehen: Allenfalls in pathologischen Ausnahmefällen sei damit zu rechnen, dass die technischen Möglichkeiten ausgeschöpft würden. Gibt es nicht auch ein Arbeitgeberinteresse daran, das Unternehmen nicht zu einem »Überwachungsstaat« im Kleinen werden zu lassen? Und gibt es nicht in Form des Datenschutzrechts und der Mitbestimmung genügend Möglichkeiten, die Nutzung der Technik auf ein verträgliches Maß zurecht zu stutzen? **9**

Diese (verbreitete) Grundhaltung ist in den vergangenen Jahren immer stärker erschüttert worden. Die oben geschilderten »Datenskandale«[75] waren Anlass, den rechtlichen Schutz skeptisch zu beurteilen; das Vertrauen war weithin verloren gegangen. War dies noch auf die betriebliche Sphäre beschränkt, so ist die ganze Gesellschaft betroffen, wenn im Prinzip jedermann bis hin zur Bundeskanzlerin von ausländischen Geheimdiensten überwacht wird und auch in Zukunft überwacht werden kann – und zwar von Organisationen, die über eine hervorragende technische Ausrüstung verfügen und deren Auftrag nicht nur darin besteht, potentielle oder tatsächliche Terroristen zu bekämpfen, sondern die auch vor Betriebs- und Geschäftsgeheimnissen der europäischen Konkurrenz nicht halt machen werden. **9a**

Die veränderte Situation macht es umso dringender, sich um das Verhältnis von Recht und Technik zu kümmern. Ist das **Recht überhaupt in der Lage**, die technischen Möglichkeiten wirksam zu beschränken? Oder gehört es zur unantastbaren unternehmerischen Freiheit, eben auch DNA-Analysen oder Überwachungssoftware zu entwickeln und auf den Markt zu bringen? **9b**

Für eine bürgerlich-liberale Rechtsordnung wie die unsrige sind technische Veränderungen im Prinzip ohne Bedeutung. Sie regelt im Kern nur den marktförmigen Austausch durch Privateigentümer. Was getauscht wird und unter welchen Lebensumständen dies die Beteiligten tun, ist rechtlich irrelevant. So finden etwa die Regeln über den Kaufvertrag nach §§ 433 ff. BGB ohne Rücksicht darauf Anwendung, ob ein Huhn, ein Motorrad oder ein Softwarepaket verkauft wird. **9c**

Der Staat beschränkt sich darauf, die Einhaltung der Spielregeln zu überwachen. Wer Verträge und allgemeine Verhaltenspflichten verletzt oder sich auf anderem als vertraglichem Wege Güter eines anderen verschafft, sieht sich Sanktionen ausgesetzt, die notfalls mit staatlichen Machtmitteln durchgesetzt werden.[76] Zwar **10**

74 Zur Verlängerung einer maßgebenden Bestimmung des Foreign Intelligence Surveillance Act (FISA) s. Spies, ZD 3/2018 S. V = ZD-Aktuell 2018, 05932.

75 Oben Rn. 2a – 2g.

76 Eingehender Däubler, ZRP 1986, S. 42 ff.

war die Rechtsordnung nie völlig mit diesem »Marktrecht« identisch; es gab immer auch Normen, die wie das Verbot der Tötung und Körperverletzung höchstpersönliche Rechtsgüter schützten oder die einen bestimmten Lebensbereich wie die Ehe nach anderen als marktorientierten Kriterien regeln wollten. Aber der Schwerpunkt lag bei den marktbezogenen Regeln.

11 Der moderne Interventionsstaat hat zur Sicherung und Erhaltung des Wirtschaftssystems dennoch zahlreiche Korrekturen vorgenommen. Sie beruhen z. T. auf bewussten strategischen Überlegungen (Beispiele: Bismarcks Sozialpolitik, Erhards soziale Marktwirtschaft in der Wiederaufbauphase der Bundesrepublik); z. T. waren sie Ergebnis des Kampfes der Gewerkschafts- und Arbeiterbewegung (Koalitionsfreiheit, Streik). Im Einzelfall konnte sich auch beides vermengen (sozialpartnerschaftliche Teile des Arbeitsrechts). Die Intervention blieb allerdings insofern immer punktuell, als die Prämissen des Rechtssystems nicht angetastet wurden. Die liberale Vertrags- und Rechtsstaatsordnung wurde in einzelnen Bereichen überlagert, nicht ersetzt.

12 Am Umgang mit der Technik wird dies hinreichend deutlich. Von einigen Ausnahmen wie dem militärischen Bereich und dem Energiesektor einmal abgesehen, ist es weiterhin **Sache der Eigentümer** und ihrer Beauftragten, im Hinblick auf den Markt darüber zu entscheiden, **welche Techniken entwickelt werden** und welches Potenzial ungenutzt bleiben soll. Ein »Technikrecht« hat sich anders als ein »Wettbewerbsrecht« nicht entwickelt; das ansonsten so expansive Wirtschaftsrecht zeichnet sich hier durch ein hohes Maß an Abstinenz aus.[77] Zwar gibt es eine Menge von technischem Sicherheitsrecht – vom Atomrecht bis zur StVZO –, doch bringt dieses gewissermaßen von außen Korrekturen an: Wenn die Gesundheit der Bevölkerung nicht über das gesetzlich zulässige Maß hinaus gefährdet wird, steht der Entwicklung neuer Techniken nichts im Wege. Das Recht ist – so der übliche Ausdruck – »technikneutral«.[78] Dies alles führt dazu, dass die Technik typischerweise einen zeitlichen Vorsprung gegenüber dem Recht hat,[79] was in jüngerer Zeit etwa am Beispiel des Web 2.0[80] oder des Cloud Computing[81] besonders deutlich wurde. Nicht die Schwerfälligkeit der Gesetzgebung oder der Gerichte ist für dieses »Nachhinken« des Rechts verantwortlich, sondern die politisch durchaus gewollten Marktfreiheiten setzen hierfür die entscheidende Ursache. Sie fördern ganz gewiss die Innovation – gleichzeitig **kanalisieren** sie den **Erfindungsreichtum** jedoch auf marktgängige, **gewinnträchtige Erzeugnisse**. Soziale Nützlichkeit spielt nur insoweit eine Rolle, als sie sich in Euro und Cent niederschlägt.

77 Dies ist im Einzelnen expliziert in Däubler-Gmelin/Adlerstein (Hrsg.), Menschengerecht. 6. Rechtspolitischer Kongress der SPD, S. 268 ff.
78 Vgl. Hamann, in: Arnold/Günther, Kap. 6 Rn. 14.
79 S. das von Weichert (DuD 2009, 7 ff.) eindringlich beschriebene Missverhältnis zwischen dem BDSG und den Persönlichkeitsgefährdungen durch das Internet.
80 Dazu Hoeren/Vossen, DuD 2010, 463 ff.
81 Weichert, DuD 2010, 679 ff.; s. auch Birk/Wegener, DuD 2010, 641 ff.

III. Aktueller Anwendungsfall: Digitale Techniken und Recht

Die juristische Verarbeitung der Informations- und Biotechnologien folgte bislang im Wesentlichen diesem Muster. Die »Industrialisierung der Kopfarbeit« (Steinmüller)[82] und die durch sie eingeleitete Umgestaltung der Lebensverhältnisse wird nicht als »kollektiver«, die gesamte Gesellschaft angehender Prozess begriffen. Würde man dies tun, so wäre es ersichtlich Sache der für Grundsatzfragen zuständigen parlamentarischen Instanzen, vielleicht sogar des souveränen Volkes selbst, die Richtung der weiteren Entwicklung festzulegen. Stattdessen erfolgen Korrekturen vom Persönlichkeitsschutz des Einzelnen her: Wer über andere Menschen Daten in Dateien speichert oder verarbeitet, bedarf hierfür einer rechtlichen Erlaubnis. Dass Verträge und vertragsähnliche Vertrauensverhältnisse den Vorrang vor dem »Recht des Einzelnen auf sein Datum« haben, versteht sich unter den beschriebenen Umständen im Grunde von selbst. Aber auch die **Einwilligung des Betroffenen** genügt – und zwar möglicherweise sogar dann, wenn sie von den Umständen nahegelegt oder durch ein Entgelt erkauft wird.[83] Im Rahmen gentechnisch relevanter Daten wurde lange Zeit entsprechend verfahren.[84] Niemand verbot also die Entwicklung von DNA-Testverfahren oder von Überwachungssoftware – um nur die beiden markantesten Beispiele zu nennen. Lediglich ihr Einsatz hängt von der Zustimmung des Betroffenen ab, soweit diese nicht, wie etwa bei der Rasterfahndung, durch eine Entscheidung des Gesetzgebers oder der Exekutive »ersetzt« wird. 13

Die »Offenheit« der technischen Entwicklung hat allerdings ihre Gefahren. Die Entstehung immer neuer, das ganze gesellschaftliche Leben durchdringender Systeme schafft »Sachzwänge«, denen sich der Gesetzgeber anpassen muss. Was mit enormen Kosten aufgebaut und eingerichtet wurde, lässt sich nicht mehr beseitigen – die wirtschaftliche wie die politische »Vernunft« sprächen dagegen. Man nimmt es deshalb z. B. hin, dass **Teile der Technik anfällig gegen Eingriffe von außen sind**. So hat die IT-Sicherheit bisher im Vergleich zum Datenschutz ein Schattendasein geführt.[85] Der Durchschnittsbürger akzeptiert es, dass Mitmenschen (selbst fühlt man sich meist nicht betroffen) nachhaltig überwacht werden, damit keine »Sicherheitsrisiken« entstehen. Ein erhebliches Stück Freiheit geht so verloren.[86] Ambivalent in ihren Wirkungen sind auch sehr viele andere technische Entwicklungen. Niemand wird es kritisieren, wenn der Einzelne seine genetischen **Dispositionen für bestimmte Krankheiten kennt** und deshalb vorsorglich den Kontakt mit einzelnen Risikofaktoren, etwa mit bestimmten 14

82 DVR 1982, S. 179ff.
83 Dazu insbesondere Simitis, in: Sokol (Hrsg.), Neue Instrumente im Datenschutz, S. 10ff. Zur Kommerzialisierung der Einwilligung s. insbesondere B. Buchner, DuD 2010, 39ff.
84 Weichert, DuD 2002, 133f.
85 S. aber nunmehr Kipker (Hrsg.), Cybersecurity, München 2020.
86 S. dazu bereits Roßnagel, in: ders. (Hrsg.), Freiheit im Griff, S. 9ff.; vgl. auch Lennartz, DuD 1989, S. 231ff.

Schadstoffen meidet.[87] Auf der anderen Seite verletzt es das Persönlichkeitsrecht, wenn jemand gegen seinen Willen mit einer entsprechenden Erkenntnis konfrontiert wird. Denkbar, ja naheliegend ist weiter die **Gefahr einer Diskriminierung**: Wer zur Gruppe von »Gen-Behinderten« gehört, die für bestimmte (oder viele?) Krankheiten anfällig sind und deshalb für bestimmte (viele?) Tätigkeiten nicht in Betracht kommen, wird bei einer Bewerbung schlechte Karten haben. Es wäre deshalb sicher zu kurz gegriffen, wollte man nur die positiven, die Lebensqualität erhöhenden Folgen oder nur die negativen, den Einzelnen zum Objekt machenden Auswirkungen sehen. Notwendig ist vielmehr ein differenzierter Umgang des Rechts und der Politik mit der Technik.

14a In einem spezifischen Teil staatlicher Tätigkeit unterscheidet sich der Umgang mit Technik von dem sonst üblichen Muster: Bei der **Strafverfolgung** wird der **Einsatz neuer technischer Mittel** von vorneherein **an** bestimmte gesetzlich festgelegte **Voraussetzungen gebunden**. Wie diese beschaffen sind, ist Gegenstand politischer Auseinandersetzungen; das Stichwort »Lauschangriff« mag hier für viele andere stehen.[88] Speicheltest, Rasterfahndung und Abhören von Telefongesprächen sind nur zulässig, wenn es um **bestimmte schwere Delikte** geht und wenn es – so die verfahrensrechtliche Absicherung – eine entsprechende Entscheidung durch ein **Gericht oder** eine **Staatsanwaltschaft** gibt. An beidem fehlt es, wenn wegen des Verdachts der üblen Nachrede eine heimliche gentechnische Untersuchung durchgeführt wird[89] oder wenn die Kontobewegungen bei über 160 000 Beschäftigten mit denen von 80 000 Geschäftspartnern abgeglichen werden.[90] Nachdenklich stimmt es auch, wenn man sich die in § 110a StPO festgelegten Voraussetzungen für den **Einsatz verdeckter Ermittler** vor Augen führt: Ist es nicht eine »verdeckte Ermittlung«, wenn sich Detektive als Praktikanten ausgeben und persönliche Gespräche führen, deren Inhalt sie dann dem Arbeitgeber als ihrem Auftraggeber übermitteln?[91] Nach § 110a StPO muss es um unerlaubten Drogen- und Waffenhandel, um Falschgeldproduktion oder um Staatsschutzdelikte gehen; die Taten müssen außerdem gewerbs- oder gewohnheitsmäßig oder »bandenmäßig« begangen werden. War bei Edeka wirklich die Drogenmafia zugange? Und warum hat man dann nicht gleich den Staatsanwalt eingeschaltet? Die Fragen sollen keinen völlig unangemessenen Verdacht zum Ausdruck bringen, sondern verweisen nur auf einen **Wertungswiderspruch**: Soll der private Arbeitgeber das, was dem Staat gewissermaßen nur in höchster Not erlaubt ist, schon dann tun können, wenn er befürchtet, es könne ihm ein Stück Käse oder eine Schachtel Zigaretten abhandengekommen sein?

15 Es ist nicht Aufgabe der folgenden Untersuchung, das Thema »Techniksteuerung durch Recht« insgesamt zu behandeln. Vielmehr geht es um ein begrenzteres, aber immer wichtiger werdendes Untersuchungsfeld: Wie wirken sich Informa-

87 Pieper, § 11 ArbSchG Rn. 7a.
88 Dazu etwa B. Hirsch, DuD 2008, 87 ff. und insbes. DuD 2009, 33 ff.
89 S. den Fall oben Rn. 1.
90 S. den Fall oben Rn. 2g.
91 S. den Fall oben Rn. 2c.

tions- und Gentechnologien auf die Kontrollmöglichkeiten aus, die dem Arbeitgeber zur Verfügung stehen? Dass die technischen Voraussetzungen vorhanden sind, den »Großen Bruder« im Betrieb zu installieren, unterliegt nach dem bisher Gesagten keinem Zweifel. Doch gibt es offenkundig rechtliche, soziale, vielleicht auch wirtschaftliche Gründe, die das Unerträgliche verhindern können. Deshalb soll zunächst auf das spezifisch arbeitsrechtliche Instrumentarium eingegangen werden, das die Technikfolgen möglicherweise beeinflusst. Später werden uns dann weitere Fragen interessieren, zu denen auch das Problem gehört, inwieweit das Strafprozessrecht evtl. Maßstäbe für Konflikte im Arbeitsleben zu setzen vermag.

IV. Technikbewältigung im Arbeitsrecht?

An sich sind die Normen des Arbeitsrechts dem bürgerlich-liberalen Recht auf den ersten Blick gleichfalls nur übergestülpt; der Arbeitsvertrag wird von den Regeln über den Dienstvertrag nach den §§ 611 ff. BGB nur »miterfasst«, trotz des seit 1. 4. 2017 geltenden § 611a BGB bleibt er ein Unterfall des Dienstvertrags.[92] 16

Beispiel:
Am deutlichsten wird dies dann, wenn »dereguliert« wird, wenn arbeitsrechtliche Schutznormen abgebaut werden. Spricht man der Gewerkschaft das Zutrittsrecht zu kirchlichen Krankenhäusern ab,[93] kommt allein das aus dem Besitz abgeleitete Hausrecht des Arbeitgebers zum Tragen. Ist Teilzeitarbeit in beliebiger Form zulässig, schneidert sich die Arbeitgeberseite das jeweils passende Vertragsmodell zusammen (dem sich der Arbeitsuchende unterwerfen muss).

Auch das »technische Sicherheitsrecht« folgt in seiner Struktur demselben Muster. Unfallverhütungsvorschriften und andere Bestimmungen des Arbeitsschutzes wollen Leben und Gesundheit der Beschäftigten schützen, sie wollen Randkorrekturen vornehmen, nicht aber die Richtung der Entwicklung verändern. Immerhin ist durch das Arbeitsschutzgesetz die im alten § 120a GewO enthaltene Einschränkung weggefallen, wonach Leben und Gesundheit nur insoweit zu schützen waren, wie es die »Natur des Betriebes« gestattete. 17

Dennoch gehen die Uhren im Arbeitsrecht anders. Der entscheidende Unterschied liegt (vereinfacht gesagt) in der **Übertragung der Vertragsfreiheit auf die kollektive Ebene**. Durch Tarifvertrag (hinter dem der Streik steht) und durch Betriebsvereinbarung (hinter der die Zwangsschlichtung durch die Einigungsstelle steht) können die Interessen der abhängig Beschäftigten unmittelbar zur 18

92 Zu einem historischen »Schichtenmodell« des Arbeitsrechts siehe Giugni, Giornale del Diritto di Lavoro e delle Relazioni Industriali 1982, S. 380.

93 BVerfG 17. 2. 1981 – 2 BvR 384/78, BVerfGE 57, S. 220 ff.; die Entscheidung ist inzwischen überholt. Dazu Däubler, Gewerkschaftsrechte, Rn. 781 ff.

Geltung gebracht und in gewissem Umfang durchgesetzt werden. Entsprechende Möglichkeiten fehlen anderen potenziellen »Opfern« der Entwicklung: Verbraucher haben nur das stumpfe Schwert der »Kaufenthaltung«. Anlieger können wegen übermäßiger Gefährdung oder vermeidbarer Emissionen beim Verwaltungsgericht klagen und eine Bürgerinitiative gründen, der meist nur wenig Druckpotenzial zur Verfügung steht. Dies bedeutet, dass das Arbeitsrecht Instrumente bereithält, auch die Technik verstärkt zu gestalten, vielleicht sogar ihre Richtung zu verändern. Wie sind sie bisher genutzt worden?

19 Auch im Arbeitsrecht ist man grundsätzlich nicht über den Bereich der **Folgenbewältigung** hinausgekommen.[94] Der Technikeinsatz selbst, die Bestimmung der Grenze zwischen erlaubter und nicht erlaubter Entwicklung und Nutzung von Technik, wird nur ganz ausnahmsweise erfasst.

20 Zunächst fällt auf, dass die Technikfolgen in sehr unterschiedlichem Maße aufgefangen und geregelt werden.[95] Wird das bestehende Arbeitsvolumen reduziert und **fallen** deshalb **Arbeitsplätze weg**, so gibt es – von der schwer zu erkämpfenden Arbeitszeitverkürzung einmal abgesehen – im Grunde kein wirksames Gegenmittel. Als erste verlieren Leiharbeiter und Soloselbstständige ihren Einsatzbereich; weder Betriebsrat noch Gewerkschaft können ihnen helfen.[96] Tarifpolitik ist darauf beschränkt, eine allzu ungleiche Verteilung der Beschäftigungsrisiken innerhalb der Stammbelegschaft zu verhindern, etwa älteren Arbeitnehmern mit längerer Betriebszugehörigkeit einen verstärkten Kündigungsschutz zu sichern. Der Betriebsrat kann mit dem Arbeitgeber über einen Interessenausgleich verhandeln, diesen jedoch nicht erzwingen. Der Mitbestimmung unterliegt allein der Sozialplan, der die drohenden wirtschaftlichen Nachteile für die, unbefristet beschäftigte, Kernbelegschaft »ausgleichen oder mildern« soll (§ 112 Abs. 1 BetrVG). In jüngerer Zeit ist der »Tarifsozialplan« hinzugekommen, der in Einzelfällen den Personalabbau erheblich verteuert hat.

21 Die Digitalisierung kann zu erheblichen **Veränderungen der Arbeitsbedingungen** führen.[97] Forderungen nach »guter Arbeit« können nicht mehr nur an der äußeren Gestalt von Betrieb und Dienststelle ansetzen; sie müssen die Technologie einschließlich der verwendeten Programme und der Kommunikationsformen einbeziehen.[98]

22 Einen **vergleichsweise geringen Schutz** genießt das von neuen Technologien bedrohte **Rechtsgut der Qualifikation**.[99] Das geltende Recht hat diesen »Wert«,

94 Überblick bereits bei Bull, CR 1988, S. 923. Dass dies auch für die wirtschaftliche Entwicklung gilt, hat Wolter (AuR 2008, 325) überzeugend herausgearbeitet. Inzwischen hat sich die Entwicklung nicht geändert.

95 Überblick bei Klebe, in: Däubler/Klebe/Wedde, § 87 Rn. 154ff.

96 Dass der Betriebsrat die »Randbelegschaften« faktisch nicht vertritt, ist in NZA 2019, 1601 herausgearbeitet.

97 Die wichtigsten sind genannt und auf ihre rechtliche Bewältigung hin untersucht bei Däubler, Digitalisierung und Arbeitsrecht, §§ 4 bis 8.

98 Zur »Software-Ergonomie« s. Martin, CuA 3/2014, S. 4 sowie Heilmann, CuA 6/2013, S. 15. Vgl. bereits Becker-Töpfer, AiB 1988, S. 147ff.

99 S. Käufer, Weiterbildung im Arbeitsverhältnis, 2001, und die Darstellungen am Beispiel CAD bei Latendorf, CR 1988, S. 664.

in dem sich eine Ausbildung von 10 Jahren und eine noch längere Berufserfahrung niederschlagen können, mit keinerlei spezifischem Schutz versehen. Dies bedeutet, dass mangelnde Nachfrage die Früchte eines halben Lebens zunichte machen kann. Manche Tarifverträge versuchen, wenigstens die Fortsetzung der Tätigkeit an den umgestalteten Arbeitsplätzen zu sichern oder den Arbeitgeber zu einer Umschulung zu verpflichten.

Der Schwerpunkt der »Bewältigungsstrategien« liegt auf dem **Persönlichkeitsschutz**: Die Informationstechnologien sollen nicht dazu führen, dass der Einzelne zum **»Überwachungsobjekt«** wird. Diesem Teil der Technikfolgen ist die vorliegende Untersuchung gewidmet.[100] 23

> **Beispiel:**
> Damit ist sicherlich nur ein Teil der auf den Einzelnen im Betrieb zukommenden Gefahren angesprochen: Gesundheitsschäden etwa oder Arbeitshetze werden herkömmlicherweise nicht als Verletzungen des Persönlichkeitsrechts gewertet. Dies hängt damit zusammen, dass auch das Arbeitsrecht in gewissem Umfang noch immer dem traditionellen Menschenbild folgt, wonach »Persönlichkeitsentfaltung« als geistiger Prozess begriffen wird, die realen Grundlagen für die Lebens- und Handlungschancen des Einzelnen jedoch ausgeblendet bleiben.[101] Dieses gravierende Defizit sollte uns jedoch nicht dazu verleiten, den Persönlichkeitsschutz in seiner heutigen Form gering zu schätzen und als »Luxusproblem« abzutun. Gerade die »Datenskandale« haben deutlich gemacht, wie sehr die Lebensqualität vieler Mitmenschen unter solchen Erscheinungen leiden kann.

Die weiteren Technikfolgen sind überdies inzwischen Gegenstand der sehr ausgedehnten Diskussion über Digitalisierung.[102] Auch wird der traditionelle Ansatz konzeptionell mit der Vorstellung von »Privacy by Design« überschritten: Die Gestaltung der Technik soll so beschaffen sein, dass der Schutz des Einzelnen von vorneherein gewahrt bleibt. Was technisch nicht möglich ist, muss durch Datenschutzgesetze nicht mehr verboten werden.[103]

100 Zu weiteren Fragen des Verhältnisses von Informationstechnologien und Arbeitsrecht s. auch Däubler, CR 2005, S. 767ff. und Digitalisierung und Arbeitsrecht, 7. Aufl. 2020.
101 Näher dazu Däubler, Arbeitsrecht 2, Rn. 594ff.
102 Dazu Krause, 71. DJT; Däubler, SR, Sonderheft Juli 2016, S. 2ff.
103 Richter, DuD 2016, 89.