Aljoscha Dietrich, Christian K. Bosse, Hartmut Schmitt

Kontrolle und Überwachung von Beschäftigten

Die Digitalisierung am Arbeitsplatz gewinnt immer weiter an Bedeutung und hat Auswirkungen auf nahezu alle Arbeitsbereiche. Dieser Trend wird jedoch flankiert durch die publik gewordenen Datenschutzskandale der letzten Jahre und kann daher bei den Beschäftigten ein grundsätzliches Unbehagen auslösen. Die zunehmende Nutzung der digitalen Möglichkeiten am Arbeitsplatz folgt jedoch auch berechtigten Interessen der Arbeitgeber, welche denen der Beschäftigten nicht zwangsläufig zuwiderlaufen müssen. Dieser Beitrag soll einen Überblick und eine Einordnung von Werkzeugen zur Kontrolle bzw. Überwachung von Beschäftigten geben, den rechtlichen Rahmen des Erlaubten aufzeigen und diese Thematik zudem aus der Sicht der Arbeitswissenschaft beleuchten.

1 Motivation

Die voranschreitende Digitalisierung verändert die Arbeitswelt auf vielfältige Weise: Neue Geschäftsmodelle und Wettbewerbsstrukturen entstehen, die Organisation der Produktions- und Arbeitsprozesse wandelt sich ebenso wie sich die Gestaltung der Arbeitsplätze, Arbeitsinhalte und Arbeitsweisen ändert. Die neuen Gestaltungsmöglichkeiten und Freiheiten, die mit der Digitalisierung und zunehmenden Vernetzung einhergehen, werden von vielen Unternehmen bereitwillig genutzt. Vor dem Hintergrund der COVID-19-Pandemie war es vielen Unternehmen durch die Digitalisierung von Prozessen überhaupt erst möglich, den Geschäftsbetrieb aufrecht zu erhalten, beispielsweise mit der Verlagerung zahlreicher Tätigkeiten ins Homeoffice.

Auch viele Beschäftigte bewerten die Digitalisierung positiv.[1] Sie erhoffen sich durch flexible Arbeitsformen und Homeoffice-Angebote mehr Freiheit, Autonomie und nicht zuletzt bessere Möglichkeiten zur Herstellung einer guten Work-Life-Balance. Allerdings sind ebenso die Kehrseiten neuer flexibler Arbeitsformen durch die Forschung belegt: die Entgrenzung von Arbeit und Privatleben sowie die Verfügbarkeitskultur[2] in vielen Unternehmen führen zu neuen Belastungen. Durch Selbstausbeutung,[3] zu der insbesondere Höherqualifizierte neigen, drohen Gesundheitsgefährdungen. Zudem besteht die Gefahr, dass Regelungen des Arbeitsschutzes, die für „klassische" Arbeitsplätze längst etabliert sind, durch die Flexibilisierung von Arbeitsort und Arbeitszeiten aufgeweicht oder ausgehebelt werden.

Digitalisierung als Gestaltungsaufgabe betrifft auch das Thema Datenschutz, in der Arbeitswelt insbesondere den Beschäftigtendatenschutz. Leistungs- und Verhaltenskontrollen der Beschäftigten werden durch die Digitalisierung erheblich erleichtert. Insbesondere Cloud-Technologien eröffnen neue Möglich-

Aljoscha Dietrich

Wissenschaftlicher Mitarbeiter am Lehrstuhl für Rechtsinformatik an der Universität des Saarlandes.

E-Mail: aljoscha.dietrich@uni-saarland.de

Christian K. Bosse

Wissenschaftlicher Mitarbeiter am Institut für Technologie und Arbeit e.V. an der Technischen Universität Kaiserslautern.

E-Mail: christian.bosse@ita-kl.de

Hartmut Schmitt

Koordination der Forschungsprojekte des saarländischen Experten für Soft- und Hardwarelösungen HK Business Solutions GmbH.

E-Mail: hartmut.schmitt@hk-bs.de

1 *Klammer*, Digitalisierung als Gestaltungsaufgabe, in: Wirtschaftsdienst, 97. Jahrgang, Heft 7, S. 459 ff., Hamburg 2017.

2 Bundesregierung, Neue Wege – Gleiche Chancen. Gleichstellung von Frauen und Männern im Lebensverlauf. Erster Gleichstellungsbericht, Bundestags-Drucksache, Nr. 17/6240, Berlin 2011, S. 237.

3 Böckler Impuls, Freiheit zur Selbstausbeutung, Ausgabe 15/2015, Hans-Böckler-Stiftung, Düsseldorf 2015, S. 2.

keiten der Vergleichbarkeit und Auswertbarkeit von Arbeit, interne und externe Rankings erhöhen den Konkurrenz- und Leistungsdruck.[4] Ohne wirksamen Datenschutz droht durch die neuen Techniken zur Überwachung und maschinellen Verhaltenskontrolle der „gläserne Beschäftigte" – eine Aussicht, die die Frage nach der Würde des Menschen aufwirft.[5]

Bei der Entwicklung neuer digitalisierter Arbeitsformen und Arbeitsplätze kommt es also darauf an, einen Ausgleich zwischen den Bedürfnissen der Beschäftigten und den betrieblichen Anforderungen zu schaffen. In diesem Artikel wollen wir daher in Abschnitt 2 zunächst einen Überblick über technische Verfahren schaffen, die zur Überwachung am Computerarbeitsplatz geeignet sind bzw. genutzt werden. In Abschnitt 3 beschreiben wir die rechtlichen Anforderungen, die bei der Überwachung von Beschäftigen bestehen. In Abschnitt 4 beleuchten wir die Thematik aus Sicht der Arbeitswissenschaft, bevor wir den Beitrag in Abschnitt 5 mit einem Fazit und Ausblick abschließen.

2 Überblick über technische Verfahren

Es lassen sich zahlreiche Methoden und Techniken zur Kontrolle und Überwachung von Beschäftigten identifizieren. Teile davon, etwa die Videoüberwachung, wurden durch die Rechtsprechung intensiv beleuchtet. Andere Methoden kommen prinzipiell völlig ohne Technologie aus, beispielsweise wenn auf die Dienste von Privatdetektiven[6] zurückgegriffen wird. Unser Untersuchungsschwerpunkt soll jedoch auf der technologiegestützten Überwachung von Beschäftigten liegen, deren Haupttätigkeit an Computern in Büro- oder Heimarbeitsplätzen ausgeführt wird. Zielobjekt der Überwachungs- und Kontrollmaßnahmen sollen ihre Tätigkeiten am Computer und die hierbei anfallenden Daten sein. Aus diesem Grund werden andere Überwachungsmethoden,[7] welche sich nicht explizit auf den beschriebenen Computerarbeitsplatz beziehen, bewusst ausgeklammert.

Wir konnten insgesamt fünf verschiedene Kategorien entsprechender Überwachungssysteme identifizieren, welche im Folgenden kurz dargestellt werden.

2.1 Rating

Rating hat im Internet bereits eine hohe Popularität gewonnen: E-Commerce ist kaum denkbar ohne die Nutzerbewertungen von Produkten oder ohne die gegenseitige Bewertung von Käufer und Verkäufer. Bewertungen schaffen in diesen Bereichen Vertrauen und Orientierung. Dieselbe Methodik kommt nun auch vermehrt in der Arbeitswelt als Evaluierungs- und Kontrollinstrument unter dem Stichwort „algorithmisches Management" zum Einsatz.

Besondere Aufmerksamkeit erregte in Deutschland der Einsatz der Software „Zonar" bei dem Versandhändler Zalando aus Berlin.[8] Diese Software ist für den Office-Bereich konzipiert, die Hauptfunktionalität basiert auf sogenanntem horizontalem Worker-Coworker-Rating, also der gegenseitigen Bewertung der Beschäftigten. Diese Bewertungen werden dann für die Klassifizierung in Low-, Good- und Top-Performer genutzt, welche schließlich in Gehalts- und Aufstiegsentscheidungen einfließen.[9]

Bei dieser Art von Management- bzw. Evaluierungs-Software handelt es sich in der Regel um konzernspezifische Eigenentwicklungen, andere populäre Pendants sind Amazons „Anytime Feedback Tool"[10] und Googles „re:Work"[11].

2.2 People Analytics

People-Analytics-Techniken erlauben es, auf der Basis von aggregierten Daten aus dem Personalwesen, die gegebenenfalls mit anderen Unternehmensdaten angereichert werden, Verhaltensvorhersagen zu treffen oder Zukunftsszenarien zu entwickeln. Bereiche, in denen diese Form der Analytik angewendet werden kann, sind beispielsweise Recruiting (z. B. Eignung für bestimmte Aufgaben, Wechselbereitschaft), Mitarbeiterentwicklung und Mitarbeiterführung. Im Bereich Zusammenarbeit bzw. interne Kommunikation kann beispielsweise anhand der Metadaten (Empfänger, Betreff, Route der E-Mails u. ä.) untersucht werden, wie stark einzelne Unternehmensbereiche miteinander vernetzt sind, in welchen Unternehmensbereichen Meinungsbildner bzw. Experten zu finden sind und wie die Stimmung im Unternehmen ist.

Neben einschlägigen HR-Produkten großer Hersteller (z. B. IBM Watson Talent Insights, SAP Workforce Analytics, Oracle Cloud HCM) gibt es eine Vielzahl von Programmen spezialisierter Hersteller. Bekanntheit erlangten auch einige People-Analytics-Projekte, z. B. die Oxygen-Studie[12], die bei Google die Eigenschaften guter Führungskräfte in Technologieunternehmen analysierte.

2.3 Überwachungssoftware

Diese Kategorie von Software ist gezielt für die Überwachung und Ausspähung von Beschäftigten entwickelt worden und wird auch entsprechend beworben. Die Software enthält häufig Funktionen, um eine automatische und differenzierte Zeiterfassung durchzuführen, beispielsweise, wie lange mit welchem Programm gearbeitet wurde, oft ergänzt durch regelmäßige Screenshots, welche nachvollziehbar machen, welche Informationen auf dem Bildschirm des Beschäftigten dargestellt wurden. Oft werden auch alle Tastatureingaben mithilfe sogenannter Keylogger erfasst und gespeichert. In der Regel sind Überwachungsprogramme so konzipiert, dass sie unbemerkt von den betroffenen Beschäftigten laufen. Produkte aus dieser Kategorie sind beispielsweise ActivTrak, InterGuard, Time Doctor und VeriClock. Die Funktio-

4 *Jürgens/Hoffmann/Schildmann*, Arbeit transformieren! Denkanstöße der Kommission Arbeit der Zukunft, Forschung aus der Hans-Böckler-Stiftung Band 189, Bielefeld 2017, S. 162.

5 *Jürgens et al*., a. a. O., S.10.

6 Die Ermittlungsarbeit von Privatdetektiven wird in der Praxis wohl auch kaum ohne Technik auskommen, gemeint ist hier jedoch, dass zunächst einmal menschliche Beobachter zum Einsatz kommen.

7 Hier sei beispielsweise an die bereits genannte Videoüberwachung oder die Standortüberwachung per GPS oder auch RFID zu denken. Diese Liste ließe sich noch deutlich erweitern.

8 Zeit Online, Datenschutzbehörde prüft Mitarbeitersoftware von Zalando, https://www.zeit.de/arbeit/2019-11/zonar-zalando-mitarbeiter-scoring-software (letzter Abruf 19.10.2020).

9 Vgl. *Staab/Geschke*, Ratings als Arbeitspolitisches Konfliktfeld, Hans Böckler Stiftung 2020, 10.

10 Vgl. *Knator/Streidfeld*, Inside Amazon: Wrestling Big Ideas in a Bruising Workplace, The New York Times 2015: https://www.nytimes.com/2015/08/16/technology/inside-amazon-wrestling-big-ideas-in-a-bruising-workplace.html?_r=0 (letzter Abruf 19.10.2020).

11 https://rework.withgoogle.com (letzter Abruf 19.10.2020).

12 *Garvin*, How Google Sold Its Engineers on Management, in Harvard Business Review, December 2013, Boston 2013, S. 75-82.

nalität gleicht häufig der von Schadsoftware bzw. Malware, welche von Kriminellen eingesetzt wird, um beispielsweise Passwörter oder Kreditkarteninformationen auszuspähen.

2.4 Arbeitsplatzanalyse

Mit Programmen aus dieser Kategorie ist es möglich, die Arbeitsweise und das berufliche bzw. private Netzwerk der Beschäftigten zu analysieren: Hierdurch – so werden die Produkte beworben – ist es möglich, Verbesserungspotenziale zu erkennen und Arbeitsroutinen anzupassen

In gängigen cloudbasierten Office-Programmen, wie Microsoft Office 365 oder G Suite kann bereits mit den Standardfunktionen die Kontoaktivität der Nutzer ausgewertet werden. Tools mit erweiterten Analysefunktionen erlauben es, sämtliche Aktivitäten der Nutzer in einem Dashboard nachzuverfolgen, so dass eine detaillierte, dauerhafte und nahezu lückenlose Auswertung des Verhaltens möglich ist.[13] Auf diese Weise kann zum einen jeder Beschäftigte selbst sein eigenes Tun analysieren (z. B. in Microsoft MyAnalytics). Zum anderen kann der Vorgesetzte Analysen auf Team-, Abteilungs- oder Unternehmensebene durchführen (z. B. mit Microsoft Workplace Analytics, Slack Analytik-Dashboard oder Zoho Analytics) und – da die Programme auf Optimierungspotenzial hinweisen – entsprechend reagieren.

2.5 Zweckentfremdete Software

Neben den beschriebenen Kategorien, die explizit entwickelt wurden, um Beschäftigte bzw. deren Arbeitsweise, Gewohnheiten und Vernetzung zu überwachen und zu bewerten, gibt es eine Reihe weiterer Softwarekategorien, die zwar eigentlich für andere Zwecke gedacht sind, aber auch im Bereich Kontrolle und Mitarbeiterüberwachung eingesetzt werden können.

In Zusammenhang mit der Corona-Pandemie hat diese zweckentfremdete Nutzung von Softwareprogrammen und -funktionen einen großen Auftrieb erfahren: viele Beschäftigte im Homeoffice, deren physische Anwesenheit nicht überprüfbar war, mussten so den Nachweis ihrer Arbeit bzw. Produktivität erbringen. Gängige Praktiken sind beispielsweise, dass der Zugriff auf Nachrichten in E-Mail- und Chatprogrammen gewährt werden muss, so dass der Vorgesetzte mitlesen kann, oder dass während des gesamten Arbeitstags eine Webcam mitläuft. Ebenfalls in diese Kategorie fällt der Einsatz von Videokonferenzen-Programmen, bei denen die Beschäftigten den Tag über eingeloggt bleiben müssen. Teilweise sind (oder waren) entsprechende Tools ausgestattet mit Attention-Tracking-Funktionen, mit denen nachverfolgt werden kann, ob ein Anwendungsfenster tatsächlich aktiv ist oder im Hintergrund abgelegt wurde.[14]

Zu nennen ist ferner das Monitoring im Bereich IT-Sicherheit, bei dem der Nutzer als Quasi-Sensor fungiert.[15] Eigentlich gedacht zur Erkennung von Anomalien, ermöglicht auch dies eine Auswertung der Benutzer-/Bedienprozesse, durchschnittlichen Bearbeitungszeiten u. ä.

13 DGB, Darum ist Microsoft Office 365 ein Fall für den Betriebsrat: https://www.dgb.de/-/nAI (letzter Abruf 19.10.2020).

14 Vgl. *Moorstedt*, In der Krise boomt auch die Überwachung durch den Chef, Süddeutsche Zeitung, 6.4.2020: https://www.sueddeutsche.de/digital/home-office-ueberwachung-tracking-chef-zoom-1.4868739 (letzter Abruf 19.10.2020).

15 Bundesamt für Sicherheit in der Informationstechnik, Hochverfügbarkeitskompendium, Band B, Kapitel 10: Überwachung, Bonn 2013, S. 18.

3 Rechtliche Einordnung und Bewertung

Nachdem im vorherigen Abschnitt eine Auswahl verschiedener Überwachungswerkzeuge vorgestellt wurde, soll im Folgenden die Frage erörtert werden, welche Überwachungsmaßnahmen durch den Arbeitgeber unter welchen Bedingungen in Deutschland zulässig sind.

3.1 Datenschutzrecht

Kontrolle und Überwachung sind Schwerpunktthemen des Beschäftigtendatenschutzes. Ein Arbeitgeber kann sich auf berechtigte Interessen berufen, die er mittels Überwachungsmaßnahmen durchsetzen kann. Beispielsweise ist es ihm erlaubt das Verhalten und die Arbeitsergebnisse seiner Beschäftigten zu kontrollieren.[16] Ein Arbeitgeber kann im Rahmen gesetzlicher Compliance-Anforderungen sogar zu Überwachungsmaßnahmen verpflichtet sein[17] und auch die Aufdeckung oder Verhinderung von Straftaten berechtigt ihn zu Kontrollmaßnahmen. Wie im vorherigen Abschnitt beschrieben, sind durch die fortschreitende Digitalisierung die Möglichkeiten zur Überwachung extrem gewachsen. Dem Arbeitgeber ist es nun möglich, die Arbeit ständig, detailliert und auch unbemerkt zu überwachen. Es stellt sich die Frage, wo die Grenze des Zulässigen liegt.

Die Einführung der Datenschutz-Grundverordnung (DSGVO) hatte zum Ziel, eine Harmonisierung des Datenschutzrechts in den einzelnen EU-Mitgliedsstaaten zu erreichen, sie gilt daher unmittelbar und geht widersprechenden nationalen Regelungen vor. Bezüglich des Beschäftigtendatenschutzes finden sich in der DSGVO jedoch keine bereichsspezifischen Regelungen und nur einzelne Vorgaben.[18] Den einzelnen Mitgliedsstaaten ist es durch die sogenannte Öffnungsklausel des Art. 88 DSGVO wiederum erlaubt, nationale bereichsspezifische Regelungen für den Beschäftigten-Kontext zu treffen.[19] Der Beschäftigtendatenschutz wurde demnach von der Vollharmonisierung ausgenommen, die Anforderungen der DSGVO gelten jedoch wohl in diesem Bereich zumindest als „Mindeststandard".[20]

3.2 Überwachung

Die Öffnungsklausel des Art. 88 Abs. 2 DSGVO sieht vor, dass die nationalen Vorschriften Maßnahmen zur Wahrung der Grundrechte der betroffenen Personen im Hinblick auf Überwachungssysteme am Arbeitsplatz umfassen.

Der deutsche Gesetzgeber hat von der Öffnungsklausel des Art. 88 DSGVO bisher nur eingeschränkt Gebrauch gemacht. Die deutschen bereichsspezifischen Regelungen finden sich in dem Bundesdatenschutzgesetz (BDSG) neuer Fassung (n.F.). Zum Beschäftigtendatenschutz gibt es allerdings nur sehr allgemeine Bestimmungen in § 26 BDSG n.F. Aufgrund dessen, dass die-

16 *König*, Beschäftigtendatenschutz in der Beraterpraxis, Rn. 64.

17 Vgl. etwa §§ 91 Abs. 2 AktG, 130 OWiG; *Riesenhuber*, BDSG § 26, in: Brink/Wolff (Hrsg.), BeckOK DatenschutzR, 32. Ed. 1.5.2020, Rn. 139.

18 Vgl. *Seifert*, Artikel 88, in: Simitis/Hornung/Spiecker (Hrsg.), Datenschutzrecht, 2019, Rn. 1.

19 Vgl. *Morsch*, Datenverarbeitung im Beschäftigungskontext – Zur Reichweite der Öffnungsklausel nach Art. 88 DSGVO, Baden-Baden 2019, S. 16 ff.; in diesem Kontext zu beachten ist auch Diskussion, ob die DSGVO hier Regelungen nach oben bzw. nach unten erlaubt, also ob die nationalen Vorschriften strengere oder lockere Vorgaben treffen dürfen, als allgemein in der DSGVO vorgesehen.

20 Vgl. *Seifert*, a. a. O., Rn. 1, Rn. 18 ff.

ser Paragraph weitgehend dem § 32 BDSG alter Fassung (a.F.) entspricht, ist davon auszugehen, dass sich die bestehende deutsche Rechtsprechung weiter anwenden lässt. Da der Beschäftigtendatenschutz auch zuvor nur allgemein geregelt war, entwickelte sich ein umfangreiches Richterrecht, welches viele Detailfragen näher ausführt.

Der deutsche Gesetzgeber ist der zuvor genannten Forderung auf Berücksichtigung von Überwachungssystemen[21] am Arbeitsplatz im Rahmen des § 26 BDSG n.F. nicht explizit nachgekommen. Aus § 26 Abs. 1 BDSG n.F. lässt sich jedoch eine Unterscheidung zwischen präventiver (S. 1) und repressiver Kontrolle zur Aufdeckung von Straftaten (S. 2) herauslesen. Nach bestehender Rechtsprechung des Bundesarbeitsgerichts (BAG)[22] ist bei einer erheblichen Pflichtverletzung, die jedoch keinen Straftatbestand erfüllt, ein Rückgriff auf S. 1 zulässig.[23]

Der (geplante) Einsatz von Überwachungs- oder Kontrollmaßnahmen verlangt eine Abwägung zwischen den verletzten Grundrechten der betroffenen Parteien. Sowohl Arbeitgeber als auch Arbeitnehmer können sich in diesem Kontext auf Grundrechte aus der EU-Grundrechtecharta (GRCh) bzw. dem deutschen Grundgesetz (GG) berufen: Der Arbeitnehmer auf sein Recht auf informationelle Selbstbestimmung[24] (Art. 7 GRCh bzw. Art. 1 und 2 GG) sowie einen angemessenen Datenschutz (Art. 8 GRCh), der Arbeitgeber auf sein Grundrecht auf unternehmerische Freiheit (Art. 16 GRCh bzw. Art. 12 Abs. 1 GG), das Eigentumsrecht (Art. 14 Abs. 1 und 2 GG) und die Vertragsfreiheit (Art 2 Abs. 1 GG).[25]

Für eine (auch heimliche) Überwachung ergeben sich aus der jüngeren BAG-Rechtsprechung[26] drei notwendige Voraussetzungen:

1. das Vorliegen eines einfachen[27] Verdachts auf eine Straftat oder schwere Pflichtverletzung des Arbeitnehmers,
2. die Erforderlichkeit der konkreten Verarbeitung als mildestes Mittel und
3. die Beachtung der Verhältnismäßigkeit unter Berücksichtigung der Interessen und verletzten Grundrechte der Betroffenen.[28]

Die Rechtsprechung des BAG bezieht sich noch auf das BDSG a.F., es ist jedoch – wie bereits erwähnt – davon auszugehen, dass diese übertragbar ist und daher weiterhin von Bestand ist.[29]

In jedem Fall verboten ist die sogenannte Totalüberwachung, da diese in unverhältnismäßiger Weise in das Grundrecht auf informationelle Selbstbestimmung eingreift.[30] Ein Beispiel für eine Totalüberwachung ist etwa der Einsatz einer Videokamera, welche das gesamte Arbeitsverhalten aufzeichnet und eine detaillierte Auswertung ermöglicht.[31] Zum Einsatz eines Keyloggers,[32] mit dem die private Internetnutzung eines Beschäftigten festgestellt werden kann, entschied das BAG, dass eine so eingriffsintensive Maßnahme nicht erforderlich sei. Eine Auswertung des Browserverlaufs hätte zu ähnlichen Erkenntnissen geführt und ein deutlich milderes Mittel zur Belegung der Pflichtverletzung dargestellt. Dennoch bedeutet dieses Urteil kein generelles Verbot von Keyloggern.[33]

3.3 Mitbestimmung des Betriebsrats

Wenn es um Kontrolle und Überwachung von Beschäftigten geht, steht auch der Arbeitsnehmervertretung eine wichtige Rolle zu. Der Betriebsrat hat nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) ein weitreichendes Mitbestimmungsrecht, wenn es im Betrieb zur Einführung von Technologien kommt, die dazu geeignet sind, die Mitarbeiter zu überwachen. Der Wortlaut des Gesetzes („die dazu bestimmt sind") legt zwar eine Überwachungsabsicht nahe, die Rechtsprechung[34] hat dies jedoch seit jeher als objektive Eignung ausgelegt. Bei der zunehmenden Digitalisierung der Arbeitswelt lässt sich § 87 Abs. 1 Nr. 6 BetrVG auf nahezu jede neue Technologie anwenden und gewährt somit dem Betriebsrat ein weitreichendes Mitspracherecht. Die jüngere Rechtsprechung des BAG[35] und LAG[36] übertrug diese Sichtweise auch auf den Betrieb von betrieblichen Facebook- und Twitter-Accounts, da sich über die Kommentarfunktionen Mitarbeiter bewerten lassen.[37] Die Literatur[38] übt an dieser extrem weiten Auslegung teils starke Kritik, eine Kursänderung ist jedoch nicht absehbar.[39]

Schwere Verletzungen des Datenschutzes sowie der Mitbestimmungsrechte können auch Beweisverwertungsverbote nach sich ziehen. Schwer bedeutet, dass beispielsweise das Persönlichkeitsrecht des Beschäftigten verletzt wurde und nicht etwa *nur* datenschutzrechtliche Informationspflichten.[40] Ähnliches gilt bei Verstößen gegen das Mitbestimmungsrecht.[41] Verletzungen gegen die Bestimmungen des Datenschutzrechts können auch zur Anwendung der strengen Sanktionen der DSGVO führen und neben Bußgeldern außerdem zu Schadensersatzforderungen führen.[42]

21 Ein Überwachungssystem kann wohl als eine automatisierte Überwachung verstanden werden, vgl. hierzu *Seifert*, a. a. O., Rn. 42.; nicht gemeint ist hingegen, wenn beispielsweise ein Vorgesetzter (regelmäßig) Strichproben durchführt, vgl. hierzu *Riesenhuber*, a. a. O., Rn. 91.

22 *BAG*, Vorgetäuschte Erkrankung und Konkurrenztätigkeit – Überwachung durch Detektiv, NZA 2017, 1179.

23 *Fuhlrott/Oltmanns*, Arbeitnehmerüberwachung und interne Ermittlungen im Lichte der Datenschutz-Grundverordnung, NZA 2019, 1105; vgl. *Däubler*, Gläserne Belegschafen, 8. Auflage, Frankfurt a. M. 2019, Rn. 253.

24 Erstmalig entwickelt im „Volkszählungsurteil", BVerfGE 65, 1, Urteil vom 15.12.1983.

25 Vgl. *Seifert,* a. a. O., Rn. 31-33, 133.

26 Vgl. BAG, Urteil vom 20.10.2016 – 2 AZR 395/15 = NJW 2017, 1193; BAG, Urteil vom 22.9.2016 – 2 AZR 848/15 = GWR 2017, 60; BAG, Urteil vom 27.7.2017 – 2 AZR 681/16 = BB 2017, 2682.

27 Vgl. *BAG*, Verdeckte Videoüberwachung wegen Verdachts der Begehung von Straftaten, NJW 2017, 1196.

28 Vgl. *Fuhlrott/Oltmanns*, a. a. O., 1106; vgl. auch *Seifert,* a. a. O., Rn. 57.

29 *Fuhlrott/*Oltmanns, a. a. O., 1110.

30 Vgl. *Kort*, Neuer Beschäftigtendatenschutz und Industrie 4.0, RdA 2018, 25.

31 Vgl. *Däubler*, Gläserne Belegschafen, a. a. O., Rn. 260a.

32 Siehe Abschnitt 2.3.

33 Vgl. *Fuhlrott*, Keylogger & Arbeitnehmerdatenschutz, NZA 2017, 1308.

34 Seit BAG NJW 1976, 261; vgl. auch *Zöllner*, Digitalisierungshemmer Betriebsrat?, in: Klawitter/Beck/Günther/Kleinert/Kontowicz/Seitz/Tölle/Tomas (Hrsg.), 9. Assistententagung im Arbeitsrecht, Baden-Baden 2020, S. 114.

35 BAG, Beschl. v. 13.12.2016 – 1 ABR 7/15; vgl. auch *Grimm/Kühne*, Mitbestimmung bei der Einrichtung und Betrieb einer Facebook-Seite, jM 2017, Heft 8, S. 330 – 333.

36 LAG Hamburg NZA-RR 2018, 655.

37 Vgl. *Zöllner*, a. a. O., 118.

38 Vgl. *Zöllner*, a. a. O., 116; *Krause*, Gutachten B zum 71. Deutschen Juristentag, 2016, S. 80; *Grimm/Kühne*, Mitbestimmung bei Einrichtung und Betrieb einer Facebook-Seite, jM 2017, 333.

39 Vgl. *Kort*, a. a. O., S. 32

40 Vgl. *Riesenhuber*, a. a. O., Rn. 190 ff.; *Kort*, a. a. O., S. 33.

41 Vgl. *Kort*, a. a. O., S. 26.

42 *Reiserer/Christ/Heinz*, Beschäftigten-Datenschutz und EU-Datenschutz-Grundverordnung, DStR 2018, 1503; *Wybitul/Brink/Albrecht*, Interview: Beschäftigtendatenschutz nach der DS-GVO, NZA 2018, 285.

3.4 Vermittlung zwischen den Interessen

Dem Arbeitgeber stellt sich die Frage, wie sich neue Werkzeuge (und auch Kontrollmaßnahmen) in einem Unternehmen einsetzen lassen, ohne dass diese gegen die Bestimmungen des Datenschutzes verstoßen oder am Betriebsrat scheitern. Teile der in Abschnitt 2 beschriebenen Technologien können durchaus auch vorteilhaft für die Beschäftigten sein. Zugleich gilt es, die Wettbewerbsfähigkeit des Unternehmens zu gewährleisten und sich gegenüber neuen Technologien nicht zu verschließen.

Allgemein gilt es, die DSGVO vollständig umzusetzen. Bei der Verarbeitung sind etwa die Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DSGVO zu befolgen. Kommt es zum Einsatz von Maßnahmen, die (auch) zur Überwachung und Kontrolle genutzt werden können, sind die Vorgaben der Rechtsprechung (vgl. Abschnitt 3.1) zu beachten.

Um potenzielle Probleme von vornherein zu vermeiden, sollten Datensparsamkeit und Datenschutz durch Technikgestaltung i. S. d. Art. 25 DSGVO beherzigt werden. Dies bedeutet grundsätzlich zu überlegen, ob es wirklich notwendig ist personenbezogene Daten zu verarbeiten, oder ob nicht genauso gut mit anonymisierten oder zumindest pseudonymisierten Daten die gleichen Erkenntnisse gewonnen werden könnten. So kann es bei Anwendungen aus dem Bereich People Analytics ausreichend sein, aggregierte Daten zu verarbeiten, beispielsweise auf Abteilungsebene statt auf Mitarbeiterebene.[43]

4 Arbeitswissenschaftliche Betrachtung

Aus arbeitswissenschaftlicher Perspektive gilt es, neben der technischen ebenso die organisationale und soziale Sphäre im Unternehmen sowie deren Wechselwirkungen untereinander zu betrachten.[44] Denn genau in diesem Zusammenwirken lässt sich die Differenzierung zwischen Kontrolle und Mitarbeiterüberwachung erkennen. Die Bereitstellung der vielfältigen Werkzeuge und technischen Verfahren im Kontext der digitalen Transformation der Arbeitswelt ist per se eine neutrale Aktion. Software und technische Lösungen werden für einen speziellen Zweck entwickelt, beispielsweise für eine schnelle und einfache Kommunikation im Unternehmen. Solche Softwarelösungen für eine kollaborative Zusammenarbeit oder zur Kommunikation lassen sich jedoch auch teilweise zweckentfremdet zur Überwachung und Kontrolle einsetzen. Dabei eröffnen insbesondere die Datenspuren, die bei jedem Einsatz digitaler Arbeitsmittel oder Softwarelösungen unweigerlich entstehen, gänzlich neue Dimensionen und Qualitäten an Auswertungsmöglichkeiten – unabhängig von der Frage der Zulässigkeit.[45] Um zu verstehen, warum digitale Werkzeuge häufig in Verbindung mit Kontroll- oder Überwachungsfunktionen eingesetzt werden, hilft der Blick über die technische Sphäre im Unternehmen hinaus.

Schon seit den frühen Zeiten der Industrialisierung ist die Kontrolle und Überwachung der Beschäftigten ein Anliegen der Arbeitgeber. Auch wenn sich seitdem – zuletzt durch die digitale Transformation – die Arbeitswelt gewandelt hat, ist das Bestreben der Arbeitgeber, die Produktivität ihrer Belegschaft durch Überwachung sicherzustellen, unverändert oder gar gestiegen. Dies belegt unter anderem der DGB-Index „Gute Arbeit". In dessen zugrundeliegender Befragung gab die Hälfte der teilnehmenden Erwerbstätigen an, die Überwachung und Kontrolle ihrer Arbeitsleistungen sei aufgrund der Digitalisierung gleichgeblieben. Weitere 46 % empfanden eine Zunahme.[46] Dieses subjektive Empfinden der Arbeitnehmer wird durch die steigende Nachfrage bei Anbietern von Überwachungssoftware, insbesondere seit dem Ausbruch der Corona-Pandemie bestätigt.[47] Trotz hoher rechtlicher Hürden in Deutschland seien laut eigenen Angaben auch deutsche Unternehmen Kunden des US-amerikanischen Start-ups Hubstaff, das Personalüberwachung über Zeiterfassungssoftware bietet.[48] Doch selbst wenn die Überwachung der Beschäftigten anhand ihrer Datenspuren erst durch den technischen Fortschritt derart umfassend möglich wird, kann die voranschreitende Digitalisierung nicht als Begründung gesehen werden. Vielmehr ist es die steigende Bereitschaft von Unternehmen auf organisationaler Ebene, auf die neuen technologischen Möglichkeiten zur Datenerfassung und -auswertung zurückzugreifen, um die Arbeitsleistung der Beschäftigten zu kontrollieren oder zu überwachen.

Neben der organisationalen muss zusätzlich aber auch die soziale Sphäre im Unternehmen betrachtet werden, wenn es um die Gründe bzw. den Ursprung für Mitarbeiterkontrolle bzw. -überwachung geht. Häufig wird seitens der Arbeitgeber ein potenzielles Fehlverhalten von einzelnen oder mehreren Arbeitnehmern vermutet. Beispielsweise gehen Führungskräfte davon aus, dass sich Beschäftigte im Homeoffice anderen Tätigkeiten widmen, anstatt ihrer Arbeit nachzugehen. Darin begründete Kontrollmaßnahmen entfalten jedoch nicht nur die intendierte Wirkung einer höheren Arbeitsleistung.[49] Häufige und insbesondere als unangemessen erachtete Kontrollen können unter anderem zu den folgend skizzierten negativen Auswirkungen führen:[50]

- In einer Unternehmenskultur des Misstrauens kann es aufgrund von unangebrachten Kontrollen zu einer psychologischen Abwehrreaktion, einer sogenannten Reaktanz, gegen-

43 Vgl. *Götz*, Big Data im Personalmanagement, Baden-Baden 2020, 87 ff.

44 Vgl. *Bosse/Hellge/Schröder/Dupont*, Digitalisierung im Mittelstand erfolgreich gestalten, in: Bosse/Zink (Hrsg.), Arbeit 4.0 im Mittelstand, Berlin 2019, S. 13-34.

45 Vgl. *Schwemmel/Wedder*, Alles unter Kontrolle? Arbeitspolitik und Arbeitsrecht in digitalen Zeiten, WISO-Diskurs 02, Bonn 2018, S. 28-32; *Hofstetter*, Das Ende der Demokratie: Wie die künstliche Intelligenz die Politik übernimmt und uns entmündigt, München 2016, S. 79.

46 Vgl. Institut DGB-Index „Gute Arbeit" (Hrsg.), Der Report 2016, Wie die Beschäftigten die Arbeitsbedingungen in Deutschland beurteilen, Themenschwerpunkt: Die Digitalisierung der Arbeitswelt – Eine Zwischenbilanz aus der Sicht der Beschäftigten, 2016, S. 13.

47 Vgl. *Moorstedt,* a. a. O.

48 Vgl. *Raidl/Tyborski*, Die digitale Überwachung: Wie Unternehmen ihre Mitarbeiter beschatten, Handelsblatt online, 24.6.2020, online verfügbar unter URL: https://www.handelsblatt.com/technik/digitale-revolution/digitale-revolution-die-digitale-ueberwachung-wie-unternehmen-ihre-mitarbeiter-beschatten/25917236.html (letzter Abruf 2.8.2020).

49 Vgl. *Enste/Grunewald/Kürten,* Vertrauenskultur als Wettbewerbsvorteil in digitalen Zeiten, IW-Trends 2/2018, S. 48-51.

50 Vgl. *Zumach/Weibel,* Vertrauenskultur. Vertrauen zieht Talente an, Personal Schweiz 2014: https://www.personal-schweiz.ch/experten-interviews/article/vertrauenskultur-vertrauen-zieht-talente-an/ (letzter Abruf 1.8.2020); *Laufer*, Vertrauensvolle Mitarbeiterführung, Hintergründe, Leitfäden, Lösungsvorschläge. Wiesbaden 2018; *Posé,* Trau schau wem, Vom Wesen einer Vertrauenskultur, Marketing-Börse 2015: https://www.marketing-boerse.de/Fachartikel/details/1514-Trau-schau-wem-vom-Wesen-einer-Vertrauenskultur/51718 (letzter Abruf 1.8.2020); SOEP – Sozio-oekonomisches Panel, Daten der Jahre 2001–2013, Berlin, Version 31: https://www.diw.de/de/diw_01.c.519355.de/soep_v31.html (letzter Abruf 1.8.2020).

über diesen Maßnahmen kommen, bei der die Beschäftigten ihre Arbeitsleistung senken. Daraufhin besteht die Gefahr, dass durch die negativen Ergebnisse häufigere oder strengere Kontrollen folgen und ein sich selbst verstärkender Kreislauf beginnt.
- Fehlendes Vertrauen in einer kontrollorientierten Unternehmenskultur kann unter anderem dazu führen, dass Fehler auf Kosten der Effizienz vermieden oder gar vertuscht werden.
- Ist die Häufigkeit der Kontrollen zu hoch oder fokussieren diese auf bereits langfristig etablierte Arbeitsprozesse und Verhaltensweisen, so können sie zu Verunsicherungen der Beschäftigten und einer sinkenden Offenheit für innovative Neuerungen führen.
- Häufige und strenge Kontrollen können zu vermehrten Konflikten mit Führungskräften führen, wodurch mittelfristig die individuelle Arbeitszufriedenheit und -leistung sinkt.

Auch wenn es neben dem Vorhandensein von strengen Regularien und häufigen Kontrollen viele weitere Faktoren gibt, die sich negativ auf die Arbeitszufriedenheit und -leistung auswirken können, ist der positive Einfluss einer vertrauensvollen Unternehmens- und Führungskultur unumstritten. So fördert Vertrauen unter anderem die Motivation und Leistungsbereitschaft, das kooperative Verhalten und die Zusammenarbeit, die Offenheit gegenüber Neuem sowie die Kreativität und Lernbereitschaft der Beschäftigten.[51] All dies sind erfolgskritische Faktoren, will ein Unternehmen in einem heutigen Unternehmensumfeld, das von Volatilität, Unsicherheit, Komplexität und Mehrdeutigkeit geprägt ist, bestehen. Vertrauen ist demnach ein wichtiger Bestandteil von einer erfolgreichen Führung in der digitalen Transformation, mit der wir erneut an die technische Sphäre der Organisation anknüpfen.

Die aufgezeigten Zusammenhänge zwischen der technischen, organisationalen und sozialen Sphäre im Unternehmen verdeutlichen, wie komplex die Wirkzusammenhänge sind, die beim – ggf. zweckentfremdeten – Einsatz von digitalen Lösungen zur Kontrolle oder Überwachung von Beschäftigten zu betrachten sind. Soll ein solches Vorgehen verhindert werden, reicht beispielsweise ein Veto des Betriebsrates bei der Einführung einer entsprechenden technischen Lösung zur Beschäftigtenkontrolle in der Regel nicht aus. Denn existiert auf der sozialen Ebene eine von Misstrauen geprägte Kultur, wird die Führungskraft andere Wege finden, die Beschäftigten zu überwachen – zum Beispiel durch den zweckentfremdeten Einsatz anderer digitaler Lösungen.

Abschließend lässt sich festhalten, dass sich eine etablierte Vertrauenskultur, wie verschiedene Studien zeigen, zwar positiv im Unternehmen auswirkt, jedoch auf Kontrollen im Arbeitsalltag nicht gänzlich verzichtet werden kann. Beispielsweise bedingen gesetzliche Regelungen spezifische Kontrollen, unter anderem bei der Einhaltung von Arbeitszeiten und Ruhephasen insbesondere im Homeoffice. Darüber hinaus kann es Beschäftigte geben, die ein gewisses Maß an Kontrolle sogar einfordern, beispielsweise, um keine Verantwortung übernehmen zu müssen. Grundlegend sollte aber immer beachtet werden, dass die Kontrollmaßnahmen angemessen und fair erfolgen sowie offen und vertrauensvoll zu kommunizieren sind.

5 Fazit und Ausblick

Kontrolle und Überwachung spielen schon seit langer Zeit eine große Rolle im Arbeitsleben. Seit es zum vermehrten Einsatz und zur stärkeren Vernetzung von IT-Systemen kommt, nehmen die Möglichkeiten jedoch rasant zu. Nach aus heutiger Sicht harmlosen Anfängen in den 1970er Jahren ist spätestens mit der Digitalisierung eine enorme Beschleunigung und Eingriffstiefe festzustellen. Die COVID-19-Pandemie ist hier als weiterer Treiber auszumachen. Schon jetzt ist es möglich, jeden Mausklick eines Beschäftigten am Computerarbeitsplatz zu überwachen. In naher Zukunft kommen noch weitere eingriffsintensive, aber nahezu unsichtbare Mittel hinzu, beispielsweise Automationssysteme für Licht und Klimatechnik, die neben Komfort und Energiesparfunktionen auch Anwesenheits- und Bewegungsprofile ermöglichen.[52] Auch Wearables in Form von Smartwatches u. Ä. finden eine immer weitere Verbreitung. Diese können Vitalfunktionen überwachen und frühzeitig Gesundheitsprobleme identifizieren.[53] Dies kann zur Fürsorge, aber auch zur Identifikation von Kündigungskandidaten genutzt werden. Mit der sogenannten vernetzten Produktion bzw. Industrie 4.0[54] entstehen weitere potenzielle Überwachungsinstrumente, die die Beschäftigen in der Fertigung betreffen. War bisher eine Kamera notwendig, um jeden physischen Arbeitsschritt zu überwachen, ist dies zukünftig ein Nebenprodukt der „vernetzten Fabrik".

Bei all diesen aus Datenschutzsicht wenig schönen Aussichten fällt jedoch auf, dass sich den Gefahren mit den bestehenden rechtlichen Werkzeugen wohl gut begegnen lässt. Die durch die deutsche Rechtsprechung entwickelten Vorgaben sind in der Regel technikneutral und lassen sich daher auch gut auf zukünftige Entwicklungen übertragen, der Kern liegt im Ausgleich der Grundrechte. Wünschenswert wäre jedoch, dass der deutsche Gesetzgeber mit einer detaillierten bereichsspezifischen Regelung für weitere Klarheit sorgt, insbesondere auch zu Überwachungssystemen am Arbeitsplatz. Bei aller Kritik und Vorsicht sollte jedoch nicht vergessen werden, dass in neuen Technologien auch viele Chancen für die Beschäftigen liegen und der Arbeitgeber in vielen Fällen zur Kontrolle berechtigt bzw. verpflichtet ist. Das Datenschutzrecht (und auch dessen Sanktionsmöglichkeiten) stößt im Idealfall eine tiefere Diskussion im Betrieb an, wie sich Kontroll- und Überwachungsmaßnahmen möglichst wenig eingriffsintensiv gestalten lassen, ganz im Sinne des Interessensausgleichs. Hierbei sind die Beschäftigten bzw. ihre Vertreter ebenfalls mit einzubinden, nicht nur aus rechtlicher Verpflichtung, sondern ebenso aus den Erkenntnissen der Arbeitswissenschaft, um eine Vertrauenskultur im Unternehmen zu etablieren.

51 Vgl. *Rump/Eilers*, Kontrolle ist gut, Vertrauen ist besser!?, in: Rump/Eilers (Hrsg.), Die vierte Dimension der Digitalisierung, Berlin, Heidelberg 2019; *Blank,* Vertrauenskultur, Voraussetzung für Zukunftsfähigkeit von Unternehmen, Wiesbaden 2011; *Pribilla*, Führung in virtuellen Unternehmen, in: Albach/Specht/Wildemann (Hrsg.), Virtuelle Unternehmen, in: Zeitschrift für Betriebswirtschaft, 2. Jg. 2000, S. 1–12.

52 Vgl. *Ruoxi* et al., Privacy-enhanced architecture for occupancy-based HVAC control. 2017 ACM/IEEE 8th international conference on cyber-physical systems (ICCPS), IEEE 2017.

53 Vgl. *Mettler/Wulf*, Physiolytics at the workplace: Affordances and constraints of wearables use from an employee's perspective, Information Systems Journal, 2019, 29. Jg., Nr. 1, S. 245-273; *Dietrich/Krüger/Potel*, Wearables im Zugriff der Strafjustiz, Trends und Communities der Rechtsinformatik: Tagungsband des 20. Internationalen Rechtsinformatik Symposions IRIS 2017, S. 561-568.

54 Vgl. *Kort*, a. a. O., 24.