Dirk Heckmann und Lorenz Marx

# *KI-Einsatz zur Leistungskontrolle am (Hochschul-)Arbeitsplatz*[1]
# *Anforderungen aus Sicht des Datenschutzrechts*



## I. Einleitung

Seit das textbasierte Dialogsystem (Chatbot) *ChatGPT* des US-amerikanischen Unternehmens OpenAI Ende 2022 zur kostenfreien Verwendung online gestellt wurde, ist ein regelrechter Hype um KI-gestützte Textgeneratoren, das zugrundeliegende Text- und Data-Mining und deren Anwendungsmöglichkeiten u.a. auch in rechtlichen Kontexten[2] entstanden. Die Fortschritte, die in der Entwicklung von KI-Anwendungen sichtbar werden, führen dazu, dass auch solche Einsatzszenarien auf den Prüfstand kommen, die schon vermeintlich rechtlich geklärt schienen. Dies gilt etwa für Leistungskontrollen bzw. Aufsichtsmaßnahmen des Arbeitgebers oder Dienstherrn gegenüber Beschäftigten.

*Der Einsatz von KI-Systemen zur Leistungskontrolle am Arbeitsplatz* ist in den vergangenen Jahren verstärkt in den öffentlichen Fokus gerückt. Im November 2019 geriet beispielsweise das Berliner Startup Zalando in die Schlagzeilen durch den Einsatz einer Personalsoftware namens „*Zonar*", mit der die Leistung und das Verhalten von Arbeitskollegen bewertet werden kann.[3] Das Thema wurde vereinzelt auch in juristischen Fachkreisen aufgegriffen.[4] Wohl in Folge der kritischen Berichterstattung nahm Zalando Änderungen an der Software vor.[5] Im Juni 2020 waren die ebenfalls von Zalando verwendeten Software-Systeme „*Zalos*" und „*Zafeto*" Gegenstand des öffentlichen Diskurses.[6] Mit diesen beiden Tools kann etwa erfasst werden, wie viele Artikel ein Beschäftigter pro Schicht bearbeitet.[7] In den beiden letzteren Fällen hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit eine Prüfung eingeleitet und Änderungshinweise erteilt.[8] Die fortwährende Erfassung von Leistungsdaten beim Online-Händler Amazon wurde hingegen - nach Untersagung durch die Landesbeauf-

1 Der Beitrag knüpft an den projektbezogenen Beitrag „*Informationelle Selbstbestimmung in der digitalen Arbeitswelt*" aus dem BMBF-geförderten Projekt „*Inverse Transparenz - Beteiligungsorientierte Ansätze für Datensouveränität in der digitalen Arbeitswelt gestalten*" an, der am 24.5.2022 im Forschungsreport „*Daten – Innovation – Privatheit: Mit Inverser Transparenz das Gestaltungsdilemma der digitalen Arbeitswelt lösen*", S. 56 ff., erschienen ist. Der vorliegende Beitrag entwickelt diese Gedanken zum KI-Einsatz im Kontext staatlicher Hochschulen weiter und sucht Lösungsansätze für eine verhältnismäßige Leistungs- und Verhaltenskontrolle mittels algorithmischer Systeme.

2 Hierzu *Bachgrund/Nesum/Bernstein/Burchard*, Das Pro und Contra für Chatbots in Rechtspraxis und Rechtsdogmatik, CR 2023, 132 ff.

3 Vgl. u.a. https://www.sueddeutsche.de/wirtschaft/zalando-ueberwachung-zonar-1.4688431 (letzter Zugriff am 27.02.2023).

4 *Lurtz*, Bewertungstechnologien im Beschäftigungsverhältnis – eine (erste) datenschutzrechtliche Bewertung, ZD-Aktuell 2020, 06926; *Holthausen*, Big Data, People Analytics, KI und Gestaltung von Betriebsvereinbarungen– Grund-, arbeits- und datenschutzrechtliche An- und Herausforderungen, RdA 2021, 19, 22 Fn. 65; *Joos*, Einsatz von künstlicher Intelligenz im Personalwesen unter Beachtung der DS-GVO und des BDSG, NZA 2020, 1216, 1221.

5 Vgl. https://www.datenschutz-notizen.de/zalando-aendert-eigene-bewertungssoftware-zonar-2829837/ (letzter Zugriff am 27.02.2023).

6 Vgl. u.a. https://t3n.de/news/ueberwachung-berlin-prueft-1286877/ (letzter Zugriff am 27.02.2023).

7 Vgl. https://www.zeit.de/wirtschaft/unternehmen/2020-05/zalando-datenschutzbeauftragte-pruefverfahren-logistikzentrum?utm_referrer=https%3A%2F%2Fwww.google.com%2F (letzter Zugriff am 27.02.2023).

8 Vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht 2020 Datenschutz und Informationsfreiheit, S. 267.

tragte für den Datenschutz Niedersachsen - erst kürzlich gerichtlich für zulässig erklärt.[9] Die in Echtzeit minutiös erfolgende Erfassung der Arbeitsschritte von Mitarbeitern wurde vom Gericht unter dem Aspekt logistischer Abläufe für erforderlich gehalten.[10]

Diese Beispiele zeigen nur einen Ausschnitt des denkbar breiten Spektrums an potenziellen Anwendungsfällen für eine KI-unterstützte Leistungskontrolle nicht nur in der Wirtschaft, sondern auch an Hochschulen und Forschungseinrichtungen, die in Zukunft durch große Trends wie Big Data und die *Verfügbarkeit immer vielfältigerer und leistungsfähigerer algorithmischer Systeme* noch wachsen dürfte. Anders als beim Einsatz von KI-Systemen im Rahmen des Bewerbungsprozesses wird der Einsatz von KI zur Leistungskontrolle während des Beschäftigungsverhältnisses in der Rechtswissenschaft noch vergleichsweise wenig diskutiert.[11] Dieser Beitrag zeigt die datenschutzrechtlichen Determinanten sowie den verbleibenden Aktionsradius auf.

## II. Verhaltens- und Leistungskontrollen im betrieblichen und wissenschaftlichen Bereich

Die fortwährende Überwachung und die Kontrolle des Verhaltens sowie der Leistung von Beschäftigten im Hinblick auf ihre (außer-)vertraglichen Pflichten ist ein eng mit der Durchführung des Arbeitsverhältnisses verbundenes Instrument.[12] Solche Verhaltens- und Leistungskontrollen sind dabei nicht automatisch Ausdruck von Misstrauen im machtasymmetrischen Verhältnis von Vorgesetzten und Beschäftigten. Vielmehr können solche Kontrollen auch geeignet sein, interne Prozesse zu überarbeiten und zu optimieren und erforderlich sein, um Compliance-Pflichten nachzukommen (s.u. IV.1.).

Dabei sind die *Arten von Leistungskontrollen* außerordentlich vielfältig. Der technische Fortschritt der digitalen Transformation und die rasch voranschreitende Automatisierung von Prozessen mittels riesiger Datenmengen ermöglicht immer neuere und weitergehende Kontrollen. Im betrieblichen Beschäftigtenkontext sind paradigmatisch die Zeiterfassung, Videoüberwachung, GPS-Tracking, die Kontrolle und Protokollierung der IT-Nutzung oder die Verarbeitung von Bewertungen von Beschäftigten und Vorgesetzten anzuführen. Derartige Instrumente erzeugen eine Vielzahl von Datenpunkten. Da sich Verhaltens- und Leistungsdaten sinnvollerweise immer bestimmten, hierdurch zumindest identifizierbaren Personen zuordnen lassen, handelt es sich in aller Regel um personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO,[13] weshalb die beschriebenen Organisationsinteressen immer auch mit dem Schutz der Persönlichkeitsrechte der Mitarbeiter in Einklang zu bringen sind (s. hierzu ausführlich IV.).

Auch in *staatlichen Hochschulen und Forschungseinrichtungen* können Verhaltens- und Leistungskontrollen zur Prozessoptimierung und Einhaltung von Compliance-Anforderungen geeignet sein und daher Anwendung finden. Hierbei ist aber streng zwischen nicht-wissenschaftlichem und wissenschaftlichem Personal zu differenzieren. Die Instrumente zur Mitarbeiterüberwachung bei nicht-wissenschaftlichem, in der Regel mit Verwaltungsaufgaben betrautem Personal können aufgrund der Linearität und Wiederholbarkeit der Aufgaben und der regelmäßig vordefinierten Ziele durchaus denen im betrieblichen Kontext (s.o.) ähneln.

Bei *wissenschaftlichem Personal* gestalten sich derartige Leistungskontrollen schwieriger. Auch wenn ihre Arbeit sich an einem Erkenntnisgewinn orientiert,[14] kann hieraus noch kein messbares Ziel geschlossen werden, zumindest kein vordefiniertes. Im Lichte der verfassungsrechtlich geschützten *Wissenschaftsfreiheit* nach Art. 5 Abs. 3 GG bzw. der Forschungsfreiheit nach Art. 13 GRCh müsste man bereits bei der Frage ansetzen, was überhaupt unter „*Leistung*" in diesem Kontext zu

9 VG Hannover 9.2.2023, 10 A 6199/20; s. hierzu auch https://www.verwaltungsgericht-hannover.niedersachsen.de/aktuelles/pressemitteilungen/datenerhebung-bei-amazon-in-winsen-ist-rechtmassig-219664.html (letzter Zugriff am 27.02.2023).

10 Vgl. auch *Montag*, Ständige Mitarbeiterkontrolle bei Amazon Logistik nicht zu beanstanden, beck-aktuell v. 10. Februar 2023 zu VG Hannover 9.2.2023, 10 A 6199/20.

11 So auch *Joos*, Einsatz von künstlicher Intelligenz im Personalwesen unter Beachtung der DS-GVO und des BDSG, NZA 2020, 1216, 1221.

12 T*aeger/Gabel/Zöll*, 4. Aufl. 2022, BDSG § 26 Rn. 41; ErfK/*Franzen*, 23. Aufl. 2023, BDSG § 26 Rn. 22.

13 Vgl. so auch *Winter*, Leistungsdaten im Kontext des Datenschutzrechts, SpuRt 2020, 168, 169.

14 Das BVerfG definiert Forschung als „*geistige Tätigkeit mit dem Ziele, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen*", s. BVerfG 29.5.1973, 1 BvR 325/72, BVerfGE 35, 79, 113, vgl. auch Dürig/Herzog/Scholz/*Gärditz*, 99. EL Sept. 2022, GG Art. 5 Abs. 3 Rn. 94.

verstehen ist und an welchen Parametern eine Leistungskontrolle ansetzen kann. Staatliche Hochschulen werden im Rahmen der Wissenschaftsfreiheit gegenüber ihren wissenschaftlichen Mitarbeitern zur Gewährleistung von Freiheit in Lehre und Forschung verpflichtet.[15] Eine *inhaltliche Kontrolle von wissenschaftlichem Personal* kann nur mit *„Mitteln des wissenschaftlichen Diskurses"* erfolgen, solange dem jeweiligen Forschungsergebnis nicht bereits der ernsthafte Versuch abgesprochen werden kann, die Grundsätze wissenschaftlichen Arbeitens zu beachten.[16] Hierbei rückt insbesondere algorithmenbasierte Plagiatssoftware in den Fokus, die riesige Mengen an Textdaten aggregiert und wissenschaftliche Texte mit den zugrundeliegenden Textdaten vergleicht, um Übereinstimmungen festzustellen. Ebenso könnte künftig die sog. Anmaßung einer wissenschaftlichen Autorenschaft, die ein mit den wissenschaftlichen Grundsätzen unvereinbares Fehlverhalten darstellt,[17] zum Beispiel durch technische Erweiterungen bereits vielfach verwendeter Projektverwaltungssoftware, die häufig alle Entwicklungsschritte und inhaltlichen Beiträge der tatsächlich beteiligten Wissenschaftler speichert, automatisiert identifiziert werden.

Darüber hinaus sind aber auch hier die neuerlichen Auswirkungen KI-gestützter Systeme wie ChatGPT zu beachten: Während herkömmliche Plagiatssoftware die Texte des Dialogsystems teilweise als *„menschlich echt"* einstufte,[18] verfügt Software, die spezifisch zur Aufdeckung ChatGPT-generierter Texte entwickelt wurde (z.B. GPTZero), noch nicht über die erforderliche Leistungsfähigkeit und Treffsicherheit.[19] Sowohl herkömmliche als auch spezifische Plagiatskontrolle funktioniert also noch nicht hinreichend zuverlässig. KI-Systeme bringen nunmehr KI-Systeme zur Plagiatskontrolle an ihre Grenzen.

Die beschriebenen betrieblichen Instrumente zur Verhaltens- und Leistungskontrolle können auf Wissenschaftler mit Blick auf deren individuell gewährleistete Wissenschaftsfreiheit nicht ohne Weiteres übertragen werden. Am ehesten kann deren Einsatz ausnahmsweise noch mit einer völlig fehlenden Beachtung der Grundsätze wissenschaftlichen Arbeitens im Einzelfall oder mit dem Erhalt der Funktionsfähigkeit[20] der jeweiligen Hochschule begründet werden.

## III. Status Quo: Grundlagen des (Beschäftigten-) Datenschutzes im Kontext von Verhaltens- und Leistungskontrolle

Trotz vereinzelter rechtspolitischer Bemühungen in der Vergangenheit gibt es in Deutschland bislang *kein (nationales) Beschäftigtendatenschutzgesetz.*[21] Ein durch das Bundesministerium für Arbeit und Soziales (BMAS) eingesetzter interdisziplinärer und unabhängiger Beirat kam in seinem Abschlussbericht im Januar 2022 zu dem Ergebnis, dass ein solches eigenständiges Gesetz aber durchaus erforderlich sei.[22] Auch mit der Neuordnung des europäischen Datenschutzrechts durch die Datenschutz- Grundverordnung (DSGVO) wird der Beschäftigtendatenschutz nicht direkt auf Unionsebene geregelt. Die DSGVO statuiert in Art. 88 Abs. 1 aber eine *Öffnungsklausel* zur Verarbeitung personenbezogener Daten im Beschäftigungskontext. Darüber hinaus zieht sie in Art. 88 Abs. 2 Grenzen für (automatisierte) Überwachungssysteme am Arbeitsplatz, besonders mit Blick auf die Menschenwürde und berechtigte Interessen der Betroffenen.[23]

In Anwendung der Öffnungsklausel des Art. 88 Abs. 1 DSGVO stellt § 26 BDSG die *relevante Rechtsgrundlage* für die Verarbeitung personenbezogener Daten im Rahmen von bestimmten Beschäftigungsverhältnissen dar, die den allgemeineren Art. 6 Abs. 1 lit. f DSGVO in ihrem Anwendungsbereich verdrängt.[24] Gemäß § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten für die Zwecke des Beschäftigungsverhältnisses (unter anderem) verarbeitet werden, wenn

15 Jarass/Pieroth/*Jarass*, 17. Aufl. 2022, GG Art. 5 Rn. 133.

16 So bzgl. Hochschullehrern auch BVerfG 8.8.2000, 1 BvR 653/97, NJW 00, 3635; Jarass/Pieroth/*Jarass*, 17. Aufl. 2022, GG Art. 5 Rn. 155.

17 DFG, Guidelines for Safeguarding Good Research Practice. Code of Conduct, 2022, S. 18 f.

18 S. hierzu auch https://www.br.de/nachrichten/netzwelt/ki-darf-chatgpt-wissenschaftliche-artikel-schreiben,TTxluZc (letzter Zugriff am 27.02.2023).

19 Vgl. auch https://t3n.de/news/app-gptzero-chatgpt-plagiat-1525329/ (letzter Zugriff am 27.02.2023).

20 BVerfG 13.4.2010, 1 BvR 216/07, BVerfGE 126, 1, 25; Jarass/Pieroth/*Jarass*, 17. Aufl. 2022, GG Art. 5 Rn. 149.

21 Hierzu Heckmann/Paschke/*Braun*, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 7 Rn. 11.

22 Vgl. zum Ergebnis des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz auch https://www.bmas.de/DE/Service/Presse/Meldungen/2022/bmas-veroeffentlicht-ergebnisse-des-beirats-zum-beschaeftigtendatenschutz.html (letzter Zugriff am 27.02.2023).

23 BeckOK DatenschutzR/*Riesenhuber*, 42. Ed. 1.11.2022, DSGVO Art. 88 Rn. 91; Paal/Pauly/*Pauly*, 3. Aufl. 2021, DSGVO Art. 88 Rn. 17.

24 *Maschmann*, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, 115, 116.

es für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. *„Die Kontrolle, ob der Arbeitnehmer seinen Pflichten nachkommt"*, gehört dabei ebenso zur Durchführung des Beschäftigungsverhältnisses und fällt deshalb in den Anwendungsbereich des § 26 Abs. 1 S. 1 BDSG.[25]

Erfolgt die Datenverarbeitung auf Grundlage einer *Einwilligung*, so legt § 26 Abs. 2 BDSG die Prüfkriterien für die Wirksamkeit der Einwilligung fest. Insbesondere die für das Beschäftigungsverhältnis charakteristische Machtasymmetrie ist nach § 26 Abs. 2 S. 1 BDSG für die Beurteilung der Freiwilligkeit der Einwilligung zu beachten. Nach § 26 Abs. 2 S. 2 BDSG kommt eine Freiwilligkeit insbesondere in Betracht, wenn ein Vorteil für die beschäftigte Person erreicht wird. Dieser Vorteil kann sowohl wirtschaftlicher als auch rechtlicher Natur sein. Eine Einwilligung kann auch insbesondere dann freiwillig sein, wenn eine kongruente Interessenlage besteht.

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten an staatlichen Hochschulen zu Zwecken der Forschung ist trotz des Spannungsverhältnisses von Datenschutz und Forschungsfreiheit unter bestimmten Voraussetzungen sinnvoll möglich.[26] Geht es um die *Verarbeitung personenbezogener Daten im Beschäftigungskontext an staatlichen Hochschulen und Forschungseinrichtungen*, gilt die Vorschrift des § 26 BDSG allerdings nicht, außer es handelt sich bei der verarbeitenden Behörde um eine Hochschule des Bundes. Denn nach § 1 Abs. 1 BDSG öffnet sich der Anwendungsbereich des Gesetzes für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes (Abs. 1 S. 1 Nr. 1) und nicht-öffentliche Stellen (Abs. 1 S. 2), wozu beispielsweise Arbeitgeber gehören.[27] Für öffentliche Stellen der Länder, also auch die allermeisten staatlichen Hochschulen, ist der Anwendungsbereich erheblich eingeschränkt (Abs. 1 S. 1 Nr. 2). Das BDSG greift hier nur, wenn diese Stellen Bundesrecht ausführen oder es sich bei den Stellen um Organe der Rechtspflege handelt und der Datenschutz nicht durch Landesrecht geregelt ist. Die allermeisten Landesdatenschutzgesetze enthalten spezielle Regelungen für den Beschäftigtendatenschutz,[28] die sich in ihrer Reichweite aber teils deutlich unterscheiden.[29]

Schließlich ist im Rahmen des Einsatzes von KI-Systemen zudem Art. 22 Abs. 1 DSGVO zu berücksichtigen. Dieser verbietet allgemein (auch im Beschäftigungskontext) ausschließlich aufgrund *automatisierter Verarbeitung* – einschließlich *Profiling* – getroffene Entscheidungen, die rechtserhebliche Auswirkungen haben. Art. 4 Nr. 4 DSGVO definiert Profiling als automatisierte Verarbeitung personenbezogener Daten, die darin besteht, bestimmte persönliche Aspekte einer natürlichen Person zu analysieren und vorherzusagen. Hierzu gehören beispielsweise das Verhalten und die Arbeitsleistung von Personen. Ein generelles Verbot von Profiling an sich enthält Art. 22 Abs. 1 DSGVO jedoch nicht, lediglich das Verbot aufgrund eines Profilings einer automatisierten beeinträchtigenden Entscheidung unterworfen zu werden.[30]

Automatisierte Entscheidungen auf Grundlage von Profiling können ausnahmsweise nach Art. 22 Abs. 2 DSGVO zulässig sein,[31] insbesondere aufgrund einer Einwilligung. Ob eine solche aber innerhalb eines Beschäftigungsverhältnisses aufgrund des strukturellen Machtungleichgewichts als freiwillig gelten kann, ist zu hinterfragen.[32]

## IV. Herausforderungen und Lösungsansätze

### 1. Interessensabwägung bei Leistungskontrolle am Arbeitsplatz

Gemäß § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten im Beschäftigungskontext (unter anderem) verarbeitet werden, wenn die Verarbeitung für die Durchführung des Beschäftigungsverhältnisses erforderlich ist.

25 Taeger/Gabel/*Zöll*, 4. Aufl. 2022, BDSG § 26 Rn. 41; zum BDSG a.F. BAG, 29.6.107, 2 AZR 597/16, NZA 2017, 1179 Rn. 26.

26 Einen guten Überblick hierzu bieten *Bronner/Wiedemann*, Rechtmäßigkeit der Datenverarbeitung bei wissenschaftlicher Forschung an staatlichen Hochschulen, ZD 2023, 77 ff.

27 Vgl. BAG 7.5.2019, 1 ABR 53/17, NZA 2019, 1218 Rn. 29 f.

28 Spezielle Regelungen zur Datenverarbeitung im Beschäftigungskontext enthalten z.B. § 15 LDSG BW, § 18 BlnDSG, § 26 Bbg DSG, § 12 BremDSGVOAG, § 10 HmbDSG, § 23 HDSIG, § 10 DSG M-V, § 12 NDSG, § 18 DSG NRW, § 20 LDSG RLP, § 22 SDSG, § 11 SächsDSDG, § 26 DSAG LSA, § 15 LDSG SH, § 27 ThürDSG.

29 Eine Übersicht und eine vergleichende Betrachtung mit § 26 BDSG findet sich bei *Gola*, Der Beschäftigtendatenschutz in den novellierten Landesdatenschutzgesetzen, ZD 2018, 448 ff.

30 *Huff/Götz*, Evidenz statt Bauchgefühl? – Möglichkeiten und rechtliche Grenzen von Big Data im HR-Bereich, NZA-Beilage 2019, 73, 76; *Rudkowski*, *„Predictive policing"* am Arbeitsplatz, NZA 2019, 72, 75.

31 Vgl. *Joos*, Einsatz von künstlicher Intelligenz im Personalwesen unter Beachtung der DS-GVO und des BDSG, NZA 2020, 1216, 1217 f. zum Einsatz von KI im Bewerbungsprozess.

32 Ablehnend bereits für den Bewerbungsprozess *Joos*, Einsatz von künstlicher Intelligenz im Personalwesen unter Beachtung der DS-GVO und des BDSG, NZA 2020, 1216, 1217, 1221, auch für die Mitarbeiterentwicklung, sofern es keinen *„echten Bestandsschutz"* für das Arbeitsverhältnis gibt. Vgl. auch *Graf/Kemper*, Optimierung und Produktivitätssteigerung durch Human Enhancement-Technologien, PinG 2021, 131, 136 f. (*„Machtasymmetrie zwischen Arbeitgeber und Beschäftigtem"*).

Erforderlich ist eine Datenverarbeitung i.S.v. § 26 Abs. 1 S. 1 BDSG, wenn die berechtigten Interessen und Zwecke des Arbeitgebers eine Datenverarbeitung erfordern.[33] Das Kriterium der Erforderlichkeit findet sich auch in den meisten landesrechtlichen Vorschriften zur Verarbeitung personenbezogener Daten im Dienst- oder Beschäftigungskontext. Die Freiheit des Arbeitgebers, grundsätzlich selbst zu entscheiden, wie er seine Betriebe und Dienststellen organisiert, ist zu achten.[34]
Im Ergebnis ist eine *zweistufige Verhältnismäßigkeitsprüfung* durchzuführen:[35]

Auf der ersten Stufe „muss die Überwachungsmaßnahme für die Wahrung eines berechtigten Interesses des Arbeitgebers erforderlich sein", auf der zweiten Stufe ist „die Verhältnismäßigkeit im engeren Sinne zu prüfen".[36]

Auf der *ersten Stufe* ist zunächst festzustellen, dass die Kontrolle, ob ein Beschäftigter seinen Pflichten nachkommt, essenziell zur Durchführung des Arbeitsverhältnisses gehört.[37] Für den Arbeitgeber sind Leistungskontrollen in gewissem Umfang regelmäßig notwendig, nicht zuletzt auch um ordnungsgemäßen Compliance-Grundsätzen zu genügen, etwa aus § 91 Abs. 2 AktG, §§ 30, 130, 9 OWiG.[38]

Auf der *zweiten Stufe* kommt es für die Beurteilung der Verhältnismäßigkeit im engeren Sinne maßgeblich auf die jeweiligen konkreten Umstände an. Aus der verfügbaren behördlichen und gerichtlichen Praxis sowie dem Schrifttum lassen sich jedoch einige „Leitplanken" ermitteln.

*Zulässige Leistungskontrolle*: Die IT-Nutzung darf grundsätzlich kontrolliert werden, wenn eine Privatnutzung verboten ist;[39] allerdings muss insbesondere die Verhältnismäßigkeit gewahrt bleiben.[40] Nach Auffassung des LArbG München kann insoweit gegebenenfalls sogar eine anlasslose Überwachung durch ein KI-IT-Sicherheitssystem verhältnismäßig sein, wenn sie darauf abzielt, auffällige Aktivitäten zu identifizieren, die Anhaltspunkte für eine Bedrohung der Informationssicherheit sein können, insbesondere vor dem Hintergrund bankenaufsichtsrechtlicher und bankenaufsichtsbehördlicher Vorgaben zur Datensicherheit.[41]

*Unzulässige Leistungskontrolle*: Jedenfalls anonyme bzw. nicht erkennbare und nicht abwendbare Überwachung stellt einen erheblichen Eingriff in das Datenschutzrecht des Beschäftigten dar.[42] Sie ist grundsätzlich unzulässig, § 26 Abs. 1 S. 2 BDSG reicht hierfür nicht.[43]

> Eine *„permanente, heimliche und in ihrem Volumen nicht einschätzbare Totalüberwachung des Umgangs mit dienstlich zu verwendenden IT-Systemen"* kann *„allenfalls dann zulässig sein, wenn ein auf den einzelnen Arbeitnehmer bezogener begründeter Verdacht für eine Straftat oder für eine schwerwiegende Pflichtverletzung besteht".*[44]

Der dauerhafte Einsatz von Keyloggern ist vor diesem Hintergrund nicht mehr verhältnismäßig.[45] In aller Regel nicht mehr verhältnismäßig ist auch eine offene präventive Videoüberwachung am Arbeitsplatz.[46] Dasselbe gilt für Videoüberwachungen, die die Intimsphäre berühren.[47]

Der *flächendeckende Einsatz* von GPS-Ortungssystemen ist nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg i.d.R. nicht erforderlich, wenn der Aufenthaltsort des

33 BeckOK DatenschutzR/*Riesenhuber*, 42. Ed. 1.11.2022, BDSG § 26 Rn. 114.
34 BeckOK DatenschutzR/*Riesenhuber*, 42. Ed. 1.11.2022, BDSG § 26 Rn. 114.
35 *Maschmann*, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, 115, 117. 36 Gola/Heckmann/*Gola/Pötters*, 3. Aufl. 2022, BDSG § 26 Rn. 156 f.
37 Taeger/Gabel/*Zöll*, 4. Aufl. 2022, BDSG § 26 Rn. 41; zum BDSG a.F. BAG, 29.6.107, 2 AZR 597/16, NZA 2017, 1179 Rn. 26.
38 Taeger/Gabel/*Zöll*, 4. Aufl. 2022, BDSG § 26 Rn. 42; *Stück*, Compliance: Überwachungsmöglichkeiten des Arbeitgebers im Lichte aktueller Rechtsprechung, ArbRAktuell 2018, 31.
39 *Maschmann*, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, 115, 122; vgl. auch BAG 27.7.2017, 2 AZR 681/16, NZA 2017, 1327.
40 *Maschmann*, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, 115, 122.
41 LArbG München 23.7.2020, 2 TaBV 126/19; hierzu *Wedde*, Streit um Einigungsstellenspruch zur Einführung eines IT-Sicherheitssystems: Anlasslose präventive Verarbeitung von Beschäftigtendaten durch KI-Software zulässig, jurisPR-ArbR 17/2021 Anm. 6.
42 Paal/Pauly/*Pauly*, 3. Aufl. 2021, DSGVO Art. 88 Rn. 16.
43 EGMR 7.12.2017, C-329/16, EuZW 2018, 169 Rn. 121; *Maschmann*, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, 115, 121.
44 *Wedde*, Streit um Einigungsstellenspruch zur Einführung eines IT-Sicherheitssystems: Anlasslose präventive Verarbeitung von Beschäftigtendaten durch KI-Software zulässig, jurisPR-ArbR 17/2021 Anm. 6.; vgl. auch BAG 27.7.2017, 2 AZR 681/16, NZA 2017, 1327.
45 *Stück*, Datenschutz = Tatenschutz? Ausgewählte datenschutz- und arbeitsrechtliche Aspekte nach DSGVO sowie BDSG 2018 bei präventiver und repressiver Compliance, CCZ 2020, 77, 81; vgl. auch BAG 27.7.2017, 2 AZR 681/16, NZA 2017, 1327.
46 Vgl. hierzu im Detail *Stück*, Datenschutz = Tatenschutz? Ausgewählte datenschutz- und arbeitsrechtliche Aspekte nach DSGVO sowie BDSG 2018 bei präventiver und repressiver Compliance, CCZ 2020, 77, 81 f.
47 *Maschmann*, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, 115, 121.

Beschäftigten auch direkt bei diesem (etwa durch einen Anruf) erhoben werden kann. Eine solche dauerhafte Ortung kann i.d.R. nicht auf eine Einwilligung gestützt werden. Sie erzeugt zudem einen permanenten Kontrolldruck und ist daher unzulässig.[48]

Bei allem sind allgemein die *Betroffenenrechte* und die Informationspflichten zu wahren.[49] Bemerkenswert ist insoweit der bereits erwähnte Beschluss des LArbG München v. 23.07.2020.[50] Das Gericht äußerte sich zu einem KI-IT-Sicherheitssystem, das einen umfassenden Datenzugriff ermöglicht und dessen Abläufe für Beschäftigte intransparent sind. Nach Ansicht des Gerichts bestünden sachliche Gründe dafür, sicherheitstechnische Details des Systems nicht vollständig offenzulegen.[51]

2. Der Einsatz von KI zur Leistungskontrolle: Verschärfung der Überwachung oder legitimes „*Feintuning*"?

KI-Einsatz und Datenschutzrecht stehen in einem *Spannungsverhältnis*.[52] Allemal definiert das Datenschutzrecht - aufgrund noch fehlender horizontaler Regulierung von KI-Tools – ein Mindestmaß an Grundregeln für den Einsatz von KI-Systemen.[53]

Beim Einsatz von KI-Systemen zur Leistungskontrolle handelt es sich in der Regel um *Profiling* i.S.v. Art. 4 Nr. 4 DSGVO,[54] dort ist als Regelbeispiel gerade die Arbeitsleistung genannt, die analysiert oder vorhergesagt werden soll. Ausschließlich auf Automatisierung beruhende Entscheidungen auf der Grundlage von Profiling sind grundsätzlich aber nicht zulässig, Art. 22 Abs. 1 DSGVO. Soweit dies gilt, setzt die Verwertung des KI-Ergebnisses voraus, dass ein Mensch mit Entscheidungsspielraum die Entscheidung in einem gewissen Umfang nachprüft.[55]

Eine Rechtfertigungsmöglichkeit aufgrund von Einwilligung dürfte aufgrund des strukturellem Machtungleichgewichts typischerweise entfallen. Gegebenenfalls können hier in gewissem Rahmen Betriebsvereinbarungen herangezogen werden.[56]

Aus datenschutzrechtlicher Sicht ist deshalb festzuhalten, dass „*KI-basierte Gesamtlösungen*" in den seltensten Fällen DSGVO-konform zu gestalten sind. Denkbar sind jedoch „*KI-basierte Einzellösungen*", die in einen komplexeren Datenverarbeitungsprozess eingebettet sind und insbesondere Raum für nicht ausschließlich automatisiert erfolgende Letztentscheidungen einräumen.[57] *Hinz* bringt diesen Ansatz mit folgendem Beispiel prägnant auf den Punkt:

> *„So darf etwa das KI-System den als unzuverlässig eingeordneten Arbeitnehmer nicht selbsttätig zu einer Compliance-Schulung verpflichten oder ihn versetzen. Hingegen kann der Arbeitgeber auf Grundlage des Predictive Policing [Unterfall des Profilings] den Arbeitnehmer zur Schulungsteilnahme anweisen."*[58]

Dieser Ansatz kann ebenso auf Beschäftigte von Hochschulen und Forschungseinrichtungen angewendet werden.

In jedem Fall erfordert der G*rundsatz der Transparenz* (Art. 13-15 DSGVO), dass die Betroffenen über den Einsatz des KI-Tools und die Folgen unterrichtet werden.[59] Es sind geeignete technisch-organisatorische Maßnahmen zu treffen, die insbesondere Erklärbarkeit

48 Ratgeber Beschäftigtendatenschutz, Landesbeauftragter für Datenschutz und Informationsfreiheit Baden- Württemberg, 4. Aufl. 2020, S. 37 f., auch zu den Anforderungen, die an eine zulässige GPS-Überwachung zu stellen sind.

49 Dies ist ein allgemeines Problem und hängt nicht speziell mit dem Arbeitnehmerdatenschutz zusammen, hierzu bspw. *Conrad*, DSGVO 2.0 – Effizienter(er) Schutz durch KI?, DSRITB 2019, 391, 401 ff.

50 LArbG München 23.7.2020, 2 TaBV 126/19; hierzu Wedde, Streit um Einigungsstellenspruch zur Einführung eines IT-Sicherheitssystems: Anlasslose präventive Verarbeitung von Beschäftigtendaten durch KI-Software zulässig, jurisPR-ArbR 17/2021 Anm. 6.

51 Vgl. *Wedde*, Streit um Einigungsstellenspruch zur Einführung eines IT-Sicherheitssystems: Anlasslose präventive Verarbeitung von Beschäftigtendaten durch KI-Software zulässig, jurisPR-ArbR 17/2021 Anm. 6.

52 Kaulartz/Braegelmann/*Paal*, Artificial Intelligence und Machine Learning, Kap. 8.7 Rn. 38.

53 Hierzu *Schefzig*, Asimov 2.0 – Datenschutzrechtliche KI-Grundregeln, DSRITB 2018, 491, 496 ff; i.E. auch *Joos*, Einsatz von künstlicher Intelligenz im Personalwesen unter Beachtung der DS-GVO und des BDSG, NZA 2020, 1216, 1217.

54 *Joos*, Einsatz von künstlicher Intelligenz im Personalwesen unter Beachtung der DS-GVO und des BDSG, NZA 2020, 1216, 1217.

55 BeckOK DatenschutzR/*von Lewinski*, 42. Ed. 1.11.2022, DSGVO Art. 22 Rn. 24a f.

56 Hierzu *Holthausen*, Big Data, People Analytics, KI und Gestaltung von Betriebsvereinbarungen – Grund-, arbeits- und datenschutzrechtliche An- und Herausforderungen, RdA 2021, 19, 28 ff.

57 Kaulartz/Braegelmann/*Meents*, Artificial Intelligence und Machine Learning, Kap. 8.8 Rn. 65 f.

58 Kaulartz/Braegelmann/*Hinz*, Artificial Intelligence und Machine Learning, Kap. 11 Rn. 25.

59 BeckOK DatenschutzR/Schild, 42. Ed. 1.11.2022, DSGVO Art. 4 Rn. 67; *Maschmann*, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, 115, 118; Dies gibt bereits der Unionsgesetzgeber in Art. 88 Abs. 2 DSGVO vor, vgl. Sydow/Marsch/*Tiedemann*, 3. Aufl. 2022, DSGVO Art. 88 Rn. 18 f.

und Transparenz gewährleisten müssen.[60] Nicht endgültig geklärt ist dabei, ob die Betroffenen auch Einsicht in den Algorithmus selbst erlangen müssen;[61] dies wird oftmals technisch nicht möglich sein, weshalb zumindest über die Eingangsdaten und die Herkunft der Daten informiert werden muss.[62]

## V. Ausblick auf den KI-Einsatz zur Leistungskontrolle im Beschäftigungskontext im Jahr 2030

Im kommenden Jahrzehnt ist zu erwarten, dass der Einsatz von KI -Tools zur Leistungskontrolle und damit verbunden die Frage nach der datenschutzrechtlichen Zulässigkeit an Bedeutung gewinnen wird. Dies betrifft Beschäftigte in der Privatwirtschaft sowie in Hochschulen und Forschungseinrichtungen gleichermaßen. Gleichzeitig sollten die hier skizzierten datenschutzrechtlichen Anforderungen nicht allein als *„Hemmschuh"*, sondern vielmehr als *„Gestaltungskorridor"* verstanden werden. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat darauf hingewiesen,

> *„dass in den nächsten Jahren entscheidende Weichenstellungen für die KI getroffen werden und der Datenschutz nicht zwangsläufig die Entwicklung beeinträchtigen muss."*[63]

Perspektivisch soll daher die folgende *These* aufgestellt werden: Richtig eingesetzt (d.h. insbesondere unter Ausschluss von automatisierten beeinträchtigenden Entscheidungen allein auf Grundlage des verwendeten KI-Tools) können *„KI-basierte Einzellösungen"* zur Leistungskontrolle nicht etwa zu einem Mehr an (Total-) Überwachung führen, sondern im Gegenteil der Wahrung der Anforderungen des Datenschutzrechts dienen:[64]

Der Einsatz von KI kann etwa zur Wahrung des Grundsatzes der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) fruchtbar gemacht werden,[65] denn eine KI kann die erhobenen Daten (zum Vorteil der betroffenen Person) unmittelbar prüfen, während eine menschliche Prüfung eine längere Speicherung der Daten erforderlich machen kann. Der Einsatz von KI kann zudem dem Gebot der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) dienen, etwa durch verlässliche Techniken der Anonymisierung.[66] Denn während etwa im Falle der Videoüberwachung ein Mensch den Beschäftigten beobachten müsste, würde eine KI an dessen Stelle treten, die datenschutzwidrige Inhalte sogleich löschen würde. Die Privatsphäre würde so also weniger tangiert. Es entfällt insbesondere das dauerhafte *„Beobachtetsein"*.

Perspektivisch gedacht könnte der Einsatz von „KI-basierten Einzellösungen" sogar eines Tages dem Stand der Technik nach Art. 25 Abs. 1 DSGVO (Stichwort *„Privacy by Design"*) entsprechen und wären daher sogar verpflichtend.[67] Dies betrifft insb. die Anonymisierung. Weitergehender Schutz von Betroffenen ist auch durch den AI Act[68] der Europäischen Union zu erwarten, der sich derzeit noch im Gesetzgebungsverfahren befindet.[69] Der Verordnungsentwurf der EU-Kommission stuft in seinem risikobasierten Regulierungsansatz solche Systeme als *„Hochrisiko-KI-Systeme"* ein, die grundsätzlich mit einem hohen Risiko für die Grundrechte von natürlichen Personen verbunden sind.[70] Solche Systeme, zu

60 *Joos/Meding*, Künstliche Intelligenz und Datenschutz im Human Resource Management, CR 2020, 834, 837 ff.

61 *Huff/Götz*, Evidenz statt Bauchgefühl? – Möglichkeiten und rechtliche Grenzen von Big Data im HR-Bereich, NZA-Beilage 2019, 73, 76.

62 *Huff/Götz*, Evidenz statt Bauchgefühl? – Möglichkeiten und rechtliche Grenzen von Big Data im HR-Bereich, NZA-Beilage 2019, 73, 77.

63 BfDI fordert datenschutzgerechten Einsatz von KI, ZD-Aktuell 2019, 06806.

64 Bisweilen wird gar eine *„Pflicht"* zum Einsatz von KI diskutiert, vgl. Kaulartz/Braegelmann/*Meents*, Artificial Intelligence und Machine Learning, Kap. 8.8 Rn. 4, der jedenfalls KI-basierte Gesamtlösungen aber i.E. als kaum bis unvereinbar mit der DSGVO einstuft, Rn. 65.

65 Ebenso Kaulartz/Braegelmann/*Meents*, Artificial Intelligence und Machine Learning, Kap. 8.8 Rn. 66.

66 Kaulartz/Braegelmann/*Meents*, Artificial Intelligence und Machine Learning, Kap. 8.8 Rn. 58 ff.

67 Kaulartz/Braegelmann/*Meents*, Artificial Intelligence und Machine Learning, Kap. 8.8 Rn. 67.

68 Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (Entwurf zum AI Act), COM (2021) 206 final.

69 Siehe zum aktuellen Stand des Gesetzgebungsverfahrens https://eur-lex.europa.eu/legal- content/EN/HIS/?uri=CELEX:52021PC0206 (letzter Zugriff am 27.02.2022).

70 Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (Entwurf zum AI Act), COM (2021) 206 final, S. 11, 13.

denen aufgrund der potenziellen Eingriffsintensität in die informationelle Selbstbestimmung betroffener Beschäftigter auch KI-Tools zur Verhaltens- und Leistungskontrolle gehören, müssen künftig eine Vielzahl von organisatorischen und technischen Anforderungen erfüllen, wozu auch eine erhöhte Transparenz im Sinne eines interpretierbaren Outputs (Art. 13 AIA-E) sowie eine mögliche menschliche Überwachung (Art. 14 AIA-E) gehören.

## VI. Handlungsempfehlungen

Nach richtiger Auffassung stellt das Datenschutzrecht keine unüberwindbaren Hürden für den Einsatz von KI-Systemen zur Leistungskontrolle am Arbeitsplatz auf. Vielmehr setzt es den äußeren Rahmen für die Gestaltung des Einsatzes solcher Tools.

Danach sind zumindest „*KI-basierte Einzellösungen*" zur Leistungskontrolle denkbar, die in einen komplexeren Datenverarbeitungsprozess eingebettet sind und insbesondere Raum für nicht ausschließlich automatisiert erfolgende Letztentscheidungen bieten.[71]

Hierzu ist es auch erforderlich, bereits in der *Entwicklungsphase* (Stichwort „*Privacy by Design*", Art. 25 Abs. 1 DSGVO) über eine Begrenzung des KI-Einsatzes zur Leistungskontrolle nachzudenken,[72] auch in zeitlicher Hinsicht oder begrenzt auf Stichproben, wobei KI wiederum helfen kann, ein angemessenes Maß zu finden.

## VII. Zusammenfassung

Eine Leistungskontrolle am Arbeitsplatz ist aus Sicht des Arbeitgebers bzw. Dienstherrn grundsätzlich legitim, besonders weil und soweit es um die Erfüllung von Compliance-Anforderungen in Betrieben und Dienststellen geht (Unterbindung von Betrug, Korruption, Spionage etc.). Dabei sind die Interessen der überwachten Beschäftigten, insbesondere deren Privatheit und Persönlichkeitsrechte, ebenso schutzwürdig. Dies gilt in besonderem Maße beim Einsatz von KI-basierten Kontrollsystemen, mit und ohne automatisierte Einzelfallentscheidung. Solange es hier aber nicht zu einer „*Totalüberwachung*" kommt, ist eine datenschutzkonforme Gestaltung der Leistungskontrolle denkbar, zumal der IT-Einsatz helfen kann, die Kontrolle auf das erforderliche und verhältnismäßige Maß zu reduzieren. Bei der Entwicklung entsprechender Systeme sollten Juristen und Informatiker zusammenwirken, ihr Einsatz muss zudem transparent und für alle Betroffenen (notfalls gerichtlich) überprüfbar sein. Eine Verhaltens- und Leistungskontrolle von wissenschaftlichem Personal an Hochschulen und in Forschungseinrichtungen ist im Hinblick auf die Wissenschaftsfreiheit nur sehr eingeschränkt möglich und zulässig. Auch hier können KI- Systeme aber künftig sinnvoll eingesetzt werden, um missbräuchlichem Verhalten Einhalt zu gebieten.

Prof. Dr. Dirk Heckmann ist Inhaber des Lehrstuhls für Recht und Sicherheit der Digitalisierung an der Technischen Universität München. Nebenamtlich wirkt er als Direktor am Bayerischen Forschungsinstitut für Digitale Transformation (www.bidt.digital) und als Verfassungsrichter am Bayerischen Verfassungsgerichtshof.

Dr. Lorenz Marx ist Corporate Counsel bei Amazon. Zuvor war er Rechtsanwalt bei verschiedenen Großkanzleien. Von 2019-2021 hat er als PostDoc und geschäftsführender Assistent maßgeblich den neuen Lehrstuhl von Professor Heckmann an der TU München mit aufgebaut.

71 Kaulartz/Braegelmann/*Meents*, Artificial Intelligence und Machine Learning, Kap. 8.8 Rn. 65 f.

72 Praktische Schwierigkeiten könnte eine solche Begrenzung des KI-Einsatzes insbesondere im Hinblick auf die fortschreitende Verbreitung von Big Data-Analysen und die immer tiefgreifendere Vernetzung i.R.v. Industrie 4.0 bereiten; hier ist es ggf. kaum mehr möglich, einzelne Use Cases/Beschäftigte/Zeitpunkte „*herauszufiltern*", vgl. *Puschky*, Datenschutzrechtliche Implikationen in der Industrie 4.0 am Beispiel des Forschungsprojekts „*IIP-Ecosphere*", ZD-Aktuell 2021, 05101.