RAT FÜR DIGITALE ÖKOLOGIE

VI2024

POSITIONS PAPIER

KONTROLLE AM VERNETZTEN ARBEITSPLATZ

DIGITAL, INTRANSPARENT, ALLUMFASSEND?

DR.
STEFAN BRINK
MAXIM KELLER
ANN-MARIE VERHOEVEN

KONTROLLE AM VERNETZTEN ARBEITSPLATZ

Digital, intransparent, allumfassend?

Zusammenfassung

Die digitale Transformation der Arbeitswelt ist in vollem Gange, auch was die Kontrollverhältnisse am vernetzten Arbeitsplatz angeht. An die Stelle persönlicher, stichprobenartiger, offener und erfahrungsbasierter Kontrolle tritt zunehmend eine **automatisierte, allumfassende, heimliche und algorithmenbasierte Kontrolle**.

Durch eine ungehemmte Digitalisierung wird allerdings der Überwachungsdruck am Arbeitsplatz weiter massiv verstärkt. Auf längere Sicht droht dadurch ein Wertewandel hin zu mehr Kontrolle am Arbeitsplatz; die über Jahrzehnte gewachsene Arbeitskultur in Deutschland verändert sich damit grundlegend: Wegen digitaler Überwachung droht eine neue Dimension der **Entfremdung von Arbeitnehmer- und Arbeitgeberseite.**

Dagegen gilt es, wertorientierte Vorstellungen von „guter digitaler Arbeit“ zu entwickeln. Rechtlich stellt sich hier die besondere Herausforderung, dass die Datenschutzgrundverordnung (DSGVO) zwar das Verhalten von Arbeitgebenden (als Verantwortliche) und von Auftragsverarbeitern (also Dienstleistern) regelt, **nicht aber die Entwickler und Anbieter von Überwachungssoftware oder -produkten** in den Blick nimmt. Viele Arbeitgebende verlassen sich jedoch darauf, dass diese Anbieter nur rechtskonforme Leistungen erbringen – was gerade bei außereuropäischen Anbietern aber keinesfalls garantiert ist. Daher müssen auch Drittanbieter in die Pflicht genommen werden.

Die meisten Unternehmen nutzen unter anderem IT-Systeme und Anwendungen von Großkonzernen wie Microsoft, Google, Amazon oder OpenAI. Häufig werden bei der Nutzung von solchen Systemen Daten von Beschäftigten erfasst und Kontrollmöglichkeiten eröffnet, die für eine Großzahl der Unternehmenskund:innen gar nicht erstrebt werden oder unerheblich sind.

Halten in dieser Konstellation zur Kontrolle geeignete Funktionen in den Betrieben Einzug, wird dadurch ein erheblicher Überwachungsdruck auf Beschäftigte aufgebaut. Deshalb ist es ratsam, die „Datensammelwut“ bereits bei der Konstruktion der Software auf Herstellerseite zu begrenzen und den Kund:innen die systemseitige Möglichkeit zu bieten, **Überwachungstools vollständig nach den eigenen Nutzungsvorstellungen zu konfigurieren.** Indem Privacy by Design für Unternehmenssoftware gesetzlich verbindlich auch für Entwickler und Anbieter gemacht wird, würde Datenschutzkonformität für die Software-Anbieter zwar voraussetzungsvoller, aber für die breite Masse der Anwender:innen würde der Nutzungsaufwand und für die Arbeitnehmenden der Überwachungsdruck am Arbeitsplatz enorm abnehmen. Dieser Ansatz wird von Arbeitgebenden wie von Arbeitnehmenden begrüßt und hat auch nach Auffassung des RDÖ hohe Priorität.

Die **Regulierung** von digitalen Mitteln der Kontrolle am Arbeitsplatz ist daher **sinnvoll und notwendig**, sowohl mittels rechtlicher Vorgaben als auch anhand außerrechtlicher Maßstäbe einer Daten-Ethik.

Der RDÖ empfiehlt daher, die Regelungen des **Bundesdatenschutzgesetzes** in Bezug auf digitale Überwachungsmaßnahmen **zu ergänzen und zu konkretisieren**. Ein **umfassendes Beschäftigtendatenschutzgesetz** sollte darauf abzielen, die Freiheitsrechte und den Datenschutz von Mitarbeiter:innen im digitalen Zeitalter zu schützen.

Zentral sind dabei **Verhältnismäßigkeit und Fairness jeder Kontrolle:**

- Es gilt der **Grundsatz der Datenminimierung:** Es dürfen nur die Daten erhoben werden, die wirklich notwendig sind, um den festgelegten Zweck zu erreichen. Damit wird die Überwachung am Arbeitsplatz auf das Notwendige reduziert.
- **Keine Totalüberwachung** am Arbeitsplatz, die sämtliche Leistungen des Arbeitnehmenden erfasst und vollumfänglich mitprotokolliert
- **Keine pauschale Überwachung** aller Arbeitnehmenden in sämtlichen Arbeitsbereichen; Kontrollmaßnahmen müssen **personell und zeitlich begrenzt sowie differenziert sein**
- **Keine unangemessene Überwachung**
- Gemessen am **Ziel** der Überwachung: Arbeitgebenden dürfen nur mit Blick auf erhebliche eigene Interessen kontrollieren, nicht wegen Kleinigkeiten oder Formalien. Es gilt der **Grundsatz der Verhältnismäßigkeit.**

- Gemessen am **Gegenstand** der Überwachung: Kontrollen während der Mittagspause oder im Bereich der **Privatsphäre**, etwa von Pausenräumen oder Toiletten, sind tabu. Das gilt besonders für die Nutzung **sensibler Daten** (Gesundheitsdaten/biometrische Daten/ethnische Herkunft) zu Kontrollzwecken.
- Gemessen am **Ergebnis** der Überwachung: Kontrollmaßnahmen dürfen nicht dazu führen, dass Mitarbeitende völlig durchleuchtet und kategorisiert werden (**Verbot von Profiling**).

Dies spricht aus Sicht des RDÖ klar für ein

- **Verwertungsverbot für Daten**, die entgegen diesen Prinzipien erhoben oder genutzt werden.

Ein solches Gesetz würde sicherstellen, dass die Rechte und Freiheiten der Mitarbeitenden gewahrt bleiben, während gleichzeitig die berechtigten Interessen der Arbeitgebenden geschützt werden. Es würde einen klaren rechtlichen Rahmen schaffen, der die berechtigten Interessen der Betriebsparteien schützt und Vertrauen sowie Transparenz fördert.

Mit diesen Maßgaben kann der **wertebasierte Einsatz von digitaler Technik am Arbeitsplatz** gelingen: In einem auf gegenseitigem Vertrauen basierenden Arbeitsverhältnis steht die Achtung vor den Arbeitnehmenden als individuelle Persönlichkeiten mit eigenen Rechten und ihr Anspruch auf Schutz vor Ausspähung und Diskriminierung im Mittelpunkt.

Inhalt

EINLEITUNG

Im ausgehenden 18. Jahrhundert entwarf Samuel Bentham ein Manufakturgebäude für den belarussischen Fürsten Potemkin, in dem „dessen ungelernte Leibeigene nach europäischem Vorbild an regelmäßige Arbeit und differenzierte Arbeitsteilung gewöhnt werden sollten“ (Kaschadt, 2001). In seinem Gebäude konnte dieser „Gewöhnungs“-Prozess aus einer zentralen Position heraus überwacht werden. Es waren diese Pläne, die Benthams Bruder Jeremy zu seiner berühmten Gefängnisarchitektur inspirierten, die als „Panoptikum“ bis heute als weitverbreitete Überwachungsmetapher dient. Es ist gewiss kein Zufall, dass diese symbolträchtige „architektonische Umsetzung der Macht des Blicks“ (Kaschadt, 2001) dem Arbeitskontext entstammt.

Denn der Arbeitgebende ist darauf angewiesen, dass die Arbeitsleistung wie vereinbart geleistet wird. Auf der anderen Seite benötigt der Arbeitnehmende den Lohn, um seinen Lebensunterhalt zu bestreiten. Das Arbeitsverhältnis ist demnach ein soziales Nähe- und Abhängigkeitsverhältnis, in dem Arbeitgebende und Arbeitnehmende gemeinsam Mehrwert schaffen. Eine Kombination aus Vertrauen und Kontrolle ist eine zentrale Voraussetzung, um die Stabilität des Arbeitsverhältnisses zu gewährleisten und die Partikularinteressen beider Parteien in Balance zu halten. Ob es sich um eine ausgewogen symbiotisch-respektvolle Beziehung oder um eine einseitig-ausbeuterische handelt, hängt von der konkreten Ausgestaltung des Arbeitsverhältnisses ab, unter anderem also auch davon, wie Kontrolle ausgeübt wird.

In der analogen Welt, also für die längste Zeit, gestaltete sich Kontrolle am Arbeitsplatz persönlich, offen und stichprobenartig. Arbeitsplätze wurden in der Regel nicht nach dem panoptischen Prinzip eingerichtet, auch wenn Großraumbüros teilweise nach ähnlichen Logiken funktionieren. Somit herrschte bislang weder ständige Beobachtung vor, noch wurde den Arbeitnehmenden die Möglichkeit einer durchgehenden Überwachung suggeriert. Genau das steht aber heute im Raum, seit Arbeit immer umfassender digitalisiert wird: Je mehr „Datenspuren der Arbeit“ anfallen, etwa in Form von Kommunikation, Logdateien oder Bewegungsdaten, desto lückenloser wird die Nachvollziehbarkeit, desto eher findet sich der Arbeitnehmende in einer panoptischen Situation wieder.

Die Digitalisierung der Arbeit birgt Möglichkeiten in sich, die sich in ganz unterschiedliche

Richtungen entfalten können. Wie für solche Basistrends üblich, wohnen auch der Digitalisierung mehrere Logiken inne. So gibt es neben der sehr dominanten Logik der Ökonomisierung und Rationalisierung auch hier eine Logik der Humanisierung, die Arbeitsbedingungen verbessern könnte. Diese Logiken konkurrieren in einem gesellschaftlichen Aushandlungsprozess miteinander, wie man gerade besonders gut an den Debatten um flexible Arbeitsgestaltung oder um Künstliche Intelligenz beobachten kann.

Viele gehen davon aus, dass alles in der Wirtschaft, was digitalisiert werden kann, digitalisiert werden wird. Es bleiben dann kaum Prozesse, die sich anhand der hinterlassenen Datenspuren nicht mehr nachvollziehen lassen. Es hängt von rechtlichen Vorgaben, gelebter Arbeitskultur und anderen Formen der Regulierung ab, was von diesen Möglichkeiten sich im jeweiligen Betrieb bzw. am jeweiligen Arbeitsplatz auch als Wirklichkeit durchsetzt.

Es ist deshalb eine wichtige Frage, wie es gelingt, die Arbeitswelt so zu regulieren, dass die Rechte der Beschäftigten geschützt werden, ohne die digitalen Möglichkeiten und damit verbundene Chancen der Innovation und der Effizienzsteigerung übermäßig zu beschränken. Auf den folgenden Seiten wird zunächst nachgezeichnet, wie sich Arbeit durch die Digitalisierung verändert hat. Danach illustrieren Fallbeispiele die neuen Möglichkeiten von digitaler Kontrolle. Der Blick auf die bestehende Rechtslage offenbart erhebliche Defizite im Umgang mit der vernetzten Arbeitswelt. Schließlich werden Handlungsbedarfe auf kultureller wie auf rechtlicher Ebene aufgezeigt und ein Prozess skizziert, wie wir als Gesellschaft zu einer zeitgemäßen Kontrolle am Arbeitsplatz finden.

DIGITALE TRANSFORMATION DER ARBEIT

Bereits 1980 wurde die damals noch junge Mikroelektronik als Kern einer dritten industriellen Revolution gelesen (Balkhausen, 1980). Heute antik anmutende Begriffe wie EDV oder „das papierlose Büro“, später Informations- und Kommunikationstechnik (IKT),

Internet und Cloud Computing können alle unter den Oberbegriff der Digitalisierung gefasst werden, genauso wie die gerade erst beginnende Adoption von Künstlicher Intelligenz und die algorithmischen Steuerung von Arbeit. Diese Formen der Digitalisierung von Arbeit haben einen regelrechten Schub während der Corona-Pandemie erfahren. Die Digitalisierung von Arbeit hat während der Corona-Pandemie einen regelrechten Schub erfahren. Als viele Tätigkeiten wegen der Lockdowns plötzlich nicht mehr analog absolviert werden konnten, hat sich - auch zur Überraschung vieler Beteiligter - herausgestellt, dass sich die meisten Varianten von Teamarbeit und Abstimmungen zwischen Produzent:innen und Kund:innen auch problemlos aus dem Home Office erledigen ließen. Der RDO hat dazu in einer qualitativen Studie die Auswirkungen der digitalen Transformation auf Beschäftigte untersucht. Dabei wurden von den Beteiligten als positive Aspekte verstärkte Teilhabe, Erhöhung von Effizienz, Vermeidung von Fahrtwegen etc. hervorgehoben (Czichi-Welzer & Welzer, 2021).

Die digitale Transformation der Arbeitswelt ist, mal rascher und mal gemächlicher, in vollem Gange. „Die Arbeitswelt“ eines jeden Beschäftigten sieht natürlich sehr unterschiedlich aus – schließlich unterscheidet sich Büroarbeit beträchtlich von der Arbeit in einer Fabrikhalle oder im mobilen Pflegedienst. Dies gilt etwa, was den Autonomie- und Mitbestimmungsgrad betrifft (wie stark also die eigene Arbeit selbst und gemeinsam gestaltet werden kann), welche Arbeitsmittel zum Einsatz kommen oder welche gesetzlichen Anforderungen bestehen. Trotzdem gibt es einige übergeordnete Entwicklungen, die mit der digitalen Transformation der Arbeit erkennbar zusammenhängen:

Mehr Daten

Die Digitalisierung geht einher mit einer neuen Qualität der datentechnischen Erfassung von Arbeitsvorgängen, bei der eine exponentiell gesteigerte Quantität an Daten produziert und ausgewertet wird. Allein diese Tatsache zeigt, dass die Fragen „Was wird erfasst?“ und „Wer hat Zugriff auf das Erfassungsresultat?“ für die Organisation dieser Arbeitsprozesse von höchster Relevanz sind.

Flexibilisierung der Arbeit

Die Digitalisierung hat die Rahmenbedingungen der Arbeit sehr stark verändert. Das mobile Arbeiten hat z.B. eine sehr viel größere Flexibilität mit sich gebracht, indem zeit- und ortsunabhängiges Arbeiten ermöglicht wurde. Durch das Home Office wurde auch eine neue Stufe der Verschränkung von Arbeitswelt und Privatem vollzogen, die mit einer Entgrenzung von Arbeit einhergeht (Atlas der digitalen Arbeit, 2022, S. 15).

Automatisierung der Arbeit

Die Automatisierung der Arbeit ist Folge des technischen Fortschritts, der gerade im Arbeitsverhältnis zu einer permanenten Umgestaltung von Arbeitsplätzen und ganzen Arbeitsfeldern führt. Mit der Automatisierung geht oft auch eine Intensivierung der Arbeit einher, etwa wenn dadurch eine Person mehr Arbeit erledigen kann, oder wenn weniger Personen nötig sind, um eine gleiche Menge an Arbeit zu bewältigen. Das ist auch der Treiber der aktuellen Euphorie für KI-Systeme in Betrieben.

Einsatz und Macht von Drittanbieter

In der Regel werden die Arbeitsmittel, die in einem Unternehmen genutzt werden, nicht mehr intern produziert und programmiert, sondern von Externen eingekauft. Je nach Spezifizität der Arbeitsmittel, etwa im Bereich der Software, können die Unternehmen deren konkretes Design mehr oder weniger mitbestimmen. Im Falle von digitalen Standardlösungen wie Slack oder Microsoft Office 365 gibt es aber für Arbeitgebende wie für Arbeitnehmende kaum Spielraum, was die Erfassung von Arbeitsleistungen und den Umgang mit Beschäftigtendaten angeht. Externe Anbieter bestimmen durch die von ihnen bereit gestellten Arbeitsmittel wesentliche Teile des Arbeitsprozesses und der Kontrollmöglichkeiten am Arbeitsplatz mit.

Veränderung in der Entscheidungsautonomie

Algorithmisches Management hat zur Folge, dass nur ein „schmaler Grat zwischen der Unterstützung menschlicher Tätigkeiten und Formen der Einschränkung der Entscheidungsautonomie besteht, die mit Arbeitsverdichtung, einer rigideren Kontrolle der Arbeitsleistung und einer Entwertung menschlichen Erfahrungswissens einhergehen kann“ (Enquete-Kommission Künstliche Intelligenz, 2020, S. 309). Damit zusammen hängt auch, dass algorithmische Entscheidungen als vermeintlich rationale und objektive Tatsachen vorgeschoben werden können, obwohl natürlich die Programmierung selbst fehleranfällig und vorurteilsbehaftet sein kann.

Neue Modelle

Mit der fortschreitenden Digitalisierung der Arbeitsverhältnisse entstehen auch neue arbeitsrechtliche Verhältnisse wie z.B. Plattform-Jobs, Soloselbstständigkeit, Click-Worker, Uber oder Handwerker-Plattformen (vgl. auch: „Verwilderung der Arbeitsbeziehungen“). Verstärkt seit der Pandemie wandelt sich auch das konkrete Arbeitsumfeld: An die Stelle von Tätigkeiten vor Ort im Betrieb tritt mehr und mehr das Home Office und der mobile Arbeitsplatz. Selbst dort, wo Arbeitsverhältnisse formal unverändert bleiben, kommt es zu signifikanten Umgestaltungen: Es gibt keine festen Arbeitsplätze mehr im Büro (Stichwort: „Rationalisierung der Raumökonomie“), Zeiten der Nichterreichbarkeit außerhalb des Betriebs werden zum Konfliktpunkt, Arbeitszeiterfassung wird erneut zum Problem und das ortsflexible Arbeiten wirft zahlreiche ungeklärte Fragen im Zusammenhang mit dem Arbeitsschutzgesetz und der Verantwortlichkeit für Datensicherheit auf.

Die Digitalisierung der Arbeitsverhältnisse ist dabei nicht nur gegebene Realität, sie ist immer auch Gestaltungsaufgabe: Führt der Einsatz digitaler Mittel am Arbeitsplatz zu Arbeitsverhältnissen, die fair, gesund, nachhaltig oder auch nur akzeptabel sind? Hier gilt es, wertorientierte Vorstellungen von „guter digitaler Arbeit“ zu entwickeln, welche die technischen Möglichkeiten als das einordnet, was sie sein sollten: Angebote zur Umgestaltung der Arbeitswelt, die man annehmen kann, wenn sie mit unseren Wertvorstellungen harmonieren, und ablehnen muss, wenn sie das nicht tun. Auf dieser Basis können und müssen rechtliche Vorgaben und Regularien formuliert werden, um diesen neuen Lebensraum, der auch immer ein Kontrollraum ist, zu gestalten, um Rechtssicherheit für Arbeitgebende und hinreichenden Schutz für Arbeitnehmende zu schaffen.

BESTANDSAUFNAHME: WIE SIEHT KONTROLLE AM ARBEITSPLATZ AUS?

Die Kontrollmöglichkeiten am Arbeitsplatz sind in Deutschland über Arbeitsrecht und Datenschutz rechtlich reguliert und spiegeln die Kultur der Arbeitsverhältnisse, die von gegenseitigem Respekt und Mitbestimmung geprägt ist. Durch die technisch bedingten Veränderungen der Arbeit stellt sich die Frage, inwiefern die technische Realität, die betroffenen Schutzgüter und das geltende Recht zusammenpassen.

Kontrolle ist dabei kein Fremdkörper, sondern gehört selbstverständlich zu Arbeitsverhältnissen dazu. Der Arbeitgebende gibt die angestrebten Arbeitsergebnisse zu einem erheblichen Grad vor und will sich regelmäßig über den Stand der erbrachten Arbeitsleistungen und den Grad der Zielerreichung informieren. Kontrollen durch den Arbeitgebenden korrespondieren demnach mit seinem Direktionsrecht, also der arbeitsvertraglich vereinbarten Befugnis des Arbeitgebenden, einseitig den Erfolg der Arbeitsleistung zu definieren. Der Arbeitnehmende ist an seinem Arbeitsplatz zudemin einem fremden Bereich, denn der Arbeitgebende ist Hausherr des Arbeitsbereichs. Grundsätzlich ist die Kontrolle durch den Arbeitgebenden daher ein zulässiges Mittel zur Prüfung der Einhaltung von Weisungen und zur Wahrung der Interessen des Arbeitgebenden.

Nichtsdestotrotz ist eine Effizienzsteigerung der Produktionsprozesse nur mit dem Arbeitnehmenden möglich und die Mitbestimmung des Arbeitnehmenden im Unternehmen ist oftmals über einen Betriebsrat (im öffentlichen Sektor entsprechend über einen Personalrat) im Sinne einer Schutzfunktion verankert. Ob solche Kontrollen vom Arbeitnehmenden als Unterstützung, Überwachung oder gar Gängelung wahrgenommen werden, hängt stark vom Verhalten des Arbeitgebenden und seines Führungspersonals ab, aber eben auch von den zum Einsatz gebrachten Kontrollinstrumenten.

Bis weit ins 20. Jahrhundert hinein gab es am Arbeitsplatz zahlreiche Formen von „analoger“ Kontrolle durch Arbeitgebende, die persönlich, offen und stichprobenartig durchgeführt wurde: Der Chef suchte den Arbeitnehmenden am Arbeitsplatz auf, schaute ihm „über die Schulter“ oder ließ sich Arbeitsproben zeigen und gab dann eine Rückmeldung, mit der er seine Einschätzung zur Qualität der Arbeitsleistung oder zu möglichen Verbesserungen

mitteilte und ordnete abschließend den Arbeitsanteil des Arbeitnehmenden in den betrieblichen Gesamtablauf und die Bedürfnisse von Kund:innen und Auftraggeber:innen ein. Diese analoge Form der Kontrolle war für den Arbeitnehmenden oft nicht schön, aber berechenbar: Zum einen kontrollierte der Arbeitgebende offen, d.h. der Arbeitnehmende wusste durch die Anwesenheit des Chefs, dass eine Kontrollsituation vorlag und wann sie wieder beendet war. In größeren Betrieben wurde die persönliche Kontrolle durch den Arbeitgebenden mittels einer Kontrolle durch seine Führungskräfte abgelöst – aber auch hier waren Anwesenheit und Kontrolle miteinander verknüpft.

Zum anderen war Kontrolle die Ausnahme, nicht die Regel: Weder der Arbeitgebende persönlich noch seine Führungskräfte konnten – abgesehen von Ausbildungsverhältnissen oder Situationen des Anlernens neuer Arbeitsschritte – ständig kontrollierend anwesend sein. Somit war Kontrolle im Grundsatz anlassbezogen – etwa, wenn eine Arbeitsleistung im Betrieb nicht weiterverwendbar war oder Beschwerden von Kund:innen über Arbeitsergebnisse vorlagen. Immer aber erfolgte sie stichprobenartig: Nie wurde die gesamte Arbeitsleistung dauerhaft kontrolliert, betrachtet wurden immer nur Ausschnitte des Arbeitsprozesses.

Mit der fortschreitenden Digitalisierung von Arbeitsverhältnissen entwickeln sich auch die Kontrollformen am Arbeitsplatz weiter. Analoge Kontrolle wird zunehmend von digitalen Kontrollformen ersetzt, die nun nicht mehr persönlich, sondern unpersönlich, technikgestützt, automatisiert oder KI-basiert erfolgen. Sie sind für den Arbeitnehmenden auch nicht mehr offen erkennbar, sondern erfolgen, implementiert in Algorithmen und Technik, verdeckt. Dies hat für Arbeitnehmende die unangenehme Folge, dass Zeitpunkt, Dauer und Intensität einer Kontrolle für sie nicht mehr klar abzuschätzen sind – was zu einer als dauerhaft empfundenen, gleichwohl unklaren Überwachungssituation führt. Schließlich erfolgt die digitale Kontrolle auch nicht mehr zwingend stichprobenartig, sondern kann durch die technisch bedingten Effizienzgewinne zugunsten des Arbeitgebenden allumfassend und pauschal sein: nunmehr ist es möglich, jede Arbeitsleistung zu jedem Zeitpunkt in beliebiger Tiefe zu kontrollieren.

Digitale Kontrolle

Der Zusammenhang zwischen Digitalisierung und Kontrolle ist zunächst ganz simpel: Digitalisierung, im Wortsinne eine „Zählbarmachung“, bedeutet zuallererst, dass etwas maschinenlesbar gemacht wird. Die informationstechnische Erfassung schafft immer auch Nachvollziehbarkeit – allein um die grundlegenden Funktionen zu gewährleisten und Fehler aufzuzeichnen, protokollieren Server, Router, Email-Programme und andere Soft-

Welche Daten werden gesammelt?

Bereits für die Unterzeichnung eines Arbeitsvertrags werden die Personaldaten des Arbeitnehmenden benötigt, insbesondere Name, Geburtsdatum, Privatadresse, versicherungspflichtige Daten und Bankverbindung. Da sich diese Angaben zum einen auf eine „natürliche Person“ beziehen und zum anderen diese Person direkt oder indirekt identifizieren, handelt es sich hierbei um **personenbezogene Daten** (Wedde, 2019, S. 129). Weitere gängige Daten, die dem Arbeitgebenden bekannt sind, sind beispielsweise Religion, Familienstand, Gehaltsrechnungen oder bestimmte Gesundheitsdaten.

Neben den genannten personenbezogenen fallen große Mengen weiterer Daten an. Zum einen können mittels digitaler Anwendungen **Kommunikationsdaten** nachvollzogen werden. Darunter fällt jede Art der Kommunikation über ein Diensthandy, das Intranet des Betriebs, Emails, Kalender oder über Software-Programme wie Slack.

Zum anderen können programmgestützt auch die **Leistungsdaten** eines Arbeitnehmenden abgebildet werden. Denn bei jeder Aufgabe, für die Software eingesetzt wird, fallen Daten an. Zusätzlich hat der Arbeitgebende Einsicht in Leistungsdaten aus Arbeitszeugnissen, Kenntnis über leistungsabhängige Vergütungskomponenten (Boni etc.) sowie Arbeitszeitdaten. Weiterhin kann der Arbeitgebende **Verhaltensdaten** über den Arbeitnehmenden erheben.

Diese Informationen aus dem Arbeitsalltag fallen ebenso wie Daten aus dem Privatleben der Arbeitnehmenden, sobald sie vom Arbeitgebenden erfasst und verwendet werden, in den Bereich des Beschäftigtendatenschutzes (Wedde, 2019, S. 132). Der Datenschutz bezieht sich daher auf verschiedenste Arten von Daten, unabhängig davon, warum sie erhoben wurden, wie bekannt sie allgemein sind oder wo sie gespeichert wurden (Wedde, 2019, S. 132).

Viele dieser Daten fallen im alltäglichen Arbeitsprozess an, sie werden demnach nicht explizit zu Zwecken der Kontrolle oder Überwachung erhoben und hätten für sich genommen keine besondere datenschutzrechtliche Bedeutung.

Werden sie jedoch mit personenbezogenen Daten verknüpft, kann sowohl die Leistung als auch das Verhalten einzelner Arbeitnehmender nachverfolgt und analysiert werden. Aus beiläufig erhobenen Daten können daher durch den Einsatz moderner Datenverarbeitungstechnik sehr aussagekräftige Datensätze werden. Neue Analyse- und Auswertungsmöglichkeiten mithilfe von Künstlicher Intelligenz bestätigen danach den Grundsatz, der bereits im Volkszählungsurteil von 1983 vom Bundesverfassungsgericht festgehalten wurde: „Es gibt keine unbedeutenden oder belanglosen Daten“ (Bundesverfassungsgericht, 1983).

ware ihre Prozesse automatisch in einer Log-Datei (oder Protokolldatei). Für digitalisierte Arbeitsschritte fallen also eine Menge Daten an und es ergeben sich neue, computerbasierte Möglichkeiten der Kontrolle. Da diese Informationen permanent erfasst werden, ergibt sich mit digitalen Mitteln eine quantitative Erweiterung der Kontrolle. In Kombination mit Künstlicher Intelligenz ist außerdem ein qualitativer Sprung in der Kontrolle möglich: Künstliche Intelligenz kann dort Muster erkennen, wo für den Arbeitgebenden keine ersichtlich waren und beispielsweise Produktivitätsrankings von Arbeitnehmenden erstellen.

Neue Kontrollformen am Arbeitsplatz können dazu führen, dass Beschäftigte Gefühle der Dauerüberwachung, Dauerbewertung, Dauerkonkurrenz, Verunsicherung und Entfremdung empfinden. Simon Schaupp beschreibt die digitale Überwachung als ein „minutiöses Protokollieren jedes Arbeitsschritts“ (Schaupp, 2021, S. 156). Auf Dauer kann das zu einem Wertewandel und zu einer insgesamt veränderten Arbeitskultur führen. Rechte können eingeschränkt werden, Demotivierungen bis hin zu inneren Kündigungen die Folge sein.

Auch für Arbeitgebende haben digitale Kontrollmöglichkeiten möglicherweise negative Konsequenzen, beispielsweise einen blinden Optimierungsdrang, Datenwust, Kontrollverlust oder Rechtsunsicherheit. Der Optimierungsdrang entsteht aufgrund der neuen Möglichkeiten, die zuvor nicht vorliegende Kennzahlen und Informationen bieten. Doch genau das kann zu einem Datenwust führen: Die Vorgabe der Europäischen Datenschutz-Grundverordnung (DSGVO) zur Datenminimierung wird selten beherzigt und viele Informationen werden nur erhoben, weil es möglich ist, nicht weil es notwendig wäre.

Ein Kontrollverlust kann auf Seiten des Arbeitgebenden entstehen, sobald durch die Nutzung von Drittanbietern für entsprechende Programme die Verhältnisse am Arbeitsplatz komplexer werden. Durch die Nutzung von Drittanbietern macht sich der Arbeitgebende abhängig (auch von technischen Updates), wobei er gleichzeitig seine Datenhoheit einschränkt und trotzdem rechtlich verantwortlich bleibt. Der Einsatz von Dienstleistern führt tendenziell zu einem digitalen Überwachungsüberschuss (vgl. Zuboff, 2018), einer „eingebauten Überwachung“ durch Dienstleister und kann schleichend einen Kulturwandel nach sich ziehen. Schließlich zählt die Rechtsunsicherheit zu einem Risiko für Arbeitgebende. Denn mit den potenzierten Möglichkeiten durch Künstliche Intelligenz werden sich die Formen digitaler Kontrolle und Überwachung am Arbeitsplatz in Zukunft weiter wandeln.

Arbeitsplätze in Deutschland: Fallbeispiele

So divers wie Arbeitsplatz und -alltag sein können, so unterschiedlich wird auch Kontrolle durch den Arbeitgebenden ausgeübt. Auf den ersten Blick scheint es so, dass sich vor allem Arbeitsplätze mit eindeutig definierten Aufgaben und mit starken Machtasymmetrien für eine digitale Überwachung anbieten.

Der folgende Abschnitt zeigt anhand von drei beispielhaften Arbeitsplätzen, dass die digitalen Möglichkeiten der Kontrolle und Überwachung für eine signifikante Zahl von Beschäftigten relevant sind: (1) die Lagerhalle, (2) die mobile Arbeit, die auch die Arbeit bei Kund:innen umfasst, und (3) das Home Office.

Die vorgestellten Arbeitsplätze werden für unsere Zwecke über ihre Rahmenbedingungen und das lokale Setting der Arbeit definiert. So umfasst die mobile Arbeit gleichermaßen die Handwerkerin, die Heizungsentlüfter eines Kunden repariert, den Fahrrad-Kurier, der Essensbestellungen ausliefert und den Pfleger, der Personen in ihrem Zuhause medizinisch versorgt. Analog lässt sich annehmen, dass die meisten Schreibtischjobs das Arbeiten an einem Computer in einem Büro oder im Home Office gemeinsam haben, und dass die Arbeitsleistung im Kontext einer Lagerhalle oder Produktionsstätte in klar strukturierten Bahnen abläuft.

Lagerhalle eines Logistikunternehmens

Das in der Öffentlichkeit wohl bekannteste Beispiel für Überwachung am Arbeitsplatz ist die Lagerhalle von Logistikunternehmen. Die Gegebenheiten des Arbeitsplatzes bieten ideale Voraussetzungen für den Einsatz von dystopisch anmutenden digitalen Kontrolltechniken. Im Folgenden werden diese branchenspezifischen Möglichkeiten der Kontrolle am Beispiel einer Niederlassung von Amazon in Niedersachsen aufgezeigt, die im Zuge eines Rechtsstreits vor dem Verwaltungsgericht Hannover detailliert beschrieben wurde.

Das Logistikzentrum in Winsen (Luhe) beschäftigt auf 64.000 Quadratmetern bis zu 2.200 Mitarbeitende, welche im Schnitt 153 Pakete pro Minute versenden. Das bedeutet, dass „[…] zwischen dem Auftragseingang und dem Zeitpunkt, zu dem das Paket spätestens an den Transporteur übergeben sein muss“, nur vier Stunden liegen (Verwaltungsgericht Hannover, 2023). Die Mitarbeitenden verteilen sich dabei auf drei verschiedene Arbeitsbereiche: den Wareneingang, die Prozessplattform und den Warenausgang. Dort sind die Beschäftigten nach dem Entladen und der Annahme für die Einlagerung („receiver“ und „stower“), Entnahme („picker“) und Verpackung („packer“) von Waren in Pakete zuständig (Christl, 2021, S. 127).

Dabei arbeiten die Beschäftigten unter „kleinteiliger Anleitung und Kontrolle“ (Christl, 2021, S. 127) durch einen Handscanner. Letzterer zählt zu den „Wearables“ - es handelt sich um einen Handschuh, in dem eine Software integriert ist (Voigt, 2021, S. 5). Dieser speichert verschiedenste Informationen, so z.B. welche Ware in welchem Regalfach deponiert wird. Später werden die Waren in ihren jeweiligen Paketen nach Transportdienstleistern sortiert. Für den Transport innerhalb des Zentrums kommt ein Fördersystem mit einer Länge von etwa 25 Kilometern zum Einsatz. Um zu erfassen, welche Ware aus einem welchem Regalfach genommen und auf welches Transportband gelegt wird, kommt eben-

Gerichtsverfahren gegen Amazon

Im Rechtsstreit zwischen dem Warenlieferanten Amazon und Barbara Thiel, der damaligen Landesbeauftragten für Datenschutz in Niedersachsen, ging es 2019 um die Frage, ob die Kontrolle der Beschäftigten in den Logistikzentren datenschutzkonform ist. Den Vorwürfen nach könnten Vorgesetzte nicht nur den Aufenthaltsort/Standort eines Beschäftigten im Logistikzentrum, sondern ebenso seine Leistungsdaten in Echtzeit nachvollziehen – diese „umfassende Erhebung personenbezogener Daten“ wurde aus behördlicher Sicht als ein „Fall der Totalüberwachung“ verstanden. Nach Auffassung der Landesbeauftragten für Datenschutz verstieß Amazon gegen BDSG und DSGVO (genauer: § 26 Abs. 5 BDSG in Verbindung mit Art. 5 DSGVO und Art. 22 Abs 1 DSGVO) und handelte rechtswidrig.

Mit behördlicher Anordnung wurde dem Online-Giganten erstens die Verarbeitung von „ununterbrochen erhobenen jeweils aktuellen und minutengenauen Quantitäts- und Qualitätsleistungsdaten der Beschäftigten“, zweitens die Bildung darauf aufbauender Leistungsprofile der Beschäftigten und drittens das Führen daran gekoppelter Feedbackgespräche untersagt.

Doch Amazon wehrte sich gegen diese Anordnung und klagte im Herbst 2020 gegen den Bescheid vor dem Verwaltungsgericht – und gewann. Im Gerichtsverfahren vertrat das Verwaltungsgericht Hannover die Auffassung, dass die Datenverarbeitung auf die DSGVO und das BDSG (genauer: Art. 88 Abs. 1 DSGVO in Verbindung mit § 26 BDSG) gestützt werden könne (Urteil v. 9.02.2023, Az. 10 A 6199/20, 2023).

Die umfassende technische Überwachung sei durchaus transparent und diene der Effizienz des Unternehmens sowie den Beschäftigten selbst, die sich durch weniger leistungsfähige Kolleg:innen in ihrer eigenen Leistungsentfaltung gehindert sehen könnten.

Auf die Frage einer bereits arbeitsrechtlich unzulässigen Totalüberwachung am Arbeitsplatz bei Amazon ging das Verwaltungsgericht Hannover nicht näher ein, auch datenschutzrechtliche Mängel bei der Transparenz der Überwachungstechnik und eine mangelnde Verhältnismäßigkeit ihres Einsatzes vermochte das Verwaltungsgericht nicht zu erkennen. Es bleibt abzuwarten, wie das Oberverwaltungsgericht Niedersachsen über die eingelegte Berufung der Datenschutzbeauftragten entscheiden wird.

falls der Handscanner zum Einsatz. Es zeigt sich: “Bei der Verrichtung ihrer Arbeit auf den verschiedenen Prozesspfaden benutzen die dort eingesetzten Mitarbeiterinnen und Mitarbeiter […] Handscanner, um jeden ihrer Arbeitsschritte zu dokumentieren.“ (Verwaltungsgericht Hannover, 2023).

Bei Amazon fließen alle durch den Handscanner erhobenen Daten anschließend in die Software „Fulfillment Center Labor Management” (FCLM). FCLM kann daraufhin beispielsweise Informationen über die Leistung von einzelnen Mitarbeitenden auf einem Prozesspfad ausgeben und sehen, wie viele Waren pro Stunde dabei abgefertigt wurden („units rollup“). Andere Daten umfassen die bearbeiteten Einheiten („units processed“), gearbeitete Stunden und Qualität der Leistungserbringung („defects per million opportunities“). Aber auch Pausenzeiten („time off task“) werden minutiös protokolliert. So sind pro Schicht 30 Minuten vorgesehen, in die der „Gang zur Toilette, das Nachfüllen der Wasserflasche oder ein Gespräch mit dem Vorgesetzten“ fallen (Christl, 2021, S. 129).

Diese Daten nutzen Vorgesetzte, um Leistungsschwankungen auf den einzelnen Prozesspfaden abzufedern. So können sie, sobald Mitarbeitende nicht „mit einem durchschnittlichen Durchsatz“ (Verwaltungsgericht Hannover, 2023) arbeiten, Ressourcen hin- und herschieben. Gemeint sind hier Kolleg:innen, welche an den jeweiligen Stellen im Prozesspfad anderen Beschäftigen zu Hilfe kommen. Für diese Art des Monitorings einzelner Arbeitsprozesse werden die Daten durch FCLM in Echtzeit erhoben.

Anschließend werden die Informationen in der Anwendung „Associate Development and Performance Tracking“ (ADAPT) analysiert. Denn ADAPT bewertet aufbauend auf FCLM die aktuelle Leistung eines Beschäftigten, den Leistungstrend und die Lernkurve. Die Anwendung dient demnach der objektiven Leistungsbewertung und generiert Feedbackvorschläge, die auch bei Personalentscheidungen wie etwa einer Entfristung berücksichtigt werden. Fließen Daten in eine Klassifizierung und schließlich in Entscheidungen zu Gehalt und Beförderung ein, so z.B. in der Funktion „Anytime Feedback Tool“ von Amazon, spricht man von „algorithmischem Management“ (Dietrich et al., 2021, S. 6).

Es zeigt sich, dass im lokalen Setting einer Lagerhalle die notwendigen Arbeitsschritte nahezu vollständig digitalisiert wurden und dass die Echtzeitdokumentation und auswertung ein hohes Maß an Kontrolle ermöglicht. Beschäftigte berichten, sich als Teil einer Maschine zu fühlen und laut der Vereinten Dienstleistungsgewerkschaft (ver.di) hat eine solche Arbeitsweise negative Auswirkungen auf die Gesundheit der Beschäftigten: Die Krankenquote liege an manchen Tagen bei über 20 Prozent, wobei Muskel- und Skeletterkrankungen und psychische Erkrankungen vorherrschend sind (Krähling, zit. in Enquete-Kommission Künstliche Intelligenz, 2020, S. 294).

Mobiles Arbeiten

Mobiles Arbeiten charakterisiert sich dadurch, dass die Beschäftigten zu ihren jeweiligen Patient:innen oder Kund:innen kommen und im Verlauf des Arbeitsalltags den Einsatzort ständig wechseln. Diese Besonderheit konnte in der Vergangenheit die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebenden erheblich einschränken. Doch inzwischen nutzen diese Berufsgruppen oftmals Diensthandys mit spezifischen Programmen und Zugängen zu Systemen, um ihre Arbeit zu verrichten. Durch das kontinuierliche Nutzen und Mitführen des Smartphones können der Aufenthaltsort mittels GPS-Signal verfolgt und Zeiträume sowie Arbeitsschritte exakt dokumentiert werden. Die Systeme werden zur Optimierung von Arbeitsschritten beworben, also zur Kontrolle der Dauer von

Arbeitsschritten, zur Einsparung von nicht notwendigen Prozessen sowie zum Leistungsvergleich in einzelnen Quartalen. Inzwischen erfassen jedoch immer feingliedrigere Updates zunehmend engmaschiger die Arbeitsschritte und Prozesse im mobilen Arbeiten.

Ein extremer Fall des mobilen Arbeitens sind dabei die Kurier:innen von Essenslieferdiensten. Diese werden nicht nur gegenüber dem Arbeitgebenden durchsichtig, sondern auch durch die Kund:innen laufend beobachtet und bewertet. Die Koordination zwischen Gastronomiebetrieben, Kund:innen und der Fahrradzustellflotte wird über digitale Plattformen abgewickelt, wobei weitgehend alle Prozessschritte automatisiert und miteinander verknüpft sind.

Ein Auftrag beginnt mit der Bestellung eine:r Kund:in über die Homepage oder App der Plattform. Ebenso wie ein mobiler Pflegedienst oder ein Handwerksbetrieb nutzen auch die Beschäftigten eines Lieferdienstes eine App auf ihrem Smartphone, um die Lieferaufträge der Bestellungen entgegenzunehmen. Der Auftrag gibt dabei an, wo der Zulieferer die Bestellung abholt, wobei vor Ort noch einmal bestätigt werden muss, dass es sich bei der erhaltenen Ware um die Richtige handelt. Erst im Anschluss erhalten die Kurier:innen die Information, wohin die Bestellung zu liefern ist. Bei der Ankunft am Ziel muss der Auftrag zum Abschluss noch bestätigt werden. Der Zusteller wird dabei über den gesamten Arbeitstag hinweg per GPS-Signal geortet (Voigt, 2021, S. 8). Auf diese Weise wird die mobile Arbeit engmaschig kontrolliert und überwacht. Darüber hinaus erfolgt auch die Erstellung von Dienst- und Schichtplänen mit KI-Systemen und kann bereits als automatisiertes Management verstanden werden (Christl, 2021, S. 55).

Im Falle der Essenslieferdienste können die automatisiert verteilten Aufträge nicht abgelehnt werden. Und wenn Aufträge verzögert angenommen werden, kann es zu automatischen Sanktionen kommen. Dazu kommen Sanktionsmöglichkeiten auf Basis eines Ranking-Systems, bei dem einzelne Daten und Informationen gewichtet werden, z.B. die Anzahl der ausgeführten Aufträge im Vergleich mit anderen Beschäftigten. Ein gutes Ranking beeinflusst zukünftige Arbeitsschichten und auf lange Sicht das Einkommen des Zustellers. Denn auf das Grundgehalt der Beschäftigten können auf der Basis von zurückgelegten Kilometern und der Anzahl an Aufträgen Boni ausgezahlt werden. Zusammengefasst besteht also ein hoher und durchgehender Überwachungsdruck, wobei nicht-optimales Verhalten direkt bestraft wird.

Home Office

Grundsätzlich gilt bei der Mitarbeiterüberwachung im Home Office nichts anderes als am üblichen Arbeitsplatz: Technisch ist vieles möglich, aber nicht jede Form der Überwachung ist zulässig.

Grundsätzlich gilt bei der Mitarbeiterüberwachung im Home Office nichts anderes als am üblichen Arbeitsplatz: Technisch ist vieles möglich, aber nicht jede Form der Überwachung ist zulässig.

2023 arbeiteten 23,5 Prozent der Erwerbstätigen in Deutschland ganz oder teilweise im Home Office, wobei eine Mehrheit dem ortsflexiblen Arbeiten positiv gegenübersteht (Bitkom e.V, 2022). Besonders geschätzt werden der Wegfall des Arbeitswegs, die selbstbestimmte Zeitgestaltung oder der Umstand, dass man weniger durch Kolleg:innen abgelenkt wird. Wenn die Arbeitnehmenden nicht mehr vor Ort tätig sind, wirkt sich das auch auf die Beziehung zu den Vorgesetzten und deren Möglichkeiten zur Kontrolle aus. Auf den ersten Blick scheint der Umzug des Arbeitnehmenden in die eigenen vier Wände mit einem Autonomiezuwachs und weniger Überwachungsdruck einherzugehen, da die direkte Aufsicht abnimmt. Da man aber auch im Home Office in aller Regel auf digitale Arbeitsmittel angewiesen ist und auf die eine oder andere Weise mit dem Unternehmen in Kontakt steht, ergeben sich in dieser Konstellation umfangreiche Möglichkeiten der Kontrolle.

Weiterhin möglich sind auch im Home Office stichprobenartige Überprüfungen, etwa durch einen Anruf. Doch ist auch eine umfassende Kontrolle möglich, da die Anwendungen, die auf privaten oder zur Verfügung gestellten Geräten laufen, zweckentfremdet und zur Überprüfung und Überwachung der Arbeitsleistung genutzt werden können. Neben Informationen aus Kalendereinträgen, Videokonferenz-Software und Projekterfassung-Tools eignet sich hierzu auch das weit verbreitete Paket Microsoft Office 365.

Mit Microsoft Office 365 können nicht nur Programme wie Word, Excel und Email genutzt werden, die Software kann das Verhalten und die Aktivitäten eines Nutzerkontos speichern. Grundsätzlich gilt, dass „sobald am PC gearbeitet wird, [..] umfassende Daten über Arbeitstätigkeiten aufgezeichnet“ (Christl, 2021, S. 16) werden.

Ein cloudbasierter Produktivitäts-Score zeigt für das gesamte Unternehmen an, wie „produktiv“ gearbeitet wird. Diese „Einführungsbewertung“ besteht aus mehreren Datenkategorien wie „Kommunikation“, „Inhaltliche Zusammenarbeit“ oder „KI-Unterstützung“. Ein

Gesamtergebnis soll dann die „Produktivität“ des Unternehmens wiedergeben, so dass man sich mit Organisationen in derselben Region mit einer ähnlichen Anwender:innenzahl vergleichen kann (Pack et al., 2024). Daran anschließend werden Vorschläge gemacht, wie man den Score der eigenen Organisation verbessern kann, z.B. Personen zu ermutigen, Outlook für Mobilgeräte zu verwenden. Dass die Informationen hierbei einzelnen Mitarbeitenden zugeordnet werden können – z.B. wie häufig Beschäftigte den Chat nutzen, wie viele Emails sie an welchen Tagen verschicken und wie lange sie ihre Kamera bei Videomeetings aktivieren –, wurde nur geändert, nachdem es öffentliche Kritik daran gab (Sokolov, 2020). Nichtsdestotrotz lassen sich Skype, Microsoft Teams, OneNote oder die Office Suite weiterhin auswerten, um zu erfassen, ob die Dienste so angewendet werden, wie es von Microsoft vorgesehen ist.

Datenschützer:innen halten daran fest, dass aktuell einsehbare Informationen die „detaillierte, dauerhafte und nahezu lückenlose Auswertung des Verhaltens“ (Dietrich et al., 2021, S. 7) ermöglichen. Im Grundsatz ist es also möglich, mit Hilfe von Business-Intelligence-Software Arbeitnehmende auch im Home Office umfassend zu kontrollieren. Diese elektronische Überwachung ist effektiver, als es menschliche Kontrolle am Arbeitsplatz je sein könnte.

Spionage-Software

Die dauerhafte und vollständige Überwachung von Beschäftigten ist heute mithilfe von digitalen Mitteln technisch möglich. In extremen Fällen werden Anwendungen genutzt, die explizit zu diesem Zweck konzipiert worden sind. Doch auch bevor es zur Totalüberwachung kommt, können Verhalten und Intention von Arbeitnehmenden analysiert und mitunter automatisch von algorithmischen Systemen als „bedenklich“ oder „gefährlich“ eingestuft werden. In diesem Fall machen sich Arbeitgebende jene Programme zu eigen, die bereits für betriebliche Prozesse im Alltag verwendet werden und deren Daten schon vorliegen – die also gemeinhin als „unverdächtig“ eingestuft werden.

Die Anreicherung und Verknüpfung dieser programmgestützten Daten mit weiteren Informationen eröffnen vorher nicht dagewesene Möglichkeiten, Arbeitnehmende zu analysieren, zu bewerten und zu kontrollieren. Hier zeigt sich die ganze Bandbreite von Kontrolle und Überwachung am Arbeitsplatz anhand unterschiedlicher Anwendungen, die

zunächst „nur“ Kontoaktivitäten erfassen und Rankings für algorithmisches Management nutzen (sogenannten „People Analytics“), bis hin zu klar als solcher bezeichneter „Überwachungssoftware“ (Dietrich et al., 2021).

Die Intensität der Überwachung kann hinsichtlich der Dauer der Überwachung oder des Grades der Personenbezogenheit bewertet werden. Unterschieden werden kann Software, die Arbeitsschritte aufzeichnet, betriebliche Prozesse vorgibt und Pausenzeiten begrenzt, und Software, die im Hintergrund läuft und bei ungewöhnlichem Verhalten Alarm schlägt, um den Schutz von Eigentum und Sicherheit des Arbeitgebenden zu gewährleisten (Kartheuser & Pabst, 2023).

Process Mining / Data Mining / Task Mining / Leistungsdaten

Wenn Daten, die durch im Betrieb genutzte Anwendungen anfallen, erfasst und ausgewertet werden, spricht man von „Process Mining“ (Christl, 2021, S. 95). Welche Daten das sein können, lässt sich gut an einem Beispiel skizzieren: So laufen circa „drei Viertel aller Unternehmensbuchungen auf der Welt“ über Systeme des Software-Unternehmens SAP (Freytag, 2022). SAP bietet verschiedenste Software-Programme an, am bekanntesten ist wohl das Standardsoftware-Programm ERP. Die Abkürzung steht für „Enterprise Resource Planning“ und dient, ganz wie der Name beschreibt, der Beplanung von Ressourcen innerhalb eines Unternehmens: die Abwicklung und Steuerung sämtlicher Prozesse von Einkauf und Produktion über Lagerung, Vertrieb, Logistik, Buchführung und Personalwesen. Im Ergebnis wird für die Materialbestellungen bis hin zur Rechnungsabwicklung im gesamten Betrieb ein und dasselbe System genutzt – und alle Daten werden zentral gesammelt (SAP Business One, o. J.).

Eines der Programme, die „Process Mining“ nutzen, ist die 2011 in Deutschland entwickelte Software Celonis. Diese greift auf die Ereignisprotokolle aus ERP-Systemen von SAP, Oracle, Microsoft oder Salesforce zurück und führt diese Daten in Echtzeit zusammen. Somit können „Abläufe, Arbeitsschritte und Tätigkeiten“ im Betrieb mit Zeitstempeln nachverfolgt werden. Sind diese Prozesse identifiziert, werden sie zu weiteren Eckdaten wie Bearbeitungsdauer und -kosten oder Kundenzufriedenheit in Relation gesetzt. So sollen Prozesse „hinsichtlich strategischer Ziele standardisiert, rationalisiert, optimiert und automatisiert werden“ (Christl, 2021, S. 95). Mit diesem Wissen kann schließlich für alle Prozesse im Betrieb ein „optimaler Verlauf“ definiert werden – und es wird klar erkennbar, wenn davon abgewichen wird und durch wen.

In diesem Fall markiert Celonis die Situation als „unerwünschte Aktivität“ und zeigt auf, wie oft diese Abweichung auftritt. In den Daten zur Ursache der „unerwünschten Aktivi-

tät“ können auch personenbezogene Informationen enthalten sein. Ergänzend zu den Informationen über betriebliche Prozesse bietet Celonis außerdem die Funktion des „Task Mining“ an, wobei Daten aus Emails, Excel oder Webseiten mit Zeitstempeln nachvollziehbar gemacht werden. Nicht nur wann, von wem, und wie lange ein Programm genutzt wurde, sondern auch was genau währenddessen und zwischendurch gemacht wurde, kann damit nachvollzogen werden – inklusive Mausklicks, Scrollen und Tastatureingaben (Christl, 2021, S. 97).

Ähnlich wie Celonis verknüpft auch die in deutschen Unternehmen genutzte Software Forcepoint verschiedene Datenquellen, wie beispielsweise Microsoft Office, Skype, Slack und GPS-Programme. Das Programm protokolliert, welche Anwendungen wie genutzt werden und wertet Kommunikation, z.B. automatisch transkribierte Telefonate, inhaltlich aus. Forcepoint soll dabei etwa erkennen können, ob Beschäftigte finanzielle Schwierigkeiten haben, kündigen wollen oder wie viel sie mit Kolleg:innen sprechen. Erkennt die Künstliche Intelligenz „auffällige“ Beschäftige, werden dem Arbeitgebenden Chats und Emails zu lesen angeboten (Wolfangel, 2021).

People Analytics / Verhaltensdaten

> *„Insbesondere mit Blick auf die heutigen Datenverarbeitungsmöglichkeiten ist davon auszugehen, dass der Arbeitgeber auch dort ohne großen Aufwand einen Personenbezug herstellen kann, wo ein solcher nicht direkt gegeben ist. […] Daher sollten Beschäftigte und vor allem Betriebs- und Personalräte stets davon ausgehen, dass ein Personenbezug zu einzelnen Informationen möglich ist.“*
> *(Wedde, 2019, S. 150)*

Anders als Celonis und Forcepoint gibt es auch Programme, deren Fokus weniger auf den arbeitsrelevanten Tätigkeiten der Arbeitnehmenden als auf deren Einstellungen und Stimmungen liegt. Um das Verhalten einzelner Beschäftigter antizipieren zu können, werden sogenannte „People Analytics“ genutzt.

Hierbei werden existierende Informationen aus dem Personalwesen sprich: personenbezogene Daten mit weiteren Daten verknüpft, um Engagement, Produktivität und Zufriedenheit der Arbeitnehmenden zu analysieren. Diese Daten können aus Betriebsumfragen und sogar aus externen Quellen wie Social-Media-Profilen stammen. Stehen solche Daten für sich allein, sind sie noch nicht besonders aussagekräftig. Werden sie jedoch mit personenbezogenen Daten verknüpft, so zeigen sich - laut Eigenwerbung – Ursache und

Wirkung einzelner Prozesse. Ein anschauliches Beispiel dafür sind die Daten zur Route einer Email, Betreff und Empfänger. Stehen diese Informationen für sich allein, sagen sie wenig, verknüpft man sie jedoch mit weiteren personenbezogenen Daten, kann analysiert werden, welche Mitarbeitende Gespräche anstoßen, Meinungen formen, Einstellungen festigen und Gegenpositionen zur Geschäftsführung beziehen.

Die Anwendung von People Analytics verspricht zudem, die Kausalzusammenhänge zwischen neuen Einstellungen und Kündigungen aufzudecken sowie zu zeigen (und zu erklären), in welcher Betriebsabteilung die meisten Krankheitsfälle gezählt werden. Die Informationen und der Erkenntnisgewinn durch die Verknüpfung von Daten sollen der Zufriedenheit der Mitarbeitenden sowie deren Entwicklung, der Förderung von Führungskräften sowie der Prognose von Entwicklungen im Betrieb dienen. Bekannte Software zur People Analytics sind IBM Watson Talent Insights, SAP Workforce Analytics und Oracle Cloud HCM (Dietrich et al., 2021).

Die Analyse von Intention und Verhalten der Beschäftigten hat besonders in der Finanzbranche einen hohen Stellenwert. Obwohl Arbeitnehmende hier zur Wahrung von Geschäftsgeheimnissen sowieso vertraglich verpflichtet sind, werden Beschäftigte mitunter gesondert analysiert und beobachtet, um Arbeitgebende vor „Risiken durch Arbeitnehmer“ zu schützen. So auch mit der Software Securonix, die Browserverläufe, Emails und deren Inhalte sowie Daten zur Nutzung von Programmen sammelt, um ungewöhnliches Verhalten von Arbeitnehmenden im Vorhinein zu erkennen. Die Daten werden für mehrere Jahre gespeichert, um einen Risiko-Score für jeden Mitarbeitenden zu berechnen. In Deutschland wird Securonix z.B. von der Hypovereinsbank genutzt.

Workforce Analytics

Als letzte Abstufung im Rahmen der digitalen Kontrolle und Überwachung gibt es unverblümt als „Überwachungssoftware“ beworbene Programme. Zu ihnen zählen ActivTrak, InterGuard, Time Doctor und VeriClock. Diese Software-Systeme erfassen nicht nur automatisch die Arbeitszeiten von Mitarbeitenden, sondern machen auch detailliertere Angaben beispielsweise zur Nutzung einzelner Programme am Arbeitsplatz. Weiterhin werden der Bildschirm mittels regelmäßiger Screenshots und die Tastatureingaben mit Keyloggern getrackt. Ein Keylogger kann auch dazu verwendet werden, um beispielsweise Passwörter oder sensible Informationen in Erfahrung zu bringen. Ein Keylogger kann sichtbar als Gerät zwischen der Tastatur und dem Computer (Hardware-Keylogger) oder unsichtbar als Programm (Software-Keylogger) installiert werden. Diese Arten von Überwachungssoftware sind „so konzipiert, dass sie unbemerkt von den betroffenen Beschäf-

tigten laufen“ (Dietrich et al., 2021, S. 6). Bereits 2017 erklärte das Bundesarbeitsgericht (BAG) die Nutzung von Keyloggern in Deutschland für unzulässig (Bundesarbeitsgericht, 2017, Az. 2 AZR 681/16).

Wichtig zu wissen ist, dass in Deutschland bei vielen Formen digitaler Kontrolle am Arbeitsplatz vorher eine Einverständniserklärung der Mitarbeitenden eingeholt wird. Doch in vielen Fällen fühlen sich Beschäftigte unter Druck gesetzt, den Regelungen des Arbeitgebenden zuzustimmen (Lang, 2021) oder sehen sich aufgrund seiner Marktmacht gezwungen, zu dessen Konditionen zu arbeiten. In solchen Fällen geht auch die DSGVO von einem „klaren Ungleichgewicht“ (Erwägungsgrund 43 der DSGVO) der Parteien aus, weswegen abgegebene Einwilligungserklärungen als unfreiwillig und damit unwirksam (Art. 4 Nr. 11 DSGVO) anzusehen sind.

Zwischenfazit: Künstliche Intelligenz als Überwachungs-Katalysator

Die beschriebenen Fallbeispiele zeigen eindeutig, dass neben den großen Datenmengen, die durch die Digitalisierung der Arbeit anfallen, besonders die Fähigkeit entscheidend ist, mit diesen Daten effizient und effektiv umzugehen. Wenn etwa eine Druckmaschine mit den Protokollen der Abläufe und Fehler, die in ihrem regulären Betrieb entstehen, pro Tag 14.000 Aktenordner füllen könnte, wäre es theoretisch schon immer möglich gewesen, diese Daten mit dem Dienstplan abzugleichen und Rückschlüsse auf das Verhalten einzelner Mitarbeitenden zu ziehen. Doch der immense Aufwand, dies von Hand zu tun, hat einer solch detaillierten Kontrolle Einhalt geboten. Durch Software, die automatisch Auffälligkeiten in Abläufen erkennt und dabei mit allen anderen denkbaren Daten verknüpft ist, bietet es sich für Unternehmen an, ein immer lückenloseres Bild des Betriebs und damit auch des Verhaltens und der Leistungen von Beschäftigten zu erfassen. Wie oben beschrieben werden dazu teilweise selbst Gespräche transkribiert und ausgewertet. Andernorts werden Beschäftigte bis auf die Ebene von biologischen Körperfunktionen (Stühle mit Sensorik, die Transpiration misst, um besonders anspruchsvolle Arbeitsschritte zu identifizieren) und auf die Zehntelsekunde genau überwacht (Schaupp, 2021, S. 157). So werden die Mitarbeitenden immer mehr zu präzise überwachten Rädchen in der Maschinerie, deren Funktionsfähigkeit und Anteil am Betriebsergebnis permanent überprüft werden kann.

Diese Überwachung wird durch den Einsatz von algorithmischer Arbeitssteuerung sogar schon auf die Mitarbeitenden selbst ausgelagert. Algorithmische Arbeitssteuerung gibt nicht nur Weisungen, sondern führt systematisch weg von einer „klassischen Überwachung, bei der Daten aus dem Arbeitsprozess den Vorgesetzten zu Disziplinarzwecken zugeleitet werden,“ hin zu einem „feedbackbasierten Modell digitaler Kontrolle, bei dem die erhobenen Daten aufbereitet an die Beschäftigten zurückgeleitet werden, damit sie selbst den Arbeitsprozess optimieren“ (Schaupp, 2021, S. 156).

Insgesamt wird deutlich, wie Künstliche Intelligenz, in Kombination mit Kontrolle und Steuerung, zur Entwertung der Arbeit und der Menschen, die unter solchen Verhältnissen angestellt sind, beitragen kann.

RECHTLICHE RAHMEN-WERKE ZU MÖGLICHKEI-TEN UND GRENZEN VON KONTROLLE AM ARBEITS-PLATZ

Die rechtlichen Rahmenbedingungen für den Beschäftigtendatenschutz liefern drei verschiedene juristische Regelwerke: einerseits (1) die Datenschutzgrundverordnung (DSGVO), die seit Mai 2018 für die gesamte EU wirksam ist. Andererseits wird diese in Deutschland durch das ebenfalls seit Mai 2018 geltende (2) Bundesdatenschutzgesetz (BDSG) ergänzt (Wedde, 2019, S. 112). Schließlich legt (3) das Betriebsverfassungsgesetz wichtige Grundlagen für den Beschäftigtendatenschutz und ermöglicht insbesondere den Abschluss von Betriebsvereinbarungen, mit denen die Zulässigkeit und der Umfang von Kontrollmaßnahmen am Arbeitsplatz reguliert werden kann.

Anhang:
Rechtliche Rahmenbedingungen

Die Gesetzestexte, auf die sich die folgenden Seiten beziehen, sind als Anhang zum Download verfügbar: **https://t1p.de/db4um**

DSGVO

Die Datenschutzgrundverordnung (DSGVO) wurde 2016 vom Europäischen Parlament angenommen und trat 2018 in Kraft. Ziel der Verordnung ist es, die wachsenden Möglichkeiten, Daten zu sammeln und zu Wirtschaftszwecken zu nutzen, mit den Selbstbestimmungsrechten der Bürger:innen über ihre persönlichen Daten in Einklang zu bringen. Die Ziele der Transparenz (formal) und der Fairness (inhaltlich) sind grundlegende Vorgaben der DSGVO. Ihre Prinzipien umfassen grundlegende Rechte auf rechtmäßige Datenverarbeitung (Art. 6 DSGVO), auf faire Datenverarbeitung zu legitimen Zwecken (Art. 5 DSGVO), auf transparente und verständliche Informationen (Art. 12 Abs. 1 DSGVO), auf Auskunft über eigene Daten (Art. 15 DSGVO) und das „Recht auf Vergessenwerden“/ Löschung (Art. 17 DSGVO).

Damit legt die DSGVO einen verbindlichen Rechtsrahmen zugunsten der Beschäftigten fest, der auch die Digitalisierung der Arbeit maßgeblich steuert und begrenzt:

Nach Artikel 5 DSGVO muss jeder, der mit persönlichen Informationen eines anderen Menschen arbeitet, dies auf faire („Treu und Glauben“) sowie auf transparente Art und Weise tun. Er muss seine Zielsetzungen offenlegen und einhalten („Zweckbindung“) und darf den Rahmen des Verhältnismäßigen („Datenminimierung“) nicht verlassen. Und er muss als Verantwortlicher belegen können, dass er diese Grundsätze einhält, indem er seine Verwendung von Daten dokumentiert („Rechenschaftspflicht“). Dies gilt auch für Arbeitgebende, die mit den Daten der Mitarbeitenden „arbeiten“.

Artikel 12 DSGVO bestimmt: Arbeitgebende müssen es den Mitarbeitenden leicht machen, zu verstehen, was mit ihren persönlichen Daten geschieht. Sie müssen kurzfristig und kostenlos Informationen über deren Daten liefern.

Das Auskunftsrecht nach Artikel 15 DSGVO ist für Mitarbeitende zentral, denn es verschafft Klarheit darüber, welche persönlichen Informationen vom Arbeitgebenden gesammelt und genutzt werden. Hier ist umfassende Transparenz gefordert.

Artikel 17 DSGVO hält das Recht auf Löschung fest. Kann der Arbeitgebende keinen guten Grund nennen, warum er persönliche Informationen der Mitarbeitenden noch speichert, dann muss er diese Daten unverzüglich löschen.

Drohen Mitarbeitenden durch die Nutzung ihrer Daten besondere Nachteile, etwa Diskriminierung oder andere Persönlichkeitsrechtsverletzungen, so können sie dies nach Artikel

21 DSGVO per Widerspruch beim Arbeitgebenden geltend machen, der dann zu ihrem Schutz reagieren muss.

Auch im Arbeitsverhältnis hat jede:r Mitarbeitende das Recht, nicht zum bloßen Objekt von Rechenoperationen gemacht zu werden – weder darf es eine technische Totalerfassung geben (sog. Profiling), noch darf die abschließende Beurteilung durch einen Menschen – und nicht durch einen Algorithmus – verweigert werden (Art. 22 DSGVO).

Der Arbeitgebende ist nach Artikel 24 DSGVO für den fairen, transparenten und verhältnismäßigen Umgang mit den persönlichen Daten aller Mitarbeitenden verantwortlich. Diese Verantwortung kann er nicht wegdelegieren, weder auf Dienstleister, noch auf andere Beschäftigte.

Datenschutz und Datensicherheit gehören zusammen, die Arbeitgebenden müssen dem Stand der Sicherheitstechnik entsprechende Maßnahmen gegen Datenklau und Datenverlust treffen (Art. 32 DSGVO).

Besteht ein besonderes Risiko, dass Datenverarbeitungen zu Schäden für die Betroffenen (hier: die Mitarbeitenden) führen, müssen die Arbeitgebenden nach Artikel 35 DSGVO vorab das Risiko einschätzen und durch Sicherheitsmaßnahmen minimieren.

Die Arbeitgebenden müssen sich zudem von einer Fachperson für den Schutz von Daten der Mitarbeitenden beraten und kontrollieren lassen (Art. 37 DSGVO).

Damit ist der Schutz von Beschäftigtendaten durch die europäische DSGVO umfangreich vorbestimmt. Diese Regelungen verpflichten die Arbeitgebenden zu umfassenden Maßnahmen: Die Beschäftigten sind über ihre Rechte zu informieren, ihnen ist Klarheit über den Umgang mit ihren persönlichen Daten zu verschaffen und der Arbeitgebende muss für eine angemessene Datensicherheit sorgen.

Allerdings, und hier besteht Handlungsbedarf, ist die DSGVO weitgehend „technikneutral“, geht also nicht auf die besonderen Risiken digitaler Technik oder des Einsatzes künstlicher Intelligenz ein und gibt insoweit auch keine konkreten Maßnahmen zum Schutz der Beschäftigtendaten vor. Hier wäre Raum für eine nationale Regelung zum Beschäftigtendatenschutz.

Grundsätzlich ist es den europäischen Mitgliedstaaten nicht erlaubt, die DSGVO durch nationales Recht anzupassen oder zu konkretisieren. Jedoch gewährt die DSGVO gerade im Bereich des Beschäftigtendatenschutzes substanzielle Regelungsspielräume zugunsten der Gesetzgeber in den Mitgliedstaaten (vgl. Art. 88 DSGVO). Die nationalen Regulierungen dürfen allerdings den Prinzipien des Datenschutzes (vgl. oben Art. 5 DSGVO) nicht widersprechen.

Der deutsche Gesetzgeber hat von dieser Ermächtigung der DSGVO mit eigenen Regelungen zum Beschäftigtendatenschutz Gebrauch gemacht:

BDSG

In Deutschland wird die Umsetzung und Ergänzung des DSGVO durch das Bundesdatenschutzgesetz BDSG geregelt. Dort ist unter anderem festgehalten, in welchen Fällen die Sammlung und Verarbeitung von Daten von Beschäftigten legitim ist. Für öffentliche Stellen der Länder können noch einmal eigene Regelungen vorliegen.

Mit Blick auf Kontrolle und Überwachung am Arbeitsplatz ist der Paragraf 26 des BDSG ausschlaggebend. Paragraf 26 BDSG regelt zunächst einmal recht unspektakulär, dass jede Datenverarbeitung im Beschäftigungsverhältnis verhältnismäßig sein muss (vgl. oben Art. 5 DSGVO). Hier macht der deutsche Gesetzgeber eigentlich nur klar, dass er von der Erlaubnis des Artikels 88 DSGVO, den Beschäftigtendatenschutz national zu regeln, Gebrauch machen will – und dass Regelungen auch durch sogenannte Kollektivverträge, also Tarifverträge (für Branchen) und Betriebsvereinbarungen (auf der Ebene einzelner Unternehmen) getroffen werden können.

Interessanter ist der zweite Satz des Absatz 1, wonach der Arbeitgebende dann seine Beschäftigten überwachen darf, wenn er konkrete Anhaltspunkte dafür hat, dass ein Mitarbeitender eine Straftat zu seinen Lasten begeht (also etwa einen Diebstahl oder eine Untreue begeht oder bestechlich ist).

Umgekehrt bedeutet das aber: Der Arbeitgebende darf nicht „ins Blaue hinein“ seine Beschäftigten ausspionieren oder Informationssammlungen „auf Vorrat“ anlegen. Beides wäre rechtswidrig.

BetrVG

Für die Einhaltung der DSGVO und des BDSG sind Betriebsräte oder andere Institutionen der betrieblichen Mitbestimmung, wichtige Kontrollorgane (analog dazu der Personalrat bei öffentlichen Arbeitgebenden nach Maßgabe des Personalvertretungsrechts in Bund und Ländern). Denn „der Arbeitgebende möchte Daten erheben, verarbeiten und nutzen, um Unternehmenszwecken zu dienen. Ein Ziel ist dabei der Schutz des Unternehmereigentums, z.B. vor Diebstahl oder anderen Straftaten“ (Wedde, 2019, S. 114). Das heißt, dass die Datenverarbeitung zunächst im wirtschaftlichen Interesse von Unternehmen liegt, sich in Grenzfällen jedoch nicht mit den Rechten der Arbeitnehmenden deckt. Hier ist die betriebliche Interessenvertretung eine kontrollierende und ggf. einschreitende Instanz, die den Überwachungsdruck auf die Beschäftigten erheblich mindern kann.

Mit dem Betriebsverfassungsgesetz (BetrVG) erfolgt eine Institutionalisierung der Mitbestimmung von Arbeitnehmenden hinsichtlich der Ausgestaltung ihrer Arbeitsplätze. Hier geht es vor allem um die Möglichkeiten, in betriebliche Prozesse einzugreifen und sie mitzugestalten, wenn die Rechtspositionen von Mitarbeitenden beeinträchtigt werden. Das bezieht die Sammlung und Verarbeitung von Daten der Beschäftigten durch den Arbeitgebenden mit ein. Hier bestimmt das Betriebsverfassungsgesetz den Umfang der Mitbestimmung durch die Arbeitnehmenden im Falle von Kontrollmaßnahmen des Arbeitgebenden, einschlägig ist der Paragraf 87, Absatz 1, Nr. 6.

Umgekehrt gibt es bislang keine allgemeine Mitbestimmung des Betriebsrats bei Fragen des Datenschutzes – dass der Arbeitgebende Daten von Beschäftigten erhebt oder nutzt, löst also für sich genommen noch keine Beteiligung des Betriebsrats aus. Ob dies im Falle des Einsatzes von Künstlicher Intelligenz am Arbeitsplatz künftig anders werden soll, wird im Bundestag kontrovers diskutiert.

Eine Möglichkeit des Betriebsrats, seine Mitbestimmungsrechte auszuüben, besteht im Abschluss von Betriebsvereinbarungen (vgl. § 77 BetrVG): Solche kollektiv verbindlichen Vereinbarungen mit dem Arbeitgebenden haben den Vorteil, dass Rechtssicherheit für eine Vielzahl von Fallgestaltungen verbindlich geschaffen werden kann – Artikel 88, Absatz 1 DSGVO (vgl. oben) gestattet dies ausdrücklich. Der Abschluss einer Betriebsvereinbarung zu Datenschutzthemen erfolgt also im Geben und Nehmen: Der Arbeitgebende bekommt so eine Grundlage für Verarbeitung der Daten der Arbeitnehmenden, der Betriebsrat erwirkt dafür Einschränkungen beim Umfang der Datenverarbeitungen und ein eigenes Kontroll- und Beteiligungsrecht.

Mit Blick auf die gesetzlichen Bestimmungen zur digitalen Kontrolle am Arbeitsplatz lässt sich daher festhalten: Es gibt mit der DSGVO und dem BDSG zwar eine Reihe von Vorschriften, die Kontrollmöglichkeiten der Arbeitgebenden am Arbeitsplatz betreffen und allgemeine Prinzipien hierfür bereitstellen. Zudem kann in Deutschland im Wege der Kollektivvereinbarung (Tarifvertrag/Betriebsvereinbarung) über Ausmaß und Grenzen der Kontrolltätigkeit der Arbeitgebenden mitbestimmt werden. Spezifische Vorschriften über digitale Kontroll- und Überwachungstechniken sucht man derzeit allerdings vergeblich – weswegen über die Regulierung mittels eines Beschäftigten-Datenschutzgesetzes intensiv gestritten wird. Bevor zum Abschluss die aus der Sicht des RDÖ wesentlichen Elemente für eine umfassende Regulation von Kontrolle am vernetzten Arbeitsplatz benannt werden, formuliert das nächste Kapitel Anforderungen an Unternehmen, die über die gesetzlichen Vorschriften hinausgehen.

ROLLE VON UNTERNEHMEN

Anforderungen an Arbeitgebende

Unternehmen sind als die Instanz, die Kontrolle ausübt, in einer besonderen Verantwortung. Ein professioneller Umgang mit Daten geht über ein gesetzeskonformes Verhalten hinaus und zeitgemäße Kontrolle am Arbeitsplatz kann neben Mitbestimmung und Transparenz auch ein vertrauensbasiertes und ergebnisorientiertes Verständnis von Arbeit umfassen. Folgende Punkte sind aus Sicht des RDÖ besonders wichtig:

Professionellen Umgang mit Überwachungsfragen entwickeln
Unternehmen mit einer gewissen Sensibilität für das Thema Datenschutz sehen von „zu neugierigen“ Funktionen ab. Unternehmen sollen nicht Daten um der Daten willen sammeln, sondern sich auf die Informationen beschränken, die für ihre Zwecke erforderlich sind. Letztendlich ist das eine Frage der Professionalität, und in der Tendenz ist das Bewusstsein in größeren Unternehmen stärker ausgeprägt, da mehr Know-how zu den unterschiedlichen Bereichen vorhanden ist und es eher eine organisierte Arbeitnehmerschaft gibt, die sich des Themas annimmt und eine Auseinandersetzung mit Datenschutzfragen forciert. Wird dieser Prozess ernsthaft geführt, fördert das auch die Akzeptanz neuer Techniken bei der Belegschaft.

Transparenz und offene Kommunikation
Ein Aspekt des professionellen Umgangs mit Systemen, die technisch zur Überwachung geeignet sind, ist Transparenz und eine offene Kommunikation über die Möglichkeiten der Systeme einerseits und die Bedenken der Belegschaft andererseits. Wenn die Mitarbeitenden erkennen, dass der Arbeitgebende sich ernsthaft mit den Risiken von Software auseinandersetzt, zuvorkommend den Austausch sucht, und sich an gesetzliche Vorgaben und allfällige Betriebsvereinbarungen hält, kann das zu einem vertrauensvollen Arbeitsverhältnis beitragen – und auch Widerstände gegen legitime Informationsverarbeitung abbauen.

Mindset: Sich ernsthaft der Kulturfrage stellen
Die betriebliche Kultur, die auch die Kommunikation umfasst, hat großen Einfluss auf die Frage nach Ausmaß und Gestaltung von Kontrolle am Arbeitsplatz. Der Grad von Autonomie und Selbstbestimmung etwa steht in einem direkten Zusammenhang mit dem Bedürfnis nach Kontrolle. Je weniger ein Arbeitnehmender in die Gestaltung, Planung und Evaluation der Arbeit involviert ist, desto größer ist tendenziell das Interesse des Arbeitgebenden, zu überprüfen, ob Arbeit und Arbeitsqualität den eigenen Vorstellungen entspricht. Anders gesagt: Je strikter Arbeitsschritte vorgegeben sind, je mehr in Präsenzkategorien gedacht wird, desto naheliegender ist eine engmaschige Überwachung. Daraus ergibt sich die Frage, an welchen Stellen Kontrolle durch Vertrauen und wo die Überwachung des Arbeitsprozesses durch Freiräume mit einem Fokus auf die Qualität des Endergebnisses und Zufriedenheit im Betrieb ersetzt werden kann.

Klarheit schaffen, Alternativen nutzen
Ein großer Teil der in Betrieben verwendeten technischen Anwendungen und IT-Systeme stammen nicht aus diesen Betrieben selbst, sondern wird von Drittanbietern als Programme oder Services eingekauft. Dadurch können nicht nur betriebliche Abläufe effizienter gestaltet werden, sondern zugleich werden auch neue Überwachungskapazitäten in das Arbeitsverhältnis integriert. Damit stellen sich neue Fragen: Wer erhebt die Beschäftigtendaten, wer verarbeitet und speichert sie? Überwacht der Arbeitgebende oder der Drittanbieter?

Es ist zunächst einmal eine vertragliche Herausforderung für Arbeitgebende, rechtssicher abzubilden, was der Dienstleister mit Beschäftigtendaten tun soll und was nicht. Es kann zudem auch eine Herausforderung darstellen, den Mitarbeitenden klar und präzise zu vermitteln, zu welchen Zwecken der Drittanbieter eingesetzt wird und wie er vom Arbeitgebenden „unter Kontrolle gebracht“ wird. Denn häufig besitzen die Dienstleister einen erheblichen technologischen Wissensvorsprung vor dem Arbeitgebenden und sind nicht selten auch wirtschaftlich mächtiger als ihr Auftraggeber. Dies beruht auch auf monopolartigen Angebotssituationen, und es ist für Arbeitgebende nicht immer einfach, alternative Angebote, etwa open-source-basierte Software, zu berücksichtigen, die nicht auf das Sammeln von Daten ausgerichtet ist. Rechtlich stellt sich hier die besondere Herausforderung, dass die DSGVO zwar das Verhalten von Arbeitgebenden (als Verantwortliche) und von Auftragsverarbeitern (also Dienstleistern) regelt, nicht aber die Entwickler und Anbieter von Überwachungssoftware oder -produkten mit in den Blick nimmt. Viele Arbeitgebende verlassen sich aber darauf (oder sehen keine eigene Prüfmöglichkeit), dass diese Anbieter nur rechtskonforme Leistungen erbringen – was gerade bei außereuropäischen Firmen aber keinesfalls garantiert ist. Daher müssen auch Drittanbieter in die Pflicht genommen werden.

Anforderungen an Microsoft & Co.: Privacy by Design

Die meisten Unternehmen nutzen unter anderem IT-Systeme und Anwendungen von Großkonzernen wie Microsoft, Google, Amazon oder OpenAI, und in der Regel handelt es sich dabei um «one-size-fits-all»-Lösungen. Häufig werden bei der Nutzung von solchen Systemen Daten von Beschäftigten erfasst und Kontrollmöglichkeiten eröffnet, die für eine Großzahl der Unternehmenskund:innen gar nicht erstrebt werden oder unerheblich sind. Die meisten Arbeitgebenden haben beispielsweise kein grundsätzliches Interesse an der Information, wann die Mitarbeitenden zuletzt bei Microsoft Teams online gewesen sind.

Für die Software-Anbieter kann es umgekehrt effizienter sein, eine einzige, maximalistische Version ihres Produkts zu veröffentlichen, mit der die Kund:innen dann ihre eigenen Nutzungsziele realisieren können – und viele Möglichkeiten des Produkts ungenutzt lassen. Andererseits haben die Software-Anbieter ein Interesse daran, mit ihren Systemen auch Daten einzusammeln, um die eigenen Produkte zu verbessern oder um etwa Künstliche Intelligenzen zu trainieren. Eine individuell auf den konkreten Kunden zugeschnittene, datensparsame Version ist in der Regel daher nicht verfügbar oder wäre sehr teuer.

Halten in dieser Konstellation zur Kontrolle geeignete Funktionen in den Betrieben Einzug, sei es als ungenutztes Feature, als Rückfallprodukt (Default) oder sogar als nicht abschaltbare Funktion, wird dadurch ein erheblicher Überwachungsdruck auf Beschäftigte aufgebaut.

Deshalb ist es ratsam, die „Datensammelwut“ bereits bei der Konstruktion der Software auf Herstellerseite zu begrenzen und den Kunden die systemseitige Möglichkeit zu bieten, Überwachungstools vollständig nach den eigenen Nutzungsvorstellungen zu konfigurieren. Indem Privacy by Design für Unternehmenssoftware gesetzlich verbindlich auch für Entwickler und Anbieter gemacht wird, würde Datenschutzkonformität für die Software-Anbieter zwar voraussetzungsvoller, aber für die breite Masse der Anwender:innen würde der Nutzungsaufwand abnehmen und für die Arbeitnehmenden würde der Überwachungsdruck am Arbeitsplatz enorm abnehmen. Dieser Ansatz wird von Arbeitgebenden wie von Arbeitnehmenden begrüßt und hat auch nach Auffassung des RDÖ hohe Priorität.

FAZIT UND HANDLUNGS-EMPFEHLUNGEN DES RATES FÜR DIGITALE ÖKOLOGIE

Die digitale Transformation der Arbeitswelt ist in vollem Gange, was natürlich auch Auswirkungen auf die Arbeitnehmerseite hat, etwa was die Kontrollverhältnisse am vernetzten Arbeitsplatz angeht, die sich mit fortschreitender Digitalisierung erheblich verändern.

- An die Stelle persönlicher, stichprobenartiger, offener und erfahrungsbasierter Kontrolle tritt eine **automatisierte, allumfassende, heimliche und algorithmenbasierte Kontrolle.**

Durch eine ungehemmte Digitalisierung würde der Überwachungsdruck am Arbeitsplatz weiter massiv verstärkt. Auf längere Sicht droht dadurch ein Wertewandel hin zu mehr Kontrolle am Arbeitsplatz; die über Jahrzehnte gewachsene Arbeitskultur in Deutschland verändert sich damit grundlegend: Wegen digitaler Überwachung droht eine neue Dimension der **Entfremdung von Arbeitnehmenden und Arbeitgebenden.**

Die Digitalisierung der Arbeitsverhältnisse ist aber nicht nur eine gegebene Tatsache, sie ist immer auch **Gestaltungsaufgabe**: Führt der Einsatz digitaler Mittel am Arbeitsplatz zu Arbeitsverhältnissen, die fair, gesund, nachhaltig oder auch nur akzeptabel sind? Hier gilt es, wertorientierte Vorstellungen von „guter digitaler Arbeit“ zu entwickeln, welche die technischen Möglichkeiten als das einordnet, was sie sein sollten:

- Technische Möglichkeiten sind Angebote zur Umgestaltung der Arbeitswelt, die man annehmen kann, wenn sie mit unseren Wertvorstellungen harmonieren. Und ablehnen muss, wenn sie das nicht tun.

Hier sind insbesondere die Arbeitgebenden gefordert: Allein die technische Möglichkeit einer umfassenderen Kontrolle von Arbeitnehmenden ist niemals ein hinreichender Grund, diese Technik auch einzusetzen.

Weiterhin ist wichtig:

- Die Arbeitgebenden dürfen zu Kontrollzwecken nur solche **Dienstleister** einsetzen, die vertrauenswürdig sind, sich an die gesetzlichen und vertraglichen Vorgaben halten und nicht „auf eigene Faust“ und zu eigenen Zwecken agieren.
- Zudem darf der Arbeitgebende nur solche Kontrolltechniken einsetzen, die er selbst auch **verstehen, erklären und verantworten** kann.
- Der Arbeitgebende trägt die **Verantwortung für den Technikeinsatz** am Arbeitsplatz.
- Er muss die **Sicherheit der Datenverarbeitung** durch seine Kontrolltechniken garantieren, riskante Techniken darf er nur nach vorheriger Prüfung und **Bewertung der Technikfolgen** einsetzen. Zur Datensicherheit zählt insbesondere der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung von Daten durch geeignete technische und organisatorische Maßnahmen.
- Setzt der Arbeitgebende **riskante Überwachungstechniken** ein, muss er sich **fachkundig beraten** lassen (intern oder extern von einem Datenschutzbeauftragten).
- Er darf sich wesentliche Entscheidungen im Arbeitsverhältnis **nicht von Technik abnehmen lassen; automatisierte Entscheidungen** ohne menschliche Kontrollinstanz darf es nicht geben.
- Er darf weder anordnen noch zulassen, dass Mitarbeitende **eigene** Techniken oder Anwendungen **persönlich** am Arbeitsplatz einbringen, die wiederum das Verhalten der Mitarbeitenden kontrollieren und dokumentieren.

Der Einsatz von „Black Box-Verfahren“ oder „Voodoo-Technik“, die der Arbeitgebende selbst weder versteht noch beherrscht, ist nicht zu rechtfertigen.

Auf dieser Basis können **rechtliche Vorgaben** und Regularien formuliert werden, um den digitalen Arbeitsraum, der immer auch ein Kontrollraum ist, zu gestalten, um **Rechtssicherheit für Arbeitgebende und hinreichenden Schutz für Arbeitnehmende** zu schaffen. Zu diesem Schutz zählen auch **Schulungsmaßnahmen** des Arbeitgebenden, durch die er alle Arbeitnehmenden zum sicheren und verantwortungsbewussten Umgang mit Kontrolltechniken befähigt und insbesondere Führungskräfte hinsichtlich der Gefahren überbordender Kontrolle **sensibilisiert**.

Regulierung

Bei einem ungebremsten und unregulierten Fortschreiten der Digitalisierung von Arbeit würde der sich öffnende „Graubereich digitaler Überwachung am Arbeitsplatz“ allein nach den **Interessen der sozial mächtigeren Gruppen**, also der Arbeitgebenden und der Digitalindustrie, besetzt. Dies kann nicht richtig sein und widerspricht der gerade in Deutschland ausgeprägten Mitverantwortung von Arbeitgebenden **und** Arbeitnehmenden für gerechte und sozialverträgliche Arbeitsbedingungen. Die **Regulierung** von digitalen Mitteln der Kontrolle am Arbeitsplatz ist daher **sinnvoll und notwendig**, sowohl mittels rechtlicher Vorgaben als auch anhand außerrechtlicher Maßstäbe einer Daten-Ethik.

- In diesen **Regulierungsprozess** müssen jedenfalls die folgenden Vertreter:innen einbezogen werden:
- Vertreter:innen der Interessen von Arbeitnehmenden (Gewerkschaften, Betriebsräte)
- Vertreter:innen der Interessen von Arbeitgebenden
- Vertreter:innen der Wissenschaft (Arbeitssoziologie, Informatik, Arbeitsrecht, Ethik)
- Vertreter:innen von Aufsichtsbehörden mit Vollzugserfahrung

Ansätze für eine rechtliche Regulierung digitaler Überwachung am Arbeitsplatz existieren bereits, insbesondere gibt die Europäische Datenschutz-Grundverordnung (DSGVO) verbindliche Regeln vor.

- Die **DSGVO** legt mit den zwar allgemeinen, aber verbindlichen Vorgaben der **Transparenz**, der **Fairness** und der **Verhältnismäßigkeit** klare Orientierungspunkte einer notwendigen differenzierten Regulierung fest.

Daneben bleiben die gesetzlichen Vorgaben des deutschen Bundesdatenschutzgesetzes (vgl. § 26 BDSG) blass und rudimentär.

- Der RDÖ empfiehlt daher, die Regelungen des **Bundesdatenschutzgesetzes** in Bezug auf digitale Überwachungsmaßnahmen **zu ergänzen und zu konkretisieren.**

Positiv ist mit Blick auf das BDSG festzuhalten, dass es von der Möglichkeit der DSGVO Gebrauch macht (Art. 88 DSGVO i.V.m. § 26 Abs. 4 BDSG), auf Betriebsebene per Betriebsvereinbarung eine differenzierte und passgenaue Regulierung des Einsatzes digitaler Kontrollinstrumente am Arbeitsplatz zu erzielen. Damit ergibt sich insbesondere für

die Arbeitnehmenden eine Chance, den digitalen Fortschritt am Arbeitsplatz nicht nur zu „erdulden“, sondern mitzugestalten. Dies schafft zugleich Rechtssicherheit für alle Betriebsparteien.

- Die vorhandenen Möglichkeiten, auf Betriebsebene eine Regulierung der Digitalisierung durch eine **Betriebsvereinbarung** zwischen Arbeitgeber- und Arbeitnehmervertretungen auszuhandeln, sollten intensiv genutzt werden.

Darüber hinaus spricht viel für eine **Stärkung der Mitbestimmungsrechte des Betriebsrats** bei der Einführung und Anwendung von Überwachungstechnologien im Betrieb.

Ein **umfassendes Beschäftigtendatenschutzgesetz** sollte darauf abzielen, die Freiheitsrechte und den Datenschutz von Mitarbeiter:innen im digitalen Zeitalter zu schützen.

Hier sind einige **wesentliche Elemente**, die ein solches Gesetz nach Auffassung des RDÖ umfassen sollte:

Transparenz und Informiertheit

- Arbeitgebende müssen ihre Mitarbeitenden vollständig und verständlich darüber informieren, welche Daten von ihnen zu Kontrollzwecken gesammelt werden, zu welchem Zweck dies erfolgt und wie diese Daten verwendet werden.
- Die erhobenen Daten dürfen nur für den festgelegten Zweck verwendet und nicht zweckentfremdet werden. Allein ein Fortschritt bei den anwendbaren Technologien rechtfertigt keine Zweckänderung auf Seiten der Arbeitgebenden.
- Es sollte dabei klar **kommuniziert** werden, welche **Überwachungstechnologien** konkret eingesetzt werden und in welchem Umfang die Überwachung stattfindet.

Die Transparenz jeder Kontrolle muss gewährleistet sein:

- Kontrollen am Arbeitsplatz müssen **angekündigt, begründet, dokumentiert, nachprüfbar** sein, **zeitnah ausgewertet und regelmäßig evaluiert** werden,
- Der Einsatz **unbeherrschter Dienstleister** oder **unbeherrschter Techniken** durch den Arbeitgebenden scheidet aus, denn dies würde sich voll zu Lasten der Mitarbeitenden auswirken.
- Ziel und Umfang der Kontrolle bestimmt und verantwortet der Arbeitgebende, nicht der Dienstleister. Ein nicht vom Arbeitgebenden, sondern vom Dienstleister angetriebener „technischer Überwachungsüberschuss“ muss ausgeschlossen werden.

Die Mitarbeitenden habe ein Recht auf Transparenz:

- Mitarbeitende haben das Recht, **Zugang** zu ihren eigenen Daten zu erhalten, unrichtige Daten zu **korrigieren** und unzulässig erhobene oder gespeicherte Daten **löschen** zu lassen.

Verhältnismäßigkeit und Fairness jeder Kontrolle

- Es gilt der **Grundsatz der Datenminimierung:** Es dürfen nur die Daten erhoben werden, die wirklich notwendig sind, um den festgelegten Zweck zu erreichen. Damit wird die Überwachung am Arbeitsplatz auf das Notwendige reduziert.
- **Keine Totalüberwachung** am Arbeitsplatz, die sämtliche Leistungen des Arbeitnehmenden erfasst und vollumfänglich mitprotokolliert.
- **Keine pauschale Überwachung** aller Arbeitnehmenden in sämtlichen Arbeitsbereichen; Kontrollmaßnahmen müssen **personell und zeitlich begrenzt sowie differenziert** sein.
- **Keine unangemessene Überwachung**
- Gemessen am **Ziel** der Überwachung: Arbeitgebende dürfen nur mit Blick auf erhebliche eigene Interessen kontrollieren, nicht wegen Kleinigkeiten oder Formalien. Es gilt der **Grundsatz der Verhältnismäßigkeit.**
- Gemessen am **Gegenstand** der Überwachung: Kontrollen während der Mittagspause oder im Bereich der **Privatsphäre**, etwa von Pausenräumen oder Toiletten, sind tabu. Das gilt besonders für die Nutzung **sensibler Daten** (Gesundheitsdaten/biometrische Daten/ethnische Herkunft) zu Kontrollzwecken.
- Gemessen am **Ergebnis** der Überwachung: Kontrollmaßnahmen dürfen nicht dazu führen, dass Mitarbeitende völlig durchleuchtet und kategorisiert werden (**Verbot von Profiling**).
- Keine ungleiche oder unfaire Überwachung durch diskriminierende Auswahl der kontrollierten Arbeitnehmenden oder überraschende, widersprüchliche oder entwürdigende Kontrollmaßnahmen.

Die Mitarbeitenden habe ein Recht auf Fairness jeder Kontrolle:

- Sollten Mitarbeitende von allgemeinen Kontrollmaßnahmen in besonderer Weise belastet werden, muss ihnen die Möglichkeit individuellen Widerspruchs beim Arbeitgebenden oder individueller Beschwerde bei der Datenschutz-Aufsichtsbehörde gegeben sein.

Diese Eckpunkte müssen vom Gesetzgeber wirksam vorgegeben werden, Verstöße dürfen nicht bagatellisiert werden und nicht folgenlos bleiben. Neben den gesetzlich bereits vorgesehenen **Sanktionen** (nach DSGVO drohen Bußgelder und Untersagungen) muss gesetzlich klargestellt werden, dass Verstöße nicht hingenommen und **Vorteile** aus ihnen **nicht gezogen** werden dürfen.

Dies spricht aus Sicht des RDÖ klar für ein

- **Verwertungsverbot für Daten**, die entgegen diesen Prinzipien erhoben oder genutzt werden

Ein umfassendes, Verhältnismäßigkeit und Fairness der digitalen Überwachung am Arbeitsplatz garantierendes Gesetz zum Beschäftigtendatenschutz würde sicherstellen, dass die Rechte und Freiheiten der Mitarbeitenden gewahrt bleiben, während gleichzeitig die berechtigten Interessen der Arbeitgebenden geschützt werden. Es würde einen klaren rechtlichen Rahmen schaffen, der die berechtigten Interessen der Betriebsparteien schützt und Vertrauen sowie Transparenz fördert.

Mit diesen Maßgaben kann der **wertebasierte Einsatz von digitaler Technik am Arbeitsplatz** gelingen: In einem auf gegenseitigem Vertrauen basierenden Arbeitsverhältnis steht die Achtung vor den Arbeitnehmenden als individuellen Persönlichkeiten mit eigenen Rechten und dem Anspruch auf Schutz vor Ausspähung und Diskriminierung im Mittelpunkt.

LITERATUR

Atlas der digitalen Arbeit: Daten und Fakten über die Beschäftigung der Zukunft. (2022). Deutscher Gewerkschaftsbund (DGB) und Hans-Böckler-Stiftung (HBS) https://www.dgb.de/politik/wirtschaft-und-transformation/digitale-transformation-der-arbeitswelt/atlas-der-digitalen-arbeit/

Balkhausen, D. (1980). Mikroelektronik – Die dritte industrielle Revolution. bpb.de, 1980(7). https://www.bpb.de/shop/zeitschriften/apuz/archiv/531496/mikroelektronik-die-dritte-industrielle-revolution/

Bitkom e.V. (2022). New Work: Die Hälfte der Deutschen arbeitet im Homeoffice. https://www.bitkom.org/Presse/Presseinformation/New-Work-Haelfte-arbeitet-im-Homeoffice

BDSG (2024). https://www.gesetze-im-internet.de/bdsg_2018/

BetrVG (2022). https://www.gesetze-im-internet.de/betrvg/

Bundesarbeitsgericht. (2017). Urteil des 2. Senats vom 27. Juli 2017, Az. 2 AZR 681/16. http://www.rechtsprechung-im-internet.de/jportal/?quelle=jlink&docid=KARE600053503&psml=bsjrsprod.psml

Bundesverfassungsgericht. (1983). Urteil des Ersten Senats vom 15. Dezember 1983, Az. 1 BvR 209/83, Rn. 1-215. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html

Christl, W. (2021). Digitale Überwachung und Kontrolle am Arbeitsplatz: Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management? Cracked Labs. https://crackedlabs.org/dl/CrackedLabs_Christl_UeberwachungKontrolleArbeitsplatz.pdf

Czichi-Welzer, N. & Welzer, H. (2021). Die Digitale Transformation der Arbeit: Eine Studie zu den Auswirkungen der Digitalen Transformation auf Beschäftigte. Rat für Digitale Ökologie. https://ratfuerdigitaleoekologie.org/images/downloads/RDOE-paper03-digitale_transformation.pdf

Dietrich, A., Bosse, C. K. & Schmitt, H. (2021). Kontrolle und Überwachung von Beschäftigten. Datenschutz und Datensicherheit - DuD, 45(1), 5–10. https://doi.org/10.1007/s11623-020-1381-2

DSGVO (2021). https://dsgvo-gesetz.de/

Enquete-Kommission Künstliche Intelligenz. (2020). Bericht der Enquete-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale (Drucksache 19/23700). Deutscher Bundestag.

Freytag, B. (2022). SAP wird 50: Bill Gates bezeichnete deutschen IT-Konzern als Unfall. FAZ.NET. https://www.faz.net/aktuell/finanzen/sap-wird-50-bill-gates-bezeichnete-deutschen-it-konzern-als-unfall-17927193.html

Kartheuser, I. & Pabst, E. (2023). Wo liegen die Grenzen der Arbeitnehmerüberwachung? Legal Tribune Online. https://www.lto.de/recht/kanzleien-unternehmen/k/arbeitsrecht-mitarbeitende-ueberwachung-leistungskontrolle-10a619920-urteil-vg-hannover-amazon/

Kaschadt, K. (2001). Von der Macht des Blicks. In T. Y. Levin, Ursula Frohne & Peter Weibel (Hrsg.), CTRL [SPACE]. Rhetorics of Surveillance from Bentham to Big Brother. https://web.archive.org/web/20020219175402/http://hosting.zkm.de/ctrlspace/d/texts/06

Lang, R. (2021). Microsoft 365: So überwachen Chefs eure Produktivität am Arbeitsplatz. netzpolitik.org. https://netzpolitik.org/2021/microsoft-365-so-ueberwachen-chefs-eure-produktivitaet-am-arbeitsplatz/

Pack, C., McAtee, C., Lobo, A., Edwards, E., & msbemba. (2024). Microsoft Einführungsbewertung. Microsoft 365. https://learn.microsoft.com/de-de/microsoft-365/admin/adoption/adoption-score?view=o365-worldwide

SAP Business One. (o. J.). SAP. Abgerufen 13. Juni 2024, von https://www.sap.com/germany/products/erp/business-one.html

Schaupp, S. (2021). Technopolitik von unten: Algorithmische Arbeitssteuerung und kybernetische Proletarisierung (Erste Auflage). Matthes & Seitz Berlin.

Sokolov, D. A. (2020). Microsoft verspricht weniger Überwachung Einzelner in Microsoft 365. heise online. https://www.heise.de/news/Microsoft-verspricht-weniger-Ueberwachung-Einzelner-in-Microsoft-365-4977233.html

Verwaltungsgericht Hannover. (2023). Urteil vom 9. Februar 2023, Az. 10 A 6199/20. https://openjur.de/u/2463624.html

Voigt, H. C. (2021). Digitale Überwachung und Kontrolle in österreichischen Betrieben: Bericht über eine explorative Untersuchung mit Fallbeispielen auf Basis von Interviews. Cracked Labs. https://crackedlabs.org/dl/CrackedLabs_Voigt_UeberwachungArbeitsplatzAT.pdf

Wedde, P. (2019). Gläsernen Belegschaften Grenzen setzen – Datenschutz im Betrieb. Soziales Recht, 9(3), 175–187.

Wolfangel, E. (2021). Überwachung am Arbeitsplatz: Der Chef sieht alles. Zeit. https://www.zeit.de/2021/38/ueberwachung-arbeitsplatz-software-arbeitnehmerrechte-datenschutz

Zuboff, S. (2018). Das Zeitalter des Überwachungskapitalismus. Campus Verlag.

DANKSAGUNG

Wir möchten an dieser Stelle all denen danken, mit denen wir im Rahmen der Erstellung dieses Positionspapiers Gespräche geführt und uns ausgetauscht haben. Ihre Vorschläge, aber auch ihre kritischen Hinweise waren für uns sehr wichtig. Die Schlussfolgerungen, die wir aus den Gesprächen gezogen haben, müssen natürlich nicht notwendigerweise mit denen unserer Gesprächspartner:innen übereinstimmen. Wir freuen uns darauf, den konstruktiven Austausch weiterführen zu können.

Wir danken besonders herzlich:

Jasmin Arbabian-Vogel (Präsidentin a.D. des Verbands deutscher Unternehmerinnen e.V. und Unternehmerin), **Susanne Dehmel** (Mitglied der Geschäftsführung beim Bitkom e.V.), **Oliver Kohl** (Unternehmensjurist bei der ENTEGA AG), **Bijan Moini** (Legal Director bei der Gesellschaft für Freiheitsrechte e.V.), **Christoph Tillmanns** (Vorsitzender Richter am Landesarbeitsgericht Baden-Württemberg), **Prof. Dr. Hans-Jürgen Urban** (Geschäftsführendes Vorstandsmitglied der IG Metall) und **Roland Wolf** (Abteilungsleiter der Abteilung Arbeitsrecht und Tarifpolitik der Bundesvereinigung der Deutschen Arbeitgeberverbände).

IMPRESSUM

Herausgeber

Rat für Digitale Ökologie

Autor:innen
Dr. Stefan Brink, Maxim Keller, M.A. und Ann-Marie Verhoeven, M.A.

Redaktion
Prof. Dr. Harald Welzer
Dipl-Soz. Dana Giesecke, M.Sc.

Studentische Mitarbeit
Martin Döscher

Kontakt
info@rdoe.org

Veröffentlicht im **August 2024**

Der RDÖ ist ein Projekt von **FUTURZWEI. Stiftung Zukunftsfähigkeit**
Gefördert von der **Allianz Foundation** und der **Schöpflin-Stiftung.**

Lehrter Str. 57 Haus 6 | 10557 Berlin | +49 (0)30 397 177 09 | info@rdoe.org | rdoe.org

ÜBER DIE AUTOR:INNEN

Dr. Stefan Brink

Stefan Brink leitet das Wissenschaftliche Institut für die Digitalisierung der Arbeitswelt (wida/Berlin), das den digitalen Wandel mit Blick auf unsere Bürgerrechte begleitet und Digital-Projekte fördert. Bis Ende 2022 war er fünf Jahre lang der Beauftragte für Datenschutz und Informationsfreiheit des Landes Baden-Württemberg, zuvor vier Jahre stellvertretender Datenschutzbeauftragter in Rheinland-Pfalz. Außerdem arbeitete er als wissenschaftlicher Mitarbeiter beim Bundesverfassungsgericht und war Richter am Verwaltungsgericht Koblenz. Brink ist Mitglied der Gesellschaft für Freiheitsrechte (GFF) und zählt durch sein Engagement und seine vielfältigen Publikationen zu den bekanntesten Datenschützern Deutschlands.

Maxim Keller, M. A.

Maxim Keller ist wissenschaftlicher Mitarbeiter beim Rat für Digitale Ökologie und PhD-Student an der Universität St. Gallen im Fachbereich Geschichte. In seiner Dissertation zu »Contentious Techno Politics« erforscht er, wie zivilgesellschaftliche Akteure die Entwicklung und den Einsatz von Informationstechnik beeinflussen, indem sie Kritik äußern, Widerstand leisten, oder eigene Alternativen zu kommerziellen Internetdienstleistungen aufbauen. Davor hat er in St. Gallen einen Master in Business Innovation absolviert.

Anni Verhoeven, M. A.

Ann-Marie Verhoeven unterstützt als Wissenschaftliche Mitarbeiterin die Forschung des Rates für Digitale Ökologie. Ihr Forschungsinteresse liegt in den Bereichen Social Media und Sucht, Desinformation und Polarisierung, sowie in der zivilgesellschaftlichen Suche nach einer gemeinwohlorientierten Digitalpolitik. Zuvor hat sie Politikwissenschaft und Soziologie in Würzburg, Kolumbien und Potsdam studiert.

ÜBER DEN RAT

Der RDÖ setzt sich für eine gemeinwohlorientierte und nachhaltige Digitalpolitik ein. Um diese Zukunftsvision zu realisieren, informiert er mithilfe von Veranstaltungen und wissenschaftlichen Studien, gibt Empfehlungen an die Politik und vernetzt die digitale Zivilgesellschaft.

Ausgangspunkt für die Gründung des Rates war die Erkenntnis, dass in der politischen Debatte oft nur Einzelaspekte der digitalen Transformation betrachtet werden, obwohl diese längst sämtliche Lebensbereiche durchdringt. Für den Rat ist die entscheidende Frage, wie es gelingt, die Digitalisierung nachhaltig und nach demokratischen Werten und Normen zu gestalten.

Zum Rat Gehören:

Unternehmerin	**Jasmine Arbabian-Vogel**
Leiter des Wissenschaftlichen Institut für die Digitalisierung der Arbeitswelt	**Dr. Stefan Brink**
Stadtplanungsexpertin	**Prof. Dr. Vanessa Miriam Carlow**
Journalist	**Florian Gless**
Transformationsforscherin	**Prof. Dr. Maja Göpel**
Menschenrechtsanwalt	**Dr. Wolfgang Kaleck**
Unternehmerin	**Diana Kinnert**
Designerin für Mensch-Computer-Schnittstellen	**Prof. Andrea Krajewski**
Vorstandsvorsitzender der Umweltstiftung Michael Otto	**Prof. Dr. Johannes Merck**
Unternehmer	**Dr. August Oetker**
Neurowissenschaftlerin	**Prof. Dr. Frederike Petzschner**
Informatiker	**Prof. Dr. Peter Reichl**
Sozialpsychologe	**Prof. Dr. Harald Welzer**
Vorstandsvorsitzende der Entega AG	**Dr. Marie-Luise Wolff**