Wolfie Christl

DIGITALE ÜBERWACHUNG UND KONTROLLE AM ARBEITSPLATZ

Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management?

GEFÖRDERT DURCH Digifonds AK WIEN

EINE STUDIE VON CRACKED LABS

Wien, September 2021

Illustrationen: Pascale Osterwalder

Wolfie Christl

Digitale Überwachung und Kontrolle am Arbeitsplatz

Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management?

Cracked Labs, Wien, September 2021

Herausgeber:
Cracked Labs – Institut für Kritische Digitale Kultur
Gumpendorfer Straße 63b, 1060 Wien, Austria
https://crackedlabs.org

Autor:
Wolfie Christl lebt in Wien und ist Forscher, Publizist und Erwachsenenbildner. Er ist Techniker und Programmierer mit sozialwissenschaftlichem Hintergrund und erforscht seit Jahren die Ökonomie persönlicher Daten.
https://wolfie.crackedlabs.org
https://twitter.com/wolfiechristl

Die Durchführung dieser Untersuchung wurde vom Digitalisierungsfonds Arbeit 4.0 der AK Wien unterstützt. Der Fonds wurde im Zuge der großen Digitalisierungsoffensive der Arbeiterkammer ins Leben gerufen und ist Teil des AK Zukunftsprogramms. Mehr unter: wien.arbeiterkammer.at/digifonds

Inhaltsverzeichnis

1. Zusammenfassung

Durch die rasante Entwicklung der Informations- und Kommunikationstechnologien dringt die Erfassung von Daten über ArbeitnehmerInnen immer mehr in den betrieblichen Alltag ein. Die umfassende digitale Protokollierung von Arbeitstätigkeiten wird schnell zur permanenten Überwachung und Kontrolle, die tief in die Rechte und Freiheiten der Betroffenen eingreift. Die Chancen und Risiken sind dabei ungleich verteilt. Während betriebliche Abläufe optimiert werden, geraten ArbeitnehmerInnen unter Druck – und unter Pauschalverdacht. Firmen nutzen permanente Datenerfassung nicht nur zur Sanktionierung von Fehlverhalten und zur Leistungsbewertung, sondern zunehmend als Grundlage für teil- oder vollautomatisierte Entscheidungen, die sich unmittelbar auf den Arbeitsalltag der Beschäftigten auswirken. Die eingesetzten Systeme sind oft komplex und intransparent, das Tempo der Entwicklung hoch. Vor zehn Jahren war etwa noch kaum absehbar, wie weitgehend das Smartphone unseren Alltag verändern wird – auch in der Arbeitswelt. Welche datenverarbeitenden Technologien und Systeme werden heute in Unternehmen eingesetzt? Welche Funktionen bietet die am Markt erhältliche Software? Wie wirken sich diese Technologien auf ArbeitnehmerInnen aus? Inwieweit verändern oder verstärken sie das Machtungleichgewicht zwischen Unternehmen und Beschäftigten? Und wohin geht die Entwicklung?

Die vorliegende Studie gibt einen Überblick über digitale Überwachung und Kontrolle am Arbeitsplatz und über die Verarbeitung personenbezogener Daten über Beschäftigte im Betrieb. Sie dokumentiert, systematisiert und kartographiert relevante Technologien, Systeme und aktuelle Entwicklungen in Hinblick auf ihre Auswirkungen auf Beschäftigte – über Branchen und Tätigkeitsbereiche hinweg, anhand vieler Fallbeispiele und in einer Form, die im deutschen Sprachraum bislang fehlt.

- Neun Fallstudien über am Markt verfügbare Systeme dokumentieren, welche technischen Möglichkeiten und Funktionen betriebliche Software bietet und wie dabei Daten über Beschäftigte verarbeitet werden.
- Zwei Fallstudien befassen sich mit Datenpraktiken bei konkreten Unternehmen – Amazon und Zalando.
- Hans Christian Voigt hat als Teil des Projekts eine kleinere Untersuchung auf Basis von Interviews mit BetriebsrätInnen durchgeführt. Ergebnis sind fünf Fallbeispiele über den konkreten Einsatz datenverarbeitender Systeme in österreichischen Unternehmen, die in der vorliegenden Studie zusammengefasst sind.
- Darüber hinaus wurde eine „Landkarte“ entwickelt, die einen systematischen Überblick über betriebliche Datenpraktiken und Systeme gibt.

Die Studie deckt viele Branchen und Tätigkeitsbereiche ab – von Callcenter, Handel, Warenlager und Zustellung bis zur Wissensarbeit im Büro. Neben Systemen für die digitale Steuerung ganzer Unternehmen und für die Zusammenführung und Analyse von Daten reicht die Bandbreite von Software für Kommunikation und Personalverwaltung bis zu Betrugserkennung und IT-Sicherheit. Mehrere Fallbeispiele dokumentieren beunruhigende und unseriöse Produkte, deren Einsatz in Österreich und Deutschland rechtlich nur schwer vorstellbar ist. Aber auch gängige Systeme wie Microsoft 365 oder SAP verarbeiten heute in exzessiver Weise Daten. Einschätzungen über die datenschutz- und arbeitsrechtliche Zulässigkeit der dokumentierten Beispiele sind aber weitgehend ausgeklammert und könnten Gegenstand einer Folgestudie sein.

Zentral für den Blickwinkel dieser Untersuchung war die Frage, wie Betriebe ihre „Datenmacht“ in Form von Informationen über ArbeitnehmerInnen und ihre Tätigkeiten ausnutzen können, um Arbeit zu steuern und zu kontrollieren. Wie können datenverarbeitende Systeme genutzt werden, um Produktivität zu erhöhen, Kosten zu senken,

Druck auf Beschäftigte auszuüben, Arbeit zu beschleunigen und zu verdichten, Freiräume einzuengen oder Autonomie zu reduzieren? Und nicht zuletzt: Wer gestaltet Digitalisierung im Betrieb – und wer profitiert?

Ein Literaturüberblick führt eine Auswahl an relevanten Publikationen an, die den inhaltlichen Rahmen für diese Untersuchung definiert haben. Wie in der Einleitung diskutiert, führt die Ausweitung der Datenerfassung zu großen Herausforderungen für Mitsprache und Mitbestimmung von Beschäftigten und BetriebsrätInnen. Eine empirische Befragung in Österreich zeigt, dass komplexere Systeme oft ohne „Betriebsvereinbarung" zwischen Betriebsrat und Geschäftsführung eingesetzt werden. In diesem Fall gleicht der betriebliche Einsatz dieser Systeme aus Beschäftigtensicht einem Blindflug.

Die Studie basiert auf mehreren Jahren Arbeit zum Thema und ist sowohl Bestandsaufnahme als auch Startpunkt für weitere Forschung. Sie soll ArbeitnehmerInnen, BetriebsrätInnen und Gewerkschaften ermöglichen, die rasanten technischen und ökonomischen Entwicklungen besser zu navigieren und ist das Hauptergebnis des Projekts „Gläserne Belegschaft", das in Kooperation mit den zwei großen österreichischen Gewerkschaften GPA und PRO-GE durchgeführt und vom Digitalisierungsfonds der österreichischen Arbeiterkammer gefördert wurde. **Wolfie Christl**, der Verfasser dieser Studie, arbeitet seit vielen Jahren zur Ökonomie persönlicher Daten im digitalen Zeitalter, zur Macht der Plattformen und zu datenbasierten „algorithmischen" Entscheidungen über Menschen.

Fallstudien über am Markt verfügbare Systeme

Mehrere Fallbeispiele zeigen, welche Funktionen betriebliche Software in unterschiedlichen Feldern bietet, wie dabei Daten über Beschäftigte verarbeitet werden und wie diese Funktionen eingesetzt werden können – auf Grundlage öffentlich verfügbarer Quellen wie Websites von Firmen, technischer Dokumentation und anderer Literatur.

Aktuell verfügbare **Callcenter-Software** ermöglicht eine nahezu vollständig automatisierte Steuerung und sekundengenaue Totalüberwachung von Arbeitstätigkeiten. Gespräche und damit Arbeitsaufgaben werden auf Basis von Verhaltensdaten automatisiert genau den Beschäftigten zugewiesen, die sie laut Analyse am effektivsten und schnellsten abwickeln werden. Leistungskennzahlen über die Anzahl und Dauer durchgeführter Gespräche sind für die Beschäftigten allgegenwärtig. Im Namen von Qualitätssicherung, Kundenzufriedenheit und „Compliance" werden Gespräche aufgezeichnet, automatisiert bewertet und können nach Stichwörtern durchsucht werden. Auch Funktionen zur Analyse der „Stimmung" in Gesprächen auf Basis von Tonfall, Sprechgeschwindigkeit, Lautstärke und erwähnten Wörtern stehen zur Verfügung. Damit soll etwa bewertet werden, wie „höflich" oder „empathisch" Beschäftigte ihre Arbeit durchführen. Einzelne Hersteller versprechen, Emotionen nicht nur zu analysieren, sondern sie mittels laufender Anweisungen gar zu „steuern". Wie die existierende Literatur zum Thema zeigt, wird zumindest ein Teil dieser Funktionen auch österreichischen und deutschen Callcentern eingesetzt (siehe Abschnitt 6.1).

In **Handel und Gastronomie** bilden Kassendaten fast den ganzen Arbeitsalltag ab und ermöglichen Rückschlüsse über Arbeitstätigkeiten. Erfasst werden neben Bezahlvorgängen auch Daten über die mit dem Barcode-Lesegerät gescannten Produkte an Supermarktkassen oder über aufgenommene Bestellungen in Restaurants. Kassensysteme aus Österreich und Deutschland bieten Funktionen zur beschäftigtenspezifischen Leistungsbewertung auf Grundlage dieser Daten. Ein System des IT-Giganten Oracle überwacht Kassendaten laufend zur Diebstahl- und Betrugserkennung. Als verdächtig eingeschätzte Kassa-MitarbeiterInnen werden namentlich in Listenansichten dargestellt. Für jeden Bezahlvorgang kann der zeitlich passende Ausschnitt eines Überwachungsvideos eingesehen werden.

Gleichzeitig stellt Oracle auf Basis der gleichen Daten umfassende Leistungsauswertungen für Kassa-MitarbeiterInnen und Verkaufspersonal zur Verfügung. Ein anderer Hersteller wertet Bewegungen von Beschäftigten in Geschäftsräumen mit Hilfe automatisierter Videoanalyse aus (siehe Abschnitt 6.2).

Der deutsche Anbieter Celonis vermarktet unter dem Schlagwort „Process Mining" eine Software zur **Analyse, Optimierung und Automatisierung betrieblicher Abläufe**, die vielfältige Daten über Arbeitstätigkeiten von Beschäftigten auswertet. Auf Basis von Aktivitätsdaten aus anderen betrieblichen Systemen von Herstellern wie SAP, Oracle, Microsoft oder Salesforce sollen ineffiziente und „unerwünschte" Abläufe und Arbeitsschritte identifiziert werden. Unter dem Schlagwort „Task Mining" bietet Celonis darüber hinaus an, mit Hilfe einer auf den Rechnern der Beschäftigten installierten Spionagesoftware Bildschirminhalte, Tastatureingaben, Mausklicks, Scrollvorgänge und sogar den Inhalt der Zwischenablage aufzuzeichnen. In Folge werden versandte E-Mails, Aufrufe von Websites oder Interaktionen mit Anwendungen wie Excel den passenden Datensätzen über Aktivitäten aus SAP und anderen Systemen zugeordnet. Auch wenn sich die meisten Auswertungen auf Gruppen, Teams, Abteilungen oder Firmenstandorte beziehen, werden dabei jedenfalls umfassende personenbezogener Daten über Beschäftigte verarbeitet. Neben Auswertungen auf Gruppenebene wirbt Celonis auch mit „Dashboards", die etwa Ranglisten namentlich genannter ArbeitnehmerInnen anzeigen – gereiht nach dem Grad der Pünktlichkeit der Auslieferung der von ihnen bearbeiteten Bestellungen. Aber auch Auswertungen über Gruppen können Druck auf Beschäftigte ausüben. Neben Auswertungen und Analysen bietet Celonis auch Funktionen, die ArbeitnehmerInnen in Echtzeit Arbeitsaufgaben zuweisen, vorschlagen oder erteilen. Bei dieser Form des **algorithmischen Managements** wirkt die Verarbeitung personenbezogener Daten direkt auf die Arbeitstätigkeit zurück (siehe Abschnitt 6.3).

Manche **Systeme für IT-Sicherheit** verarbeiten in einer Weise Verhaltensdaten über ArbeitnehmerInnen, die einer Totalüberwachung des Arbeitsalltags gleichkommt. Neben Bedrohungen von außen – etwa in Form von Cyberangriffen – stehen oft auch Beschäftigte als mögliche „Insider" unter Pauschalverdacht. Die Software von Forcepoint führt zum Beispiel Logdaten aus dem ganzen Betrieb zusammen, berechnet laufend Risikobewertungen für ArbeitnehmerInnen und verspricht, „ungewöhnliches" Verhalten zu erkennen. Überwacht wird jede Nutzung von Geräten und Programmen, jede Ansicht oder Änderung einer Datei, jegliche Kommunikation via E-Mail, Chat oder Telefon, die aufgerufenen Websites, Suchbegriffe, Druckvorgänge und der physische Zutritt zu Räumen. Auch Leistungsdaten aus der Personalverwaltung, GPS-Standorte, die Aktivierung von Kamera und Mikrofon am Rechner oder gar Aufzeichnungen von Bildschirminhalten, Tastatureingaben und Kopiervorgänge über die Zwischenablage können einbezogen werden. Dabei werden Einschätzungen darüber getroffen, ob Beschäftigte in finanziellen Schwierigkeiten stecken, ob sich ihre Arbeitsleistung verringert hat, ob sie Kündigungsabsichten haben, wieviel sie mit KollegInnen kommunizieren, ob sie „obszöne" Inhalte aufrufen oder ob in ihrer Kommunikation eine „negative" Stimmung herrscht. Die Hersteller haben oft einen militärischen oder geheimdienstlichen Hintergrund. Dennoch wird derartige Software in immer mehr Branchen eingesetzt – auch im deutschen Sprachraum (siehe Abschnitt 6.4).

Der Einsatz invasiver Systeme zur **Überwachung der Anwesenheit an Arbeitsplätzen mit Bewegungsmeldern** wird mit Zielen wie Energieeinsparung, einer effizienteren Raumnutzung und Kostensenkung gerechtfertigt. Die Bewegungsmelder von OccupEye, ein Produkt eines Anbieters von Technologie für die Gebäudeverwaltung, können unter Schreibtischen montiert werden. Neben Bewegungen im Raum vermessen die Geräte mit weiteren Sensoren Raumtemperatur, Luftqualität, Luftdruck, Geräuschpegel, Lichtintensität und Feuchtigkeit. Die Anwesenheit von Beschäftigten an Schreibtischen kann auf individueller Ebene in Echtzeit dargestellt und rückwirkend ausgewertet werden. Der Netzwerk-Gigant Cisco bietet an, diese Anwesenheitsdaten mit Informationen über Bewegungsmuster im Büro zu ergänzen und ermöglicht dazu die **Ortung von ArbeitnehmerInnen in Innenräumen**. Die

WLAN-Router, die die Räumlichkeiten mit einem drahtlosen Internetzugang versorgen, dienen als Ortungsgeräte für Laptops, Smartphones und Tablets von Beschäftigten (siehe Abschnitt 6.5).

Einen Schritt weiter geht die US-Firma Humanyze, die ein Produkt für „People Analytics" zur **Vermessung von Bewegungs- und Kommunikationsmustern im Büro** vermarket. Dabei tragen Beschäftigte über den ganzen Arbeitstag hinweg kleine Geräte am Körper, die mit Hilfe eines Mikrofons und anderer Sensoren wie Infrarot und Bluetooth laufend sprachliche Kommunikation und Bewegungen auswerten. Die Software von Humanyze berechnet daraus Kennzahlen, die die „Effektivität", „Anpassungsfähigkeit" und „Produktivität" der Belegschaft bewerten sollen. Auch Charaktereigenschaften, Zufriedenheit, Kreativität, die Einstellung zum Job oder die Zusammenarbeit in Teams wurde mit dem Gerät bereits vermessen. Dazu können Daten aus Systemen von Drittherstellern wie Microsoft, SAP, Workday, Salesforce, Slack oder Zoom können einbezogen werden. Humanyze behauptet, die Software beruhe auf dem „global größten" Datensatz für „Verhaltensweisen am Arbeitsplatz" (siehe Abschnitt 6.6).

Auch die Verbesserung von **Arbeitssicherheit- und -gesundheit** dient als Rechtfertigung für invasive Datenerfassung. Ein Hersteller vermarktet ein am Gürtel getragenes Gerät, das **gesundheitsschädliche Bewegungen** wie falsches Bücken oder exzessive Drehungen erkennen soll und warnt in diesem Fall mit Vibrationen. Aber auch Vorgesetzte können die Zahl der täglichen „Hochrisiko-Bewegungen" von Einzelpersonen einsehen. Ein System von IBM soll mit am Körper getragenen Geräten und **Sensoren in Schuhen und Helmen** die Sicherheit und Gesundheit auf Baustellen oder in der Fabrik verbessern. Neben der Überwachung von Verstößen gegen Sicherheitsregeln wie dem Abnehmen des Helms oder dem Betreten unerlaubter Areale verspricht IBM, mit Hilfe von Standort- und anderen Sensordaten Stürze, Unfälle, schlechte Luftqualität oder große Hitze genauso zu erkennen wie eine zu hohe Herzfrequenz, Dehydrierung, Überanstrengung oder Übermüdung. Bei Problemen erhalten Beschäftigte Warnungen. Führungskräfte haben Zugriff auf Live-Kartenansichten und Auswertungen. Ein anderer Anbieter vermarktet eine Software, die verspricht, durch die Überwachung von **Tippverhalten und Mausbewegungen** die Ermüdungsgrad von Bildschirm-ArbeiterInnen einzuschätzen – etwa im Callcenter. Vorgesetzte sehen individuelle Auswertungen, die die „gemessene" Ermüdung ins Verhältnis zu Leistungskennzahlen setzen (siehe Abschnitt 6.7).

Ein **Fuhrparkverwaltungs-System** des österreichischen Anbieters Easytrack, das für Branchen wie Transport, Bau, Handwerk oder Gesundheitswesen beworben wird, erfasst vielfältige Daten wie exakte GPS-Standorte, Motor-Leerläufe, plötzliche Beschleunigungen und Bremsungen, gefahrene Routen und Arbeitszeiten. Vorgesetzte können E-Mail-Benachrichtigungen bekommen, wenn ein Beschäftigter zu schnell fährt, den Motor zu lang im Stand laufen lässt, das Fahrzeug außerplanmäßig stoppt oder einen definierten Bereich verlässt. Es wird betont, man könne das Gerät im Fahrzeug „gut versteckt verbauen". Routific, eine Software zum **automatisierten Management von ZustellerInnen und Routen**, steuert die zu fahrenden Routen und damit den Arbeitsalltag weitgehend automatisiert. Das System verspricht, die Routen in Echtzeit immer wieder neu zu optimieren. Grundlage dafür sind nicht nur Echtzeit-Standortdaten, Zustelladressen, Zeitpunkte, Fahrzeugkapazitäten und Schichtpläne, sondern auch Voreinstellungen für die Zeit, die den ZustellerInnen vor Ort zur Verfügung steht. Vorgesetzte können für einzelne Beschäftigte individuell eine Soll-Geschwindigkeit vorgeben. Diese kann zwischen 10% und 190% der vom Navigationsdienst berechneten Geschwindigkeit liegen. (siehe Abschnitt 6.8).

International bieten mehrere Unternehmen Software zur Auswertung und **Überwachung von Socialmedia-Aktivitäten** von Beschäftigten an – vor Neueinstellungen, aber auch für bestehendes Personal. Sie werten damit Daten über Verhaltensweisen außerhalb des Arbeitsverhältnisses aus und versprechen etwa, Kündigungsabsichten vorherzusagen oder Qualifikationsprofile für die Personalplanung zu erstellen. Auch der Grad der „Identifikation" mit

dem Unternehmen, der Grad der digitalen Vernetzung von ArbeitnehmerInnen oder die Stimmungslage in der Belegschaft werden auf Basis von Socialmedia-Daten vermessen. Neben der Erkennung von Betrug oder Bedrohungen für die Sicherheit oder die „Reputation" eines Unternehmens können die Socialmedia-Aktivitäten von Beschäftigten auch in Hinblick auf Mobbing, sexuelle Belästigung, rassistische Aussagen, sexuell explizite Kommunikation oder „potenziell illegale Aktivitäten" ausgewertet werden. Prewave, ein in Wien beheimatetes Startup, bietet an, auf Basis von Socialmedia-Daten **Streiks** und andere „Risiken" für die Lieferkette vorherzusagen. Wie 2020 bekannt wurde, hat Amazon sogar „private" Facebook-Diskussionsgruppen teilautomatisiert ausgewertet, in denen sich Beschäftigte aus den USA, Spanien und Großbritannien gewerkschaftlich organisiert haben (siehe Abschnitt 6.9).

Fallstudien über Systeme in konkreten Betrieben

Zwei Fallbeispiele dokumentieren algorithmische Kontrolle in den Logistik- und Verteilzentren von Amazon sowie ein umfassendes System zur Personalsteuerung auf Basis gegenseitiger Bewertungen bei Zalando.

Der Plattform-Gigant Amazon setzt in seinen globalen Paketverteilzentren für hunderttausende Beschäftigte ein umfassendes System zur sekundengenauen **Leistungskontrolle und automatisierten Steuerung** jedes noch so kleinen Arbeitsschritts auf Basis von Handscannern ein. Die Handscanner sind dabei nicht nur mobile Aufzeichnungs- und Überwachungswerkzeuge, sondern geben mittels Display vor, welches Produkt als nächstes aus einem Regal geholt, in eine Kiste gelegt oder in ein Regal gestellt werden soll – und zählen die Sekunden hinunter, die für den nächsten Arbeitsschritt zur Verfügung stehen. Ist der Zähler abgelaufen, wird die restliche Zeit als „unproduktive" Zeit aufsummiert. Leistungsauswertungen über die Zahl der bearbeiteten Produkte pro Stunde oder die durchschnittliche Taktrate in Sekunden pro Produkt sind für die Beschäftigten allgegenwärtig. Werden die Vorgaben nicht erfüllt, erfolgen automatisierte Verwarnungen und gar Kündigungen. Berichte aus Deutschland und Österreich legen nahe, dass zumindest Teile des Systems auch hierzulande im Einsatz sind, dass die Leistungskontrolle und mögliche Sanktionen aber nicht offen erfolgen, sondern indirekt durch Vorgesetzte vermittelt (siehe Abschnitt 7.1).

Der deutsche Versandhandelsriese Zalando setzt seit 2017 ein umfassendes Kontrollsystem ein, das laufende gegenseitige Bewertungen unter KollegInnen beinhaltet – wie eine von der gewerkschaftlichen Hans-Böckler-Stiftung veröffentlichte Studie zeigt. Der Konzern sortiert tausende Beschäftigte im Bürobereich in **drei Leistungsgruppen von niedrig über mittel bis hoch**. Laut einem internen Handbuch wird das System für Entscheidungen über Gehaltserhöhungen und Beförderungen eingesetzt. Beschäftigte nehmen es als „System der totalen Kontrolle" wahr. Die Studienautoren, gegen die Zalando rechtlich vorgegangen ist, sehen es als intransparentes Kontrollinstrument, das innerbetriebliche Konkurrenz und Leistungsdruck verstärkt, Solidarität unterminiert, potenziell zu Willkür führt und negative Auswirkungen auf Betriebsklima und Arbeitsqualität haben könne. Durch die gegenseitigen Bewertungen werde betriebliche Kontrolle verschleiert. Das System werde als objektives Messverfahren dargestellt, sei aber einseitig im betrieblichen Interesse gestaltet und verzerre damit die Ergebnisse. Eine systematische Verknappung positiver Bewertungen diene der Kostensenkung und Lohnrepression (siehe Abschnitt 7.2).

Fallbeispiele aus österreichischen Betrieben

Fünf Fallbeispiele zeigen auf Grundlage von Interviews mit BetriebsrätInnen, wie digitale Überwachung und Kontrolle in österreichischen Betrieben eingesetzt wird. Sie sind das Ergebnis einer von Hans Christian Voigt im Rahmen des Projekts durchgeführten explorativen Untersuchung, die in der vorliegenden Studie zusammengefasst ist:

- Bei Beschäftigten in der **Anlagenwartung im Außendienst** werden Arbeitsschritte über eine Smartphone-App nicht nur digital dokumentiert, sondern auch immer mehr vorgegeben. In der Zentrale ist einsehbar, wer

woran arbeitet. Auch Kundenbetriebe bekommen Einblick, Beschäftigtendaten werden zum Produkt. Das Smartphone hat die Überwachung und Kontrolle der Belegschaft verschärft und Arbeit beschleunigt. In Gesprächen mit Vorgesetzten wird teils wöchentlich die Zeit für einzelne Arbeitsschritte diskutiert. Die für Tätigkeiten zur Verfügung stehende Zeit hat sich im Lauf der Jahre auf einen Bruchteil reduziert. Die Komplexität der Systeme und laufende Updates machen sie intransparent (siehe Abschnitt 8.1).

- Von drei Organisationen aus dem **Sozial- und Gesundheitsbereich** kommt keine ihren Informationspflichten nach. Die BetriebsrätInnen wissen nicht genau, welche datenverarbeitenden Systeme im Einsatz sind. In zwei Betrieben wurden Beschäftigte mit Ranglisten und unzulässigen Auswertungen von Krankenständen unter Druck gesetzt. In einem Betrieb ist ein System im Einsatz, das Daten über einzelne Arbeitsschritte erfasst, Normzeiten vorgibt und so den Arbeitsalltag in ein rigides Raster zwängt (siehe Abschnitt 8.2).
- Bei einem **Plattform-Zustelldienst** zur Essensauslieferung werden die Arbeitstätigkeiten von FahrradbotInnen fast vollständig mittels Smartphone-App gesteuert und kontrolliert. Ein Teil des Verdiensts hängt von den bewältigten Kilometern und Zustellvorgängen ab. Ein wöchentliches Leistungs-Ranking bestimmt darüber, wer als erstes die besten Schichten für die Folgewoche auswählen kann. Fehlverhalten kann zu Sanktionen wie einer automatischen Beendigung der Schicht durch die App führen (siehe Abschnitt 8.5).
- Zwei weitere Fallbeispiele zeigen, wie der Betriebsrat einer **„Smart Factory“** damit umgeht, dass monatlich neue datenverarbeitende Systeme eingeführt werden, und wie in der **Banken- und Finanzbranche** erfolgreich die Einführung invasiver Personalverwaltungssysteme verhindert wurde (siehe Abschnitte 8.3 und 8.4).

Landkarte betrieblicher Datenpraktiken und Systeme

Im Rahmen der Studie wurde eine Systematik betrieblicher Datenpraktiken entwickelt. Auch wenn die Grenzziehung zwischen den Kategorien teils unscharf ist, soll das Resultat als „Landkarte“ einen Überblick über die Vielfalt betrieblicher Systemen, die heute personenbezogene Beschäftigtendaten verarbeiten, bieten.

Steuerung und Kontrolle von Arbeitstätigkeiten. Zur Erfüllung ihrer Kerntätigkeiten setzen Unternehmen in Produktion und Dienstleistung unterschiedliche datenverarbeitende Systeme ein, die betriebliche Abläufe und Arbeitstätigkeiten organisieren, steuern und kontrollieren. Dabei wird offen oder versteckt eine Vielfalt an personenbezogenen Daten über Beschäftigte verarbeitet, die zur Überwachung von Arbeitsleistung und Verhalten eingesetzt werden kann. Nahezu jedes technische System protokolliert heute Daten über Aktivitäten und Verhaltensweisen. Computer und Smartphones samt der darauf genutzten betrieblichen Software speichern Logdaten, die potenziell Auskunft über kleinste Arbeitsschritte geben. Immer mehr Geräte, Maschinen, Fahrzeuge und Räumlichkeiten sind mit vernetzten Sensoren ausgestattet. Viele Systeme erfassen gezielt Informationen über die Dauer, Durchführung und Ergebnisse von Abläufen und Arbeitstätigkeiten. SAP und andere ERP-Systeme, die zur Steuerung mittlerer und großer Betriebe genutzt werden, ermöglichen eine lückenlose Nachvollziehbarkeit vieler Arbeitsschritte. In der Produktion dokumentieren Betriebs- und Maschinendaten aus Systemen für Fertigungssteuerung und Qualitätssicherung fast jeden Arbeitsschritt. Auch viele andere branchen- und tätigkeitsspezifische Systeme erfassen detaillierte Daten über Arbeitstätigkeiten, die sich für die Kontrolle von Verhalten und Leistung eignen, zum Beispiel:

- Kassendaten in Einzelhandel und Gastronomie
- Daten von Handscannern oder anderen tragbaren Geräten in Logistikzentren und Produktionshallen
- Daten über gefahrene Routen in Logistik und Zustellung
- Mobile Daten über Aufträge und Fahrten in Außendienst, Handwerk, technischer Wartung oder Pflege
- Protokolldaten über Tätigkeiten in Microsoft 365 von Office bis Kommunikation

- Daten aus Systemen für Projektmanagement und Aufgabenverwaltung
- Daten über Verkäufe und Kundenkontakte aus Salesforce und anderen CRM-Systemen
- Daten über die Anzahl, Dauer und zum Teil sogar über den Inhalt von Gesprächen in Callcentern

Wo Arbeitstätigkeiten nicht nur vermessen, sondern auf der Basis von Datenerfassung und -analyse auch digital gesteuert werden, kann von algorithmischem Management gesprochen werden. In vielen Bereichen werden Arbeitsaufgaben heute teil- oder vollautomatisiert vorgegeben, zugewiesen, vorgeschlagen oder priorisiert – etwa Anrufe im Callcenter, Zustellrouten, die zu bearbeitenden Produkte im Logistikzentrum, Tätigkeiten bei der Wartung von Anlagen oder Arbeitsschritte bei der Bearbeitung von Versicherungsfällen und anderen standardisierten Abläufen. Die Einhaltung von Leistungs- und Zeitvorgaben kann durch automatisierte Rückmeldungen an Beschäftigte sichergestellt werden – von Warnungen über einen „Rückstau" zugewiesener Tätigkeiten bis zu den herabzählenden Sekunden, die in den Verteilzentren von Amazon anzeigen, wieviel Zeit für den aktuellen Arbeitsschritt noch zur Verfügung steht. Auch die tagesaktuelle Anpassung von Schichtplänen oder die Verteilung des anwesenden Personals auf Maschinen, Verkaufsabteilungen oder Baustellen werden automatisiert – ebenso die Zuweisung von Tätigkeiten im Projektmanagementsystem auf Basis von Beurteilungen von Fähigkeit und Leistung. Auf der Makroebene kann jede digitale Strukturierung von Arbeitsabläufen in ERP-Systemen oder die Ableitung betrieblicher Handlungen aus Kennzahlen als eine Form des algorithmischen Managements betrachtet werden (siehe Abschnitt 5.3).

Personalverwaltung. Zeitgenössische Personalverwaltungssysteme wie SAP SuccessFactors oder Workday gehen weit über die Erfassung von An- und Abwesenheiten, Stammdaten und Gehaltsabrechnung hinaus. Sie bieten Funktionen zur Profilierung und Bewertung von Fähigkeiten, Kompetenzen, Arbeitsleistung und „Potenzial" von ArbeitnehmerInnen. Unter Einbeziehungen von Beurteilungen durch KollegInnen können ganze Belegschaften in gute und schlechte Beschäftigte sortiert werden. Auch Daten über Arbeitstätigkeiten, Weiterbildungsmaßnahmen oder Online-Umfragen können einfließen. In Kombination mit Zielvorgaben, Belohnungen und Bestrafungen entsteht ein umfassendes Kontrollsystem, das für Entscheidungen über Entlohnung, Versetzungen, Beförderungen und die Zuweisung zu Positionen, Projekten und innerbetrieblichen Fördermaßnahmen genutzt wird – oder gar für die Disziplinierung bis hin zur Kündigung. Eine unternehmensweite Personalsteuerung mit Zielvorgaben, Beurteilungen und davon abgeleiteten Maßnahmen kann als eine Form des algorithmischen Managements betrachtet werden. Auch nichtmaterielle Anreize können zur Leistungssteuerung und -steigerung eingesetzt werden – etwa in Form von Spielmechaniken mit Punktesystemen, Wettbewerben und Ranglisten. Die Vorhersage von Kündigungsabsichten, künftiger Arbeitsleistung oder der künftigen Eignung für bestimmte Jobs und Fördermaßnahmen kann ganze Erwerbsbiografien prägen. Daten über Fähigkeiten und Leistung können auch unmittelbar in den Arbeitsalltag einbezogen werden – von automatisierter Personaleinsatz- und Schichtplanung bis zur Zuweisung von Arbeitstätigkeiten im Callcenter, bei mobilen Wartungstätigkeiten oder in Systemen für Projektmanagement und Aufgabenverwaltung. Auch Leistungskennzahlen über Teams oder Abteilungen können Druck ausüben (siehe Abschnitt 5.4).

Infrastruktur und Verwaltung. Auch abseits von betrieblicher Kerntätigkeit und Personalverwaltung erfassen Unternehmen an vielen Stellen Beschäftigtendaten. Räume und Gebäude werden zunehmend zu vernetzten Umgebungen, in denen unterschiedlichste Vorgänge und Zustände digital gesteuert und überwacht werden – von Instandhaltung, Reinigung und Müllentsorgung über Raumtemperatur und Beleuchtung bis zu Rauch- und Feuermeldern, Alarmanlagen und Überwachungskameras. Viele Geräte, Maschinen, Werkzeuge oder Fahrzeuge erfassen Daten – von Kaffeemaschinen und Reinigungsgeräten über Baumaschinen und medizinischen Geräten im Krankenhaus bis zur „Smart Factory". Zutrittssysteme wissen, wer das Gebäude oder Innenräume wie Liftanlagen, Büros, Bespre-

chungsräume, Produktionshallen, Labore oder Rechenzentren betritt. Wer zutrittsberechtigt ist, wird mittels Chipkarte, Code oder Fingerabdruck geprüft. Auch die Anmeldung bei Geräten wie Kassenterminals, Maschinen, Druckern, Kopierern oder die Entnahme von Schutzausrüstung oder Werkzeugen aus Ausgabeautomaten kann erfasst werden. Das digitale Gegenstück zur physischen Zutrittskontrolle sind die Useraccounts und Berechtigungen, die festlegen, wer auf welche Programme, Funktionen und Daten zugreifen darf. Sobald ein Login erfolgt, kann potenziell jede Aktivität einer bestimmten Person zugeordnet werden. Die betriebliche IT-Infrastruktur ermöglicht meist einen weitreichenden Zugriff auf Daten über das Verhalten von ArbeitnehmerInnen. Wer Zugang zum gesamten Datenverkehr auf Netzwerkebene hat, hat umfassende Kontrolle über Web-Nutzung, E-Mail-Kommunikation und andere Dienste. Viele dieser Daten werden protokolliert. Rechner, Laptops, Smartphones oder andere Geräte und die darauf installierte Software werden meist vollständig aus der Ferne kontrolliert (siehe Abschnitt 5.5).

IT-Sicherheit, Diebstahl- und Betrugserkennung, Arbeitssicherheit und -gesundheit. Wie in vielen Gesellschaftsbereichen dient auch im Betrieb „Sicherheit“ als Rechtfertigung für teils exzessive Überwachungsmaßnahmen. Videoüberwachung wird schon lange problematisiert. Ihr Kontrollcharakter erhöht sich nochmals massiv durch Technologien, die Kamerabilder automatisiert auswerten, um Verhalten zu analysieren oder Personen zu identifizieren. Darüber hinaus werten Unternehmen zur Verhinderung von Diebstahl, Betrug, Korruption, kriminellem Verhalten oder sonstiger Verstöße gegen betriebliche Regeln oft umfassende Datenbestände aus, die Auskunft über betriebliche Abläufe und Arbeitstätigkeiten geben – etwa auf Basis von Daten aus ERP-Systemen wie SAP. Auch das Schlagwort „Compliance“ dient als Rechtfertigung. Im Handel überwachen Systeme zur Betrugserkennung Daten über Kassatätigkeiten und berechnen laufend Risikowertungen für Beschäftigte. Neuere Software im Bereich IT-Sicherheit führt Verhaltensdaten aus vielen anderen betrieblichen Systemen in einer Weise zusammen, die einer Totalüberwachung gleichkommt. Analysiert wird die Nutzung von Geräten und Programmen, Zugriffe auf Websites, Änderungen an Dateien, Kommunikation via E-Mail, Chat und Telefon oder gar sämtliche Tastatureingaben und Bildschirminhalte. Neben Bedrohungen von außen geraten Beschäftigte als mögliche „Insider“ unter Pauschalverdacht. Manche Produkte treffen Einschätzungen über die finanzielle Situation von ArbeitnehmerInnen, über ihre Arbeitsleistung und ihr Kommunikationsverhalten. Auch zur Verbesserung von Arbeitssicherheit und -gesundheit werden Produkte angeboten, die sehr sensible Daten erfassen und auswerten – wie etwa die Überwachung sämtlicher Bewegungen und Körperfunktionen mit Hilfe tragbarer Geräte (siehe Abschnitt 5.6).

Kommunikation und Zusammenarbeit. Unternehmen haben meist weitreichenden Zugriff auf Daten über zwischenmenschliche Kommunikation im Betrieb via Telefon, Smartphone, E-Mail, Chat oder Videokonferenz. Neben Diensten für einzelne Kommunikationskanäle kommen Systeme zum Einsatz, die mehrere Kanäle miteinander verbinden – bis hin zum innerbetrieblichen „sozialen Netzwerk“. Während Kommunikationssysteme sehr sichtbar sind, ist kaum nachvollziehbar, wie die Daten ausgewertet werden. Neben den Inhalten der Kommunikation ermöglichen auch Metadaten – also Informationen darüber, wer mit wem zu welchen Zeitpunkten in welcher Form kommuniziert – vielfältige Auswertungen. Manche Systeme für IT-Sicherheit oder zur Verhinderung von Betrug und anderen unerwünschten Verhaltensweisen überwachen systematisch jegliche betriebliche Kommunikation. Im Callcenter werden Kommunikationsdaten für die Bewertung der Arbeitsleistung genutzt – bis hin zur Vermessung von Stimmung und Emotionen in Gesprächen. Eine US-Firma wertet mit tragbaren Geräten mit eingebautem Mikrofon aus, wie ArbeitnehmerInnen im Büro miteinander sprechen. Auch Microsoft, das mit Outlook, Teams und anderen Produkten viele Arten der betrieblichen Kommunikation und Zusammenarbeit abdeckt, ermöglicht exzessive Auswertungen. Mit Microsoft „Workplace Analytics“ können Firmen analysieren, wieviel Zeit Beschäftigte mit Videokonferenzen, Besprechungen oder E-Mail-Versand verbringen – innerhalb und außerhalb der Arbeitszeit. Neben fragwürdigen Auswertungen über die Beziehungen zwischen den Beschäftigten oder der „Qualität“ von Besprechungen

können Kommunikationsvorgänge automatisiert nach Schlüsselwörtern in Betreffzeilen durchsucht werden. Auch wenn sich die meisten Berichte auf Gruppen beziehen und bei Auswertungen über Einzelpersonen keine Namen dargestellt werden, werden dabei umfassende Kommunikationsdaten verarbeitet. Delve, ein anderes Produkt von Microsoft, nutzt diese Daten für personalisierte Empfehlungen. Plattformen wie Microsoft Teams oder Slack können Kommunikation für bestimmte Zwecke durch Erweiterungen von Drittherstellern in einer Art strukturieren, die sie zu Systemen der Steuerung und Kontrolle von Abläufen und Arbeitstätigkeiten macht (siehe Abschnitt 5.7).

Datenintegration und Analyse. Die in einzelnen technischen Systemen für bestimmte Zwecke erfassten Daten werden zunehmend zusammengeführt, um betriebliche Abläufe – und damit auch das Verhalten der Beschäftigten – zu analysieren, zu bewerten und schlussendlich zu steuern. Abläufe sollen kostengünstiger oder effizienter werden. Kennzahlen spielen dabei eine wichtige Rolle. Grundlage für Analysen sind digitale Protokolle, in denen SAP und andere betriebliche Software detaillierte Informationen über sämtliche Aktivitäten speichern. Neben Auswertungen unter Schlagwörtern wie „Business Intelligence“ oder „Process Mining“ können personenbezogene Daten auch in einer Weise zusammengeführt und analysiert werden, die unmittelbar in den Arbeitsprozess zurückwirkt – etwa in Form von Vorgaben oder Handlungsempfehlungen. Die Verlagerung von Datenverarbeitung und Software in die „Cloud“ führt einerseits dazu, dass Betriebe die direkte Kontrolle an die Anbieter cloudbasierter Dienste abgeben. Andererseits speichern diese Dienste laufend Daten über Aktivitäten und Verhalten und können meist einfach miteinander integriert und verbunden werden. APIs und andere Schnittstellen ermöglichen einen automatisierten Zugriff auf Daten und Funktionen. Cloudbasierte Systeme werden zur „Plattform“, deren Funktionen durch die Aktivierung einer zusätzlichen „App“ schnell erweitert werden kann. Die laufende Speicherung von Aktivitätsdaten, laufende Updates und die unkomplizierte Integration und Erweiterbarkeit cloudbasierter Dienste führen dazu, dass Beschäftigte kaum mehr nachvollziehen können, welche personenbezogenen Daten zu welchen Zwecken verarbeitet werden – und welcher Anbieter sie überhaupt verarbeitet. Mächtige cloudbasierte Systeme wie Microsoft 365 spielen im Arbeitsalltag eine so wichtige Rolle, dass die innerhalb dieser Dienste verarbeiteten Daten für sich alleine bereits eine weitreichende Zusammenführung von Daten über Arbeitstätigkeiten darstellen kann. Manche cloudbasierten Dienste verarbeiten Beschäftigtendaten sogar über mehrere Betriebe hinweg (siehe Abschnitt 5.8).

2. Einleitung

Durch die rasante Entwicklung der Informations- und Kommunikationstechnologien dringt die Erfassung von Daten über ArbeitnehmerInnen immer mehr in den betrieblichen Alltag ein. Die umfassende digitale Protokollierung von Arbeitstätigkeiten wird schnell zur permanenten Überwachung und Kontrolle, die tief in die Rechte und Freiheiten der Betroffenen eingreift. Die Chancen und Risiken sind dabei ungleich verteilt. Während betriebliche Abläufe optimiert werden, geraten ArbeitnehmerInnen unter Druck – und unter Pauschalverdacht. Firmen nutzen permanente Datenerfassung nicht nur zur Sanktionierung von Fehlverhalten und zur Leistungsbewertung, sondern zunehmend als Grundlage für teil- oder vollautomatisierte Entscheidungen, die sich unmittelbar auf den Arbeitsalltag der Beschäftigten auswirken. Die eingesetzten Systeme sind oft komplex und intransparent, das Tempo der Entwicklung hoch. Vor zehn Jahren war etwa noch kaum absehbar, wie weitgehend das Smartphone unseren Alltag verändern wird – auch in der Arbeitswelt. Welche datenverarbeitenden Technologien und Systeme werden heute in Unternehmen eingesetzt? Welche Funktionen bietet die am Markt erhältliche Software? Wie wirken sich diese Technologien auf ArbeitnehmerInnen aus? Inwieweit verändern oder verstärken sie das Machtungleichgewicht zwischen Unternehmen und Beschäftigten? Und wohin geht die Entwicklung?

Die vorliegende Studie gibt einen Überblick über digitale Überwachung und Kontrolle am Arbeitsplatz und über die Verarbeitung personenbezogener Daten über Beschäftigte im Betrieb. Sie dokumentiert, systematisiert und kartographiert relevante Technologien, Systeme und aktuelle Entwicklungen in Hinblick auf ihre Auswirkungen auf Beschäftigte – über Branchen und Tätigkeitsbereiche hinweg, anhand vieler Fallbeispiele und in einer Form, die im deutschen Sprachraum bislang fehlt. Sie ist Bestandsaufnahme sowie Auftrag für weitere Forschung und soll ArbeitnehmerInnen, Mitbestimmungsorganen und Gewerkschaften ermöglichen, die rasanten technischen und ökonomischen Entwicklungen besser zu navigieren.

Die Studie ist das Hauptergebnis des Projekts „Gläserne Belegschaft“, das in Kooperation mit den zwei großen österreichischen Gewerkschaften GPA und PRO-GE durchgeführt und vom Digitalisierungsfonds der österreichischen Arbeiterkammer gefördert wurde. **Wolfie Christl**, der Verfasser dieser Studie, arbeitet seit vielen Jahren zur Ökonomie persönlicher Daten im digitalen Zeitalter, zur Macht der Plattformen und zu datenbasierten „algorithmischen“ Entscheidungen über Menschen – bislang hauptsächlich aus Sicht der VerbraucherInnen. Er hat mehrere umfangreiche Studien veröffentlicht und zu Untersuchungen über die zeitgenössische Datenindustrie beigetragen, die prominent auf globaler Ebene wahrgenommen und vielfach zitiert wurden.[1] Gleichzeitig hat er für österreichische Gewerkschaften seit 2014 zahlreiche Seminare und Schulungen für insgesamt hunderte BetriebsrätInnen und andere Beschäftigte über Datenschutz und Überwachung durchgeführt und dabei wertvolle Einblicke in betriebliche Datenpraktiken erhalten. Sowohl seine Arbeit über die Logiken der Datenindustrie aus Sicht der VerbraucherInnen als auch sein Einblick in den betrieblichen Bereich waren wichtige Grundlagen für diese Studie.

Inhaltlicher Rahmen und Blickwinkel

Überwachung ist nach David Lyon (2007) die „zielgerichtete, systematische und alltägliche Aufmerksamkeit auf persönliche Details für Zwecke der Einflussnahme, der Führung, des Schutzes oder der Lenkung“. Überwachung ist nach dieser Definition nicht zwingend immer unerwünscht. Sie kann die Sicherheit oder Gesundheit der Überwachten sicherstellen – von den RettungsschwimmerInnen am Badestrand bis zu Überwachungstechnologien, die

[1] Siehe z.B. Christl und Spiekermann (2016), Christl (2017), Norwegian Consumer Council (2020)

das Überleben auf einer Intensivstation sicherstellen. Sie kann aber auch dazu dienen, die Überwachten zu lenken und zu kontrollieren. Überwachung ist in Gesellschaften, die auf Informationstechnologie beruhen, alltäglich. In den daraus entstehenden Machtbeziehungen sind die Überwachenden privilegiert. Überwachung kann auch eine ständige Sortierung, Klassifizierung und Bewertung der Überwachten beinhalten – auf Basis von Informationstechnologie und Daten über Einzelpersonen oder Gruppen (vgl. Lyon 2003). Sobald die Betroffenen in Folge unterschiedlich behandelt werden, ist eine derartige Sortierung per se diskriminierend und hat potenziell Einfluss auf die Chancen und Möglichkeiten der Betroffenen. Im Betrieb herrscht grundsätzlich ein Machtungleichgewicht zwischen Unternehmen und Beschäftigten. Wie digitale Überwachungstechnologien dieses Machtungleichgewicht verändern oder verstärken, zählt zu den Kernfragen, die dieser Studie zugrunde liegen. Die Ausweitung der Datenerfassung bietet Unternehmen Möglichkeiten, Abläufe – und Beschäftigte – besser zu steuern und zu kontrollieren.

Durchdringung vieler betrieblicher Bereiche mit Datenverarbeitung. In vielen Bereichen der Arbeitswelt ist die Verarbeitung personenbezogener Daten – ähnlich wie in unserem privaten Leben – geradezu allgegenwärtig geworden. War Microsoft Word früher eine Anwendung, die recht isoliert und eigenständig auf dem PC gelaufen ist, speichert Microsoft 365 heute kontinuierlich Daten über Aktivitäten und Verhaltensweisen in der Cloud. Sobald am PC gearbeitet wird, werden umfassende Daten über Arbeitstätigkeiten aufgezeichnet – ob im Callcenter oder in der hochqualifizierten Wissensarbeit. Mächtige Systeme wie SAP, die in mittleren und großen Unternehmen viele betrieblichen Abläufe und Arbeitstätigkeiten steuern, protokollieren jeden Arbeitsschritt. Aus Smartphone-Apps für die Zeiterfassung wird durch Funktionen für Arbeitsorganisation und Kundenabrechnung schnell ein umfassendes Kontrollwerkzeug – egal ob im Verkauf, bei der Wartung von Anlagen, bei der Hausreinigung oder in der mobilen Pflege. Dabei sind Smartphones heute bei weitem nicht die einzigen Geräte, die mit einer Vielzahl an Sensoren permanent Daten über das Verhalten ihrer Nutzer und ihrer Umgebung erfassen und diese über eine Netzwerkverbindung in Echtzeit in unterschiedlichen Datenbanken ablegen.

Während der Barcode-Scanner an der Supermarktkasse, in der Fabrik oder in einem Warenlager schon länger Daten über diejenigen erfasst, die damit arbeiten, dehnt sich die zentralisierte Speicherung von Verhaltensdaten heute in viele andere Bereiche aus – vom vernetzten Bauschuttcontainer über das vernetzte Hochdruckreinigungsgerät bis zum vernetzten Servierwagen im Hotel. Maschinen, Fabrikhallen, Bürogebäude, Fahrzeuge und andere Arbeitsplätze werden zu digital vernetzten Umgebungen. Nahezu jedes technische System protokolliert heute Aktivitäten, Abläufe und Verhaltensweisen – und wird potenziell zur Datenquelle. Die erfassten Daten werden zunehmend zusammengeführt und ausgewertet – lokal, in Datenbanken von Konzernzentralen und in der Cloud.

Invasive Eingriffe und unheimliche Technologien. In der öffentlichen Debatte zu Überwachung am Arbeitsplatz werden oft besonders invasive Eingriffe in Privatsphäre und Persönlichkeitsrechte von Beschäftigten diskutiert. Neben Kameras in Umkleidebereichen oder der Überwachung von Toilettenbesuchen geht es dabei etwa um den Missbrauch von Gesundheitsdaten, Kündigungen bei Schwangerschaften oder gar das gezielte Ausspionieren des Betriebsrats. Während die Verhinderung eines gezielten Missbrauchs sensibler Daten, der durch die Ausweitung der Datenerfassung zweifellos sehr viel einfacher geworden ist, als Minimalvoraussetzung gelten muss, werden derartige Eingriffe in dieser Studie nur am Rande thematisiert. In zweiter Linie werden oft besonders spektakuläre Praktiken diskutiert, die entweder die massenhafte Auswertung besonders sensibler Daten beinhalten – oder besonders sensible Schlussfolgerungen über Beschäftigte. Dazu zählen Systeme, die systematisch Kommunikation, Bewegungen oder andere Verhaltensdaten über ganze Belegschaften auswerten, aber auch Technologien, die unter dem Schlagwort der „künstlichen Intelligenz“ vermarktet werden und versprechen, Einschätzungen oder Vorhersagen zu treffen, die von vielen Menschen als invasiv und unheimlich wahrgenommen werden – zum Beispiel über

Charaktereigenschaften, Fähigkeiten, Beziehungen, Emotionen oder über zukünftige Arbeitsleistung. Die Studie enthält diesbezüglich mehrere Fallbeispiele. Manchmal bleibt jedoch unklar, ob solche als besonders invasiv oder unheimlich wahrgenommenen Technologien überhaupt ihre Verkaufsversprechen erfüllen können. Außerdem stellt sich die Frage, ob sie auch diejenigen sind, die in der Praxis die relevantesten Auswirkungen auf Beschäftigte haben.

Steuerung und Kontrolle von Arbeitstätigkeiten. Im Mittelpunkt dieser Studie steht die Frage, wie Betriebe Daten über ArbeitnehmerInnen und ihre Tätigkeiten – und damit ihre Machtposition als Beobachtende – ausnutzen können, um Arbeit zum Nachteil der Beschäftigten effizienter zu steuern und zu kontrollieren, Produktivität zu erhöhen oder Kosten zu senken. Wie können datenverarbeitende Systeme genutzt werden, um Druck auf Beschäftigte auszuüben, Arbeit zu beschleunigen und zu verdichten, Freiräume einzuengen, Autonomie und Sinnstiftung zu reduzieren, Arbeit besser auslagern zu können oder gar Löhne zu senken? In den letzten Jahren ist oft vom „digitalen Taylorismus" die Rede, die Neuauflage einer Management-Lehre, die sich schon Anfang des 20. Jahrhunderts damit befasst hat, wie Arbeitstätigkeiten standardisiert, vermessen und kontrolliert werden können (vgl. Taylor 1911). Im Callcenter wird heute die Zeit bis zur Annahme eines Anrufs in Sekunden vermessen, in den Logistikzentren von Amazon jeder einzelne Arbeitsschritt erfasst und ausgewertet. Damit soll die Arbeitsleistung der Beschäftigten gesteuert und kontrolliert und schlussendlich erhöht werden. Wo finden sich derartige Praktiken in anderen Branchen und Tätigkeitsbereichen und welche Funktionen bieten die verfügbaren technischen Systeme?

Gabriele Faßauer (2008) versteht unter betrieblicher **Leistungssteuerung** alle „organisationalen Aktivitäten der Schaffung und Anwendung von Rahmenbedingungen und Instrumenten", die „der Anpassung des Verhaltens und der Handlungen der Organisationsmitglieder an die Ziele der Organisation dienen und in der Weise ‚Arbeitsleistung' definieren". Digitale Überwachung im Sinne von David Lyon ist dazu geeignet, genau diese Anpassung des Verhaltens der Beschäftigten an die geschäftlichen Ziele des Unternehmens zu verbessern. Für diesen Zweck ist nicht unbedingt eine Totalüberwachung erforderlich. Sobald zum Beispiel in eine Smartphone-App zur Steuerung und Kontrolle von Arbeitstätigkeiten die Beginn- und Endzeitpunkte von Besuchen bei KundInnen eingegeben werden – und für Abrechnungszwecke vielleicht auch noch Informationen über die Art der durchgeführten Tätigkeiten – kann die Arbeitsleistung bewertet werden. Außerdem stehen damit auch ohne permanentes GPS-Tracking Informationen über den aktuellen Standort der Beschäftigten zur Verfügung.

Arbeit kann mit Hilfe einer Smartphone-App nicht nur vermessen, sondern auch digital strukturiert werden. Stehen etwa nur bestimmte Auswahlmöglichkeiten für die Art der Tätigkeiten zur Verfügung, die eingegeben werden können, müssen alle durchgeführten Tätigkeiten in dieses Raster passen. Sobald Tätigkeiten vorgegeben oder empfohlen werden, wird eine App schnell zum mobilen Chef. Ähnliches gilt für Systeme zur Organisation von Abläufen und Arbeitsaufgaben im Büro. Auch eine relativ wenig invasive Datenerfassung – die vielleicht sogar sehr transparent erfolgt – kann auf diese Weise massive Auswirkungen auf den Arbeitsalltag von Beschäftigten haben. Dies gilt natürlich umso mehr für die betriebliche Nutzung von versteckt erfassten Verhaltensdaten.

Herausforderungen für die Mitbestimmung. Im globalen Vergleich haben Beschäftigte und Betriebsrat in Österreich und Deutschland relativ gute Mittel, beim Einsatz datenverarbeitender Systeme im Betrieb mitzureden und extreme Formen von Überwachung und Kontrolle zu verhindern. Zentraler Hebel für die Mitbestimmung ist neben dem Datenschutzrecht in Form der DSGVO vor allem das Arbeitsrecht – in Deutschland das Betriebsverfassungsgesetz (vgl. Däubler 2017, S. 75), in Österreich das Arbeitsverfassungsgesetz (vgl. Haslinger et al 2020, S. 131). Die Beschäftigten und – wenn hoffentlich vorhanden, der Betriebsrat – haben vielfältige Informations- und Kontrollrechte in Bezug auf die eingesetzten Systeme (vgl. Haslinger et al 2020, S. 138; Däubler 2017, S. 429ff). Bei

Technologien, die Verhalten und Leistung von ArbeitnehmerInnen überwachen und kontrollieren, regeln sogenannte Betriebsvereinbarungen zwischen Betriebsrat und Geschäftsführung, wie dabei personenbezogene Daten verarbeitet werden dürfen (vgl. Haslinger et al 2020, S. 155; Däubler 2017, S. 460ff). Wichtige Grundlage im Datenschutzrecht ist außerdem die Zweckbindung. Bei jeder Verarbeitung personenbezogener Daten muss ausdrücklich ein bestimmter Zweck benannt werden, der später nicht einfach geändert werden kann (vgl. Haslinger et al 2020; S. 160). An dieser Stelle kann keine erschöpfende Darstellung des bestehenden gesetzlichen Rahmens erfolgen. Diese Studie dokumentiert Datenpraktiken und Funktionen verfügbarer Systeme und Technologien und klammert Fragen der datenschutz- und arbeitsrechtlichen Zulässigkeit weitgehend aus. Dennoch zeigen Literatur und viele Gespräche des Verfassers mit BetriebsrätInnen und gewerkschaftlichen Beratungsorganen, dass die betriebliche Mitbestimmung vor großen Herausforderungen steht.

Komplexe und intransparente Systeme. Für eine im Mai 2021 veröffentlichte Studie über die „Verarbeitung personenbezogener Beschäftigtendaten und Grenzen betrieblicher Mitbestimmung in einer digitalisierten Arbeitswelt“ wurden fast 700 Personen aus Betriebsrat und Personalvertretung in österreichischen Unternehmen befragt (vgl. Riesenecker-Caba und Astleithner 2021). Dabei zeigte sich, dass zwar altbekannte Bereiche wie Videoüberwachung, Zeiterfassung, Zutrittskontrolle oder die Nutzung von Telefon, Internet und E-Mail bei immerhin 50-70% der Befragten mit einer Betriebsvereinbarung geregelt sind, diese Zahl aber rapide abnimmt, je komplexer die eingesetzte Technologie wird. Obwohl im Einsatz, ist das mächtige ERP-System SAP zum Beispiel bei nur 42% der Befragten mit einer Betriebsvereinbarung geregelt, konzernweite Personaldatenbanken bei nur 41%, Software zur Tätigkeitserfassung bei 33%, Systeme zur Zusammenführung und Analyse von Daten bei 30% und Microsoft 365 bei nur 23% der Befragten. Knapp die Hälfte der Befragten sieht die Komplexität der Systeme als Hindernis für deren Regelung. Bei nur 20% der Befragten informiert das Unternehmen den Betriebsrat aus eigener Initiative über die Verarbeitung personenbezogener Daten. Damit kommen offenbar viele Betriebe ihren Informationspflichten nicht nach. Ohne Betriebsvereinbarung oder gar ohne Informationen über die genutzten Systeme gleicht der Einsatz derartiger Technologien aus Beschäftigtensicht einem Blindflug – Mitbestimmung ist nicht vorhanden.

Systematische Zweckentfremdung? Der deutsche Datenschutz- und Arbeitsrechtler Wolfgang Däubler (2007, S. 267ff) weist zudem darauf hin, dass Betriebe exzessive Datenverarbeitung zunehmend mit dem Argument rechtfertigen, dass es dabei nur um eine „bessere und rationellere Arbeitsorganisation, nicht aber um die Kontrolle der Leistung“ von ArbeitnehmerInnen gehe. Der Zweck einer rationelleren Arbeitsorganisation sei aber unscharf und die Gefahr der Zweckentfremdung darum groß. Eine „Totalerfassung“ des Verhaltens sei zwar rechtlich ausgeschlossen. Eine Erhebung von „Kontrolldaten“ über die „Quantität und Qualität der vom einzelnen Arbeitnehmer erbrachten Leistung“ könne aber außerdem „im Hinblick auf die Funktionsfähigkeit des Unternehmens“ durchaus legitim sein (ebd., S. 268). Grundsätzlich kann ein „überwiegendes Unternehmerinteresse“ im Rahmen einer Abwägung bestimmte Eingriffe in die Rechte und Freiheiten der Beschäftigten legitimieren (ebd., S. 269). Betriebe erfassen in der Praxis zum Beispiel oft detaillierte Daten über durchgeführte Tätigkeiten zum Zweck der Abrechnung gegenüber ihren KundInnen.

Eine verwandte Problematik besteht darin, dass technische Systeme globaler Anbieter heute meist sehr umfangreiche Funktionen bieten, die personenbezogene Daten für unterschiedliche Zwecke verarbeiten und diese zusammenführen – wie viele Beispiele in dieser Studie zeigen. Darunter sind auch Funktionen, die nur schwer mit den rechtlichen Rahmenbedingungen in Deutschland oder Österreich vereinbar sind, aber potenziell mit einem Klick aktiviert werden können. Dies trifft insbesondere für cloudbasierte Dienste zu, deren Datenverarbeitungspraktiken manchmal

nicht einmal mehr für die betriebseigene IT-Abteilung nachvollziehbar sind. Peter Wedde (2017) befürchtet diesbezüglich gar ein „Ende der Mitbestimmung".

Daten über Gruppen. Die beschriebenen Herausforderungen für die Mitbestimmung weisen auf Grenzen der aktuellen datenschutz- und arbeitsrechtlichen Regelungen und deren praktische Umsetzung hin. Beim Datenschutzrecht kommt neben der mangelhaften bis inexistenten Durchsetzung der DSGVO gegen globale Konzerne[2] dazu, dass es stark auf individuelle Rechte und Daten über Einzelne ausgerichtet ist. Die Auswirkungen von Datenverarbeitung auf Gruppen oder Gesamtgesellschaft kommt dabei manchmal zu kurz (vgl. Taylor 2017). Im Betrieb können auch Auswertungen, die nur Informationen über Teams, Abteilungen, Firmenstandorte oder den gesamten Konzern zeigen und keinerlei Daten über Einzelpersonen enthalten, Druck auf Beschäftigte ausüben. Derartige Auswirkungen sind zwar zum Teil datenschutz- und arbeitsrechtlich abgedeckt, wenn etwa eine digitale Bewertung auf Gruppenebene auf einzelne Mitglieder der Gruppe „durchschlägt" (vgl. Däubler 2017, S. 484f). Dennoch können sich Auswertungen auf Grundlage umfassender personenbezogener Beschäftigtendaten auf viele andere Arten auf die Machtverhältnisse zwischen Betrieb und Beschäftigten auswirken, auch wenn die Ergebnisse keinerlei Personenbezug mehr aufweisen. Betriebliche **„Datenmacht"** im Sinne von Wissen über betriebliche Abläufe und Arbeitstätigkeiten kann auch abseits individueller Auswertungen zu einer kompletten Umstrukturierung von Tätigkeiten und des gesamten Arbeitsalltags führen (vgl. Schörpf et al 2020, S. 16ff). Sie kann die Verlagerung oder Auslagerung von Tätigkeiten an Drittfirmen erleichtern (ebd., S. 9), ArbeitnehmerInnen ersetzbarer machen (vgl. Kellogg et al 2020) oder gar zur Senkung von Löhnen beitragen (vgl. Newman 2016).

Betriebliche Kontrolle im Zeitalter der „Datafizierung". Diese Studie kann weder eine systematische Einschätzung der Auswirkungen auf Beschäftigte noch eine Einschätzung der gesetzlichen Rahmenbedingungen oder Empfehlungen für deren Verbesserung leisten. Dennoch definieren die beschriebenen Problematiken den Blickwinkel, aus dem heraus auf den folgenden Seiten konkrete Datenpraktiken und technische Systeme aus Beschäftigtensicht analysiert und dokumentiert werden. Der Literaturüberblick in Kapitel 4 führt eine Auswahl an Publikationen an, die Grundlage für die Entwicklung der Landkarte betrieblicher Datenpraktiken sowie der Fallstudien waren. In der akademischen Forschung gibt es bislang wenig Literatur zur Frage, wie die Ausweitung der Datenerfassung betriebliche Steuerung und Kontrolle verändert. Relevante Beiträge dazu stammen von Katherine Kellogg et al (2020) sowie von einer Gruppe an der Universität St. Gallen in der Schweiz, die an einer Systematik arbeitet, die die Auswirkungen von „Datafizierung" auf betriebliche Kontrolle untersucht. Simon Schafheitle et al (2020) halten fest, dass diese Entwicklungen noch nicht ausreichend verstanden wurden. Eine kohärente Klassifikation datenbasierter Kontrolle fehle bis jetzt. Die vorliegende Bestandsaufnahme betrieblicher Datenpraktiken samt vieler Beispiele hat das Ziel, hier einen Beitrag zu leisten, kann aber nur der Startpunkt für weitere Forschung sein.

Wessen Digitalisierung? Informationstechnologie, Datenverarbeitung und Digitalisierung im Betrieb können viele positive Effekte haben. Die in dieser Studie dokumentierten Praktiken werfen aber viele Fragen auf. Wie sieht diese Digitalisierung im Betrieb eigentlich aus? Wer bestimmt, wie sie aussieht? Und wer profitiert? Unternehmen gestalten Digitalisierung und Datenverarbeitung prinzipiell im Sinne ihrer ökonomischen Interessen. Um dieser einseitigen Gestaltungsmacht etwas entgegenzusetzen und Mitbestimmung zu gewährleisten, brauchen Beschäftigte und BetriebsrätInnen Wissen, Schulung und Unterstützung. Diese Studie möchte einen Beitrag dazu leisten.

[2] Vgl. z.B. Murgia, Madhumita und Espinoza, Javier (2021): Ireland fails to enforce EU law against Big Tech. Financial Times, 13.9.2021. Online: https://www.ft.com/content/5b986586-0f85-47d5-8edb-3b49398e2b08

3. Hintergrund, Fragestellungen, Reichweite und Methodik

Diese Studie ist das Hauptergebnis von mehr als einem Jahr intensiver Arbeit am Projekt „Gläserne Belegschaft. Überwachung und Kontrolle am Arbeitsplatz 4.0“, das von Ende 2019 an in Kooperation mit den zwei großen österreichischen Gewerkschaften GPA und PRO-GE durchgeführt und vom Digitalisierungsfonds Arbeit 4.0 der Arbeiterkammer Wien[3] unterstützt wurde. Ziel des Projekts war die Untersuchung, Zusammenfassung und Aufbereitung aktueller betrieblicher Datenpraktiken und die Kartographierung relevanter Technologien, Systeme, Trends und Auswirkungen auf Beschäftigte. Neben der Untersuchung wurden Materialien für Schulung und Beratung entwickelt sowie Seminare für BetriebsrätInnen durchgeführt.

Neben der vorliegenden Studie wurde im Rahmen des Projekts von Hans Christian Voigt eine kleinere auf Interviews mit BetriebsrätInnen basierende explorative Untersuchung[4] über den Einsatz von Überwachungs- und Kontrollsystemen in österreichischen Unternehmen und dem Umgang der Belegschaften damit durchgeführt. Die Ergebnisse sind in Kapitel 8 zusammengefasst. Hans Christian Voigt hat auch für die Konzeption und Umsetzung des Gesamtprojekts und der vorliegenden Studie wichtige Unterstützung geleistet. Das gesamte Projekt wurde in engem Austausch mit maßgeblichen ExpertInnen auf Seiten der ArbeitnehmerInnenvertretung durchgeführt. Unter anderem haben Clara Fritsch und Eva Angerler von der GPA-Grundlagenabteilung Arbeit & Technik[5], Susanne Haslinger von der Gewerkschaft PRO-GE und Thomas Riesenecker-Caba von der Forschungs- und Beratungsstelle Arbeitswelt (FORBA)[6] wichtige Beiträge geleistet. Die Illustrationen und Infografiken wurden gemeinsam mit Pascale Osterwalder[7] entwickelt und von ihr umgesetzt.

Fragestellungen. Ausgangspunkt der Untersuchung waren folgende Hauptfragestellungen:

- Wie werden personenbezogene Daten über Beschäftigte in Betrieben erfasst, verknüpft, ausgewertet und eingesetzt? Welche Arten datenverarbeitender Systeme sind relevant und welche Funktionen bietet die am Markt erhältliche Software? Welche stehen vor der Einführung und welche könnten in einigen Jahren auch in Österreich und Deutschland relevant werden? Welche Technologien sind in welchen Branchen und Tätigkeitsbereichen relevant – vom niedrig qualifizierten Bereich bis zur Wissensarbeit?
- Welche Rolle spielen Verhaltensdaten, Logdaten, Standortdaten und Sensordaten? Welche Rolle spielt die Zusammenführung von Daten in cloudbasierten Systemen? Welche Arten der Analyse sind verfügbar?
- Welche Datenpraktiken bergen besonders hohe Risiken für ArbeitnehmerInnen, von der Aussonderung abweichenden Verhaltens bis zur Leistungskontrolle? Wie können datenverarbeitende Systeme genutzt werden, um Arbeit digital zu strukturieren und sie nicht nur überwachen und zu kontrollieren, sondern auch teil- oder vollautomatisiert zu steuern? Wie verändert das die Machtverhältnisse zwischen Betrieben und Beschäftigten? Welche Rolle spielen dabei gruppenspezifische Daten?
- Wo führt Datenerfassung für bestimmte betriebliche Zwecke potenziell zur Verarbeitung oder Auswertung für andere Zwecke?

[3] https://wien.arbeiterkammer.at/service/digifonds/Ueber_den_Digifonds.html
[4] Voigt, Hans Christian (2021): Digitale Überwachung und Kontrolle in österreichischen Betrieben. Bericht über eine explorative Untersuchung mit Fallbeispielen auf Basis von Interviews. Eine Studie von Cracked Labs, Wien, September 2021. Online: https://crackedlabs.org/dl/Cracked-Labs_Voigt_UeberwachungArbeitsplatzAT.pdf
[5] https://arbeitundtechnik.gpa.at/
[6] https://www.forba.at/
[7] https://www.elaxa.ch/cv/

Aufbau der Studie. Diese Fragestellungen werden in vier Hauptkapiteln behandelt:

- Kapitel 5 arbeitet auf und dokumentiert, welche Arten personenbezogener Daten über Beschäftigte in Betrieben verarbeitet werden und welche Arten technischer Systeme dafür eingesetzt werden. Resultat ist eine Landkarte betrieblicher Datenpraktiken samt Infografik.
- Kapitel 6 präsentiert neun Fallstudien über am Markt verfügbare Systeme konkreter Hersteller für unterschiedliche Aufgabenbereiche und Branchen und dokumentiert, in welcher Form die untersuchten Produkte Daten über Beschäftigte verarbeiten und wie sie eingesetzt werden können. Der Abschnitt über digitale Personalverwaltungssysteme in Kapitel 5 könnte als weitere, zehnte Fallstudie betrachtet werden.
- Kapitel 7 präsentiert zwei weitere Fallstudien über den konkreten Einsatz datenverarbeitender Systeme in zwei konkreten Unternehmen auf Basis existierender Literatur und öffentlich zugänglicher Quellen.
- Kapitel 8 fasst fünf Fallstudien über den konkreten Einsatz datenverarbeitender Systeme in österreichischen Betrieben unterschiedlicher Branchen auf Basis von Interviews mit Betriebsräten zusammen (siehe oben).

Einleitend gibt Kapitel 4 einen Überblick über die im Rahmen der Studie durchgeführte Literaturrecherche, die Grundlage für die weitere Untersuchung betrieblicher Datenpraktiken und Fallstudien war.

Methodik. Die Studie basiert auf mehreren Jahren Forschung zum Thema. Nach Projektstart wurde eine ausführliche und systematische Literaturrecherche durchgeführt. Neben Literatur über klassischen Beschäftigtendatenschutz aus Rechtswissenschaft und gewerkschaftlicher Beratungs- und Forschungspraxis aus dem deutschsprachigen Raum wurden relevante Publikationen zur Überwachung von Beschäftigten, zur Datafizierung im Betrieb und zu algorithmischem Management aus Europa und aus den USA einbezogen. Ausgewertet wurden neben akademischer Forschung aus Rechtswissenschaft, Informatik, Datensicherheit, Betriebswirtschaft, Soziologie und Surveillance Studies auch Berichte von Ministerien, Regulierungsbehörden, internationalen Organisationen, Nichtregierungsorganisationen und Marktforschungsfirmen. Auch die Archive von Zeitungen, Magazinen, Online-Medien und Blogs wurden systematisch durchsucht. Im Zuge der Literaturrecherche wurden die Quellen beschlagwortet. Auf diese Weise entstand Schritt für Schritt eine nunmehr aus etwa 300 Schlagworten bestehende Taxonomie betrieblicher Datenpraktiken, Systeme und Auswirkungen auf Beschäftigte. Diese Taxonomie wurde in Folge zur Strukturierung der Landkarte betrieblicher Datenpraktiken sowie zur Auswahl und Durchführung der Fallstudien genutzt. Die Taxonomie ist aktuell noch nicht veröffentlichungsfähig. Eine Weiterentwicklung und Veröffentlichung kann je nach Ressourcenlage hoffentlich zu einem späteren Zeitpunkt erfolgen.

Für die Analyse der konkreten datenverarbeitenden Produkte und Systeme wurden darüber hinaus öffentlich verfügbare Quellen wie Websites von Unternehmen, Marketingmaterialien, Broschüren, Videos, Schulungsmaterialien und technische Dokumentationen ausgewertet. Der Umfang verfügbarer Dokumentation über die Funktionen von am Markt angebotene Produkte ist sehr unterschiedlich. In manchen Fällen sind nur sehr oberflächliche Marketing-Aussagen verfügbar, in anderen Fällen tausende Seiten an technischer Dokumentation samt detaillierter Angaben über Datenbanktabellen und API-Schnittstellen. Vereinzelt wurden auch historische Versionen von Websites sowie unternehmensinterne Dokumente einbezogen, die aus verschiedenen Gründen an die Öffentlichkeit gelangt sind.

Reichweite und Einschränkungen. Diese Studie dokumentiert konkrete Praktiken betrieblicher Datenverarbeitung im Lichte ihrer Auswirkungen auf Beschäftigte und versucht, einen Überblick zu geben. Die Ergebnisse unterliegen folgenden Einschränkungen:

- Die Verarbeitung personenbezogener Daten über BewerberInnen im Zuge von Neueinstellungen ist nicht Gegenstand dieser Studie.
- Auch wenn neue Technologien der digitalen Kontrolle insbesondere in der Plattformarbeit am weitesten fortgeschritten sind, wird diese nur rudimentär einbezogen.
- Einschätzungen über die datenschutz- und arbeitsrechtlichen Zulässigkeit der dokumentierten Praktiken sind weitgehend ausgeklammert. Auch Fragen politischer und rechtlicher Handlungsoptionen für die ArbeitnehmerInnenvertretung sowie konkrete Handlungsoptionen für betroffene Beschäftigte und Betriebsräte sind jenseits des Rahmens dieser Studie.
- Trotz systematischer Einbeziehung vielfältiger Quellen von technischen Dokumentationen bis zu traditioneller Literatur zu betrieblichem Datenschutz im deutschsprachigen Raum und Rückkopplung mit gewerkschaftlicher Beratungspraxis sind die dokumentierten Praktiken nur eingeschränkt generalisierbar. Weitere quantitative und qualitative Forschung könnte die Generalisierbarkeit verbessern.
- Trotz des Versuchs, einen Überblick über die betriebliche Verarbeitung personenbezogener Daten über ArbeitnehmerInnen zu geben, kann die vorliegende „Landkarte“ maximal den Startpunkt für eine weitere Systematisierung betrieblicher Datenpraktiken und ihrer Auswirkungen auf Beschäftigte bilden.

Aus diesen Einschränkungen ergibt sich der Bedarf für weitere Arbeit zum Thema. Um ArbeitnehmerInnen und ihre Vertretungen angesichts der Ausweitung betrieblicher Datenverarbeitung zu ermächtigen und politische Handlungsempfehlungen abzuleiten, ist eine weitergehende Systematisierung und Klassifizierung betrieblicher Datenpraktiken im Lichte ihrer Auswirkungen auf Beschäftigte notwendig. Eine fundierte Einschätzung der rechtlichen Zulässigkeit der dokumentierten Praktiken sowie weitere qualitative und quantitative Untersuchungen über den konkreten Einsatz in Unternehmen sind Voraussetzung für die Identifikation regulatorischen Handlungsbedarfs.

4. Literaturüberblick

Im Rahmen der Studie wurde eine ausführliche Literaturrecherche durchgeführt. Dieser Abschnitt gibt einen Überblick über wichtige Publikationen, die Grundlage für die Entwicklung der Landkarte betrieblicher Datenpraktiken sowie der Fallstudien waren.

4.1 Dt. Sprachraum: Datenschutz, Arbeitsrecht und Digitalisierung

Literatur über Systeme digitaler Überwachung und Kontrolle im Betrieb im deutschsprachigen Raum hat oft die Perspektive von Beschäftigtendatenschutz und Arbeitsrecht als Ausgangsbasis. Neben der Rechtswissenschaft spielt hier die gewerkschaftliche Beratungs- und Forschungspraxis eine zentrale Rolle.

Wolfgang Däubler's „Gläserne Belegschaften. Das Handbuch zum Beschäftigtendatenschutz" gilt in Deutschland als Standardwerk, ist inzwischen in 9. Auflage erschienen[8] und gibt auf fast 800 Seiten nicht nur detailliert Auskunft über rechtliche Fragen, sondern versammelt auch eine Vielzahl an Beispielen betrieblicher Datenpraktiken (Däubler 2017). Peter Wedde (2017) gibt in seinem Artikel „Beschäftigtendatenschutz in der digitalisierten Welt" einen kompakten Überblick über aktuelle Entwicklungen, betriebliche Praktiken und Herausforderungen. Auch der von Rüdiger Krause verfasste Forschungsbericht des deutschen Bundesministeriums für Arbeit und Soziales zu „Digitalisierung und Beschäftigtendatenschutz" fasst „neuere technische Entwicklungen mit Kontrollpotenzial" zusammen (Krause 2017). Die studentische Arbeit „Überwachung von Arbeitnehmern im Betrieb. Eine Technikfolgenabschätzung digitalisierter Informations- und Kommunikationssysteme" von Timo Frühbrodt (2018) bietet ebenfalls einen guten Überblick.

In Österreich kann das nun in zweiter Auflage im gewerkschaftlichen ÖGB Verlag erschienene Buch „Beschäftigtendatenschutz. Handbuch für die betriebliche Praxis" – herausgegeben von Susanne Haslinger, Andreas Krisch und Thomas-Riesenecker-Caba – als Standardwerk bezeichnet werden. Es versammelt Beiträge mehrere AutorInnen – darunter ein Überblick über datenverarbeitende Systeme im Betrieb (Haslinger et al 2020, S. 36ff). Die Wiener Forschungs- und Beratungsstelle Arbeitswelt (FORBA) hat 2011 die „Verwendung personenbezogener Daten" im Betrieb untersucht und dabei die Arten der eingesetzten Systeme abgefragt – mit Rückmeldungen von 1.200 Beschäftigten und BetriebsrätInnen (Riesenecker-Caba und Bauernfeind 2011). Eine Folgestudie wurde im Mai 2021 veröffentlicht und zeigt, wie sich der Einsatz datenverarbeitender Systeme in österreichischen Betrieben seit 2011 verändert hat (Riesenecker-Caba und Astleithner 2021).

Außerdem hat FORBA aus einem etwas breiteren Blickwinkel in zwei Studien „Entwicklungstrends digitaler Arbeit" untersucht. Die erste Publikation fasst auf Basis von Interviews mit ExpertInnen Schlüsselentwicklungen der letzten Jahre zusammen – von mobile Arbeit und der zunehmenden Vernetzung von IT-Systemen über die Digitalisierung von betrieblicher Kommunikation und Kooperation bis zur Automatisierung komplexer Arbeitsabläufe (Schörpf et al 2018). Die zweite Studie untersucht auf Basis von Interviews mit Beschäftigten, BetriebsrätInnen und Führungskräften aus vier Betrieben mit einem Fokus auf konkrete technische Systeme wie SAP oder Jira, wie Prozessautomatisierung, Leistungskontrolle, digitale Kommunikation sowie Informations- und Wissensmanagement umgesetzt und gestaltet werden (Schörpf et al 2020). Hannah Mormann beleuchtet in ihrem Buch „Das Projekt

[8] https://shop.bund-verlag.de/glaeserne-belegschaften-978-3-7663-7071-6

SAP. Zur Organisationssoziologie betriebswirtschaftlicher Standardsoftware“, wie ein System wie SAP betriebliche Abläufe und damit den Organisationsalltag mitgestaltet (Mormann 2016).

Herausragende Publikationen für **Teilbereiche betrieblicher Datenerfassung** wurden von der gewerkschaftlichen Hans-Böckler-Stiftung veröffentlicht – etwa ein Artikel zur „Vermessung der Belegschaft“ über die Analyse betrieblicher sozialer Netzwerke (Höller und Wedde 2018) oder eine Studie über ein umfassendes Bewertungssystem beim deutschen Online-Handelsriesen Zalando (Staab und Geschke 2020). Eberhard Kiesche und Matthias Wilke (2012) haben „Neue Überwachungsformen in Call-Centern“ beleuchtet, Sandra Stern et al (2010) Erfahrungsberichte über die Arbeit in österreichischen Callcentern gesammelt. Auch die gut recherchierten und belegten Broschüren der Abteilung „Arbeit & Technik“ der österreichischen Gewerkschaft GPA sind wertvolle Ressourcen – etwa zu Überwachung im Außendienst (GPA-djp 2012), Kennzahlen und Quantifizierung (Fritsch 2012), Zielvereinbarungen und Leistungssteuerung (Angerler et al 2018), digitaler Personalentwicklung (Fritsch 2017), Mitgestaltung von Digitalisierung im Betrieb (Angerler et al 2018) und zu Microsoft 365 (Fritsch 2021). Katrin Sommer hat über Personalverwaltungssysteme wie SAP SuccessFactors und Workday geschrieben (Sommer 2014, Somme 2017). Im Rahmen des Forschungsprojekts „Automatisiertes Personalmanagement und Mitbestimmung“ der deutschen Nonprofit-Organisation AlgorithmWatch sind Publikationen zu ethischen Aspekten datengesteuerter Systeme im Personalmanagement (Michele 2021) und zu arbeitsrechtlichen und –datenschutzrechtlichen bei der Automatisierung im Personalmanagement (Wedde 2020) entstanden. Die von Volkswagen herausgegebene Buchpublikation der Dissertation von Christian Jaksch (2019) über „datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes“ bietet Einblicke in datenschutzrelevante Aspekte von Technologien wie digitale Assistenten, Cloud Computing und „People Analytics“ – also die fortgeschrittene Analyse und Auswertung von Beschäftigtendaten.

Auch wenn **Plattformarbeit** nicht im Fokus der vorliegenden Studie steht, sei auf die von der Hans-Böckler-Stiftung veröffentlichte Untersuchung von Ivanova et al (2018) über Kontrolle und Autonomie bei App-basiertem Management anhand von Plattformen zur Essensauslieferung sowie auf die ÖGB-Verlag erschienene Publikation zu „Arbeit in der Gig-Economy“ hingewiesen (Risak und Lutz 2017).

4.2 International: Überwachung, Datafizierung, algorithmische Kontrolle

Wichtige Grundlage für die vorliegende Studie war die am „Data Justice Lab“ an der Universität Cardiff (UK) entstandene Publikation „The datafication of the workplace“ von Javier Sánchez-Monedero and Lina Dencik (2019). Entstanden im Rahmen eines EU-Projekts über Datafizierung und soziale Gerechtigkeit geht der Bericht über den Blickwinkel des klassischen Datenschutzes hinaus und gibt einen Überblick über neue betriebliche Datenpraktiken und deren Auswirkungen auf die Arbeitswelt in Europa – von traditioneller Überwachung über digitale Leistungskontrolle bis zum algorithmischen Management. Der Bericht enthält viele Beispiele über technische Systeme, einige davon wurden für die Fallbeispiele in der vorliegenden Studie aufgegriffen.

Die Publikationen des „Data & Society“ Institut in New York bewegen sich naturgemäß weit abseits der Perspektive europäischen Beschäftigtendatenschutzes. Die Publikationen zu „Workplace Monitoring & Surveillance“ und „Algorithmic Management in the Workplace“ von Alexandra Mateescu und Aiha Nguyen (2019, 2019b) bieten einen guten Überblick über aktuelle betriebliche Datenpraktiken in den USA und stellen die Frage, wie diese das Machtungleichgewicht zwischen ArbeitnehmerInnen und Unternehmen verändern. Auch der Bericht „The Datafication of Employment“ von Sam Adler-Bell und Michelle Miller (2018) sowie der Artikel „How hard will the robots make us work?“ von Josh Dzieza (2020) beinhalten viele Beispiele über betriebliche Datenpraktiken in den USA.

Zu international vielzitierten akademischen Überblicksartikeln zur **Überwachung von Beschäftigten** zählen „Workplace Surveillance: An Overview“ der Überwachungsforscherin Kirstie Ball (2010) und „Limitless worker surveillance“ von Ifeoma Ajunwa, Kate Crawford und Jason Schultz (2017). Edwards et al (2018) entwickeln im Artikel “Employee Surveillance: The Road to Surveillance is Paved with Good Intentions” ein fünfstufiges Modell, das Überwachungspraktiken am Arbeitsplatz beschreibt. Nils Leopold und Martin Meints (2008) haben sich mit Profiling von Beschäftigten in Europa beschäftigt. Neben Personalverwaltung und der Überwachung von E-Mail und Internet steht in ihrem Artikel Betrugserkennung auf Basis von Kassendaten im Einzelhandel im Fokus. Ein Bericht der US-Bürgerrechtsorganisation EFF gibt einen Überblick über besonders invasive Überwachungssoftware, die Web- und App-Nutzungsverhalten, Tastaturdaten oder gar die Laptop-Kamera auswertet (Cyphers und Gullojune 2020).

Einen viel breiteren Blickwinkel nimmt die Studie „Algorithms at Work: The New Contested Terrain of Control“ von Kellogg et al (2020) ein. Die Autorinnen, die am MIT und in Stanford und damit an den Leitinstitutionen der US-Technologieindustrie lehren, entwickeln darin eine Systematik aus sechs Mechanismen, die beschreiben, wie Datafizierung und Algorithmen **betriebliche Steuerung und Kontrolle** verändern. Mittels vieler Beispiele werden die Unterschiede zu traditioneller technischer und bürokratischer Kontrolle herausgearbeitet. Die Studie fasst Algorithmen am Arbeitsplatz in Anlehnung an die Arbeitsprozesstheorie als umkämpftes Feld und beschreibt Auswirkungen auf Beschäftigte und deren Widerstandsstrategien. Die in dieser Arbeit entwickelte Systematik ist eine wichtige theoretische Grundlage für die vorliegende Studie und für mögliche weiterführende Forschung. Auch eine Gruppe an der Universität St. Gallen in der Schweiz hat unter dem Titel “No Stone Left Unturned? Toward a Framework for the Impact of Datafication Technologies on Organizational Control” auf empirischer Basis eine erste Version einer Systematik entwickelt, die die Auswirkungen von Datafizierung auf betriebliche Kontrolle entlang von 11 Gestaltungsdimensionen untersucht (Schafheitle et al 2020).

Für **Teilbereiche betrieblicher Datenpraktiken** seien einige herausragende internationale Arbeiten angeführt – zum Teil aus US-Perspektive, methodisch oft auf Basis ethnografischer Feldforschung. Madison Van Oort befasst sich mit Datenpraktiken im Einzelhandel und deren Auswirkungen auf Beschäftigte – von Systemen zur Schichtplanung bis zur Auswertung von Kassendaten – etwa im Buchkapitel „Employing the Carceral Imaginary: An Ethnography of Worker Surveillance in the Retail Industry” und im Artikel „The Emotional Labor of Surveillance: Digital Control in Fast Fashion Retail“ (Van Oort 2019, Van Oort 2019b). Auch Alex Wood hat sich in seinem Buch „Despotism on Demand. How Power Operates in the Flexible Workplace“ mit der Rolle von Schichtplanung im Handel beschäftigt und dafür den Begriff des „flexiblen Despotismus“ geprägt (Wood 2020).

Karen Levy hat im Artikel „The Contexts of Control: Information, Power, and Truck-Driving Work” digitale Kontrolle in der LKW-Logistik untersucht – von Standort- und Leistungsüberwachung bis zum Flottenmanagement (Levy 2015). Gemeinsam mit Solon Barocas hat sich Levy damit befasst, wie die Erfassung von Daten über *eine* Gruppe von Menschen digitale Kontrolle über eine *andere* Gruppe verstärken kann – wenn etwa Daten über KundInnen dazu genutzt werden, Beschäftigte zu überwachen. In ihrem Artikel „Privacy at the Margins. Refractive Surveillance: Monitoring Customers to Manage Workers” haben sie dafür den Begriff “refraktiven Überwachung” geprägt (Barocas und Levy 2018). Jacob Metcalf (2018) hat dieses Konzept auf den Bereich mobile Pflege in den USA übertragen.

Kristiansen et al (2018) haben im Artikel „Accountability in the Blue-Collar Data-Driven Workplace” die Auswirkungen mobiler Technologie auf ElektrikerInnen erforscht – insbesondere in Hinblick auf die Verarbeitung von Zeit- und Standortdaten. Die britische Forscherin Phoebe V. Moore beschäftigt sich seit Jahren mit Datenerfassung

und Quantifizierung in prekäre Arbeitswelten, mit digitalem Taylorismus in Plattformarbeit, Fabrik und Büro sowie mit affektiver Arbeit und der Rolle von „Selbststeuerung" – etwa in ihrem Buch „The Quantified Self in Precarity: Work, Technology and What Counts" (Moore 2018). Der von ihr mit herausgegebene Band „Humans and Machines at Work" versammelt Artikel unterschiedlicher AutorInnen zu Digitalisierung, Automatisierung und Kontrolle am Arbeitsplatz in Bereichen wie Journalismus, Pflege, Callcenterarbeit oder Personentransport (Moore et al 2018b).

Plattformarbeit steht nicht im Zentrum der vorliegenden Studie. Nichtsdestotrotz sei an dieser Stelle auf die Arbeit von Alex Rosenblat hingewiesen, die Informations- und Machtungleichgewichte zwischen der Taxivermittlungsplattform Uber und deren FahrerInnen erforscht hat. Rosenblat war lange eine der bekanntesten Uber-KritikerInnen und ist seit 2021 überraschenderweise bei Uber für „Fairness" zuständig.[9] Das schmälert aber nicht ihre herausragenden Beiträge zu umfassender digitaler Überwachung, Steuerung und Kontrolle von Arbeit mittels App. Neben ihrem Buch „Uberland: How Algorithms Are Rewriting the Rules of Work" (Rosenblat 2019) sei etwa die Studie "Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers" erwähnt. Auch Jeremias Prassl hat sich in seinem Buch "Humans as a Service: The Promise and Perils of Work in the Gig Economy" ausführlich mit digitaler Kontrolle in Plattformökonomien befasst – unter Berücksichtigung von Perspektiven europäischen Arbeitsrechts (Prassl 2018).

Weitere Literatur. Valerio De Stefano hat zu Plattformarbeit geforscht und darüber hinaus zu Algorithmen, Automatisierung und künstlicher Intelligenz im Verhältnis zu europäischem Arbeitsrecht publiziert (z.B. De Stefano 2019, De Stefano 2020). Zur Frage, vor wessen Automatisierung ArbeitnehmerInnen mehr zu befürchten haben – vor ihrer eigenen oder vor der ihrer Vorgesetzten – hat David Banks (2020) im Artikel „Automatic for the Bosses" geschrieben. Nathan Newman untersucht im Artikel „UnMarginalizing Workers" aus einer US-Perspektive, wie algorithmische Überwachung und Kontrolle abseits der möglichen individuellen Folgen für Beschäftigte kollektiv dazu beitragen können, systematisch Löhne zu senken (Newman 2016).

Zur Frage, wie Gestaltung und Logiken von Software für „Supply Chain Management" (SCM) – etwa von SAP – globale Lieferketten und am Ende den Alltag von Beschäftigten überall in der Welt prägen, hat Miriam Posner (2019) in ihrem Artikel „The Software That Shapes Workers' Lives" geschrieben. Auch Ned Rossiter behandelt in seinem Buch „Software, Infrastructure, Labor" die gesellschaftliche Rolle von Software für SCM oder Enterprise Resource Planning (ERP) und adressiert dabei immer konkrete Funktionen dieser Systeme (Rossiter 2016).

[9] Ford, Brody (2021): Uber Hires Prominent Critic to Focus on Treatment of Drivers. Bloomberg, 17.2.2021. Online: https://www.bloomberg.com/news/articles/2021-02-17/uber-hires-prominent-critic-to-focus-on-treatment-of-drivers

5. Personenbezogene Daten und Systeme im Betrieb

Dieses Kapitel gibt einen systematischen Überblick über datenverarbeitende technische Systeme in der Arbeitswelt.

5.1 Landkarte betrieblicher Datenpraktiken und Systeme

Folgende Infografik fasst zusammen, welche Arten personenbezogener Daten über Beschäftigte in Betrieben verarbeitet und welche Arten technischer Systeme dafür eingesetzt werden:

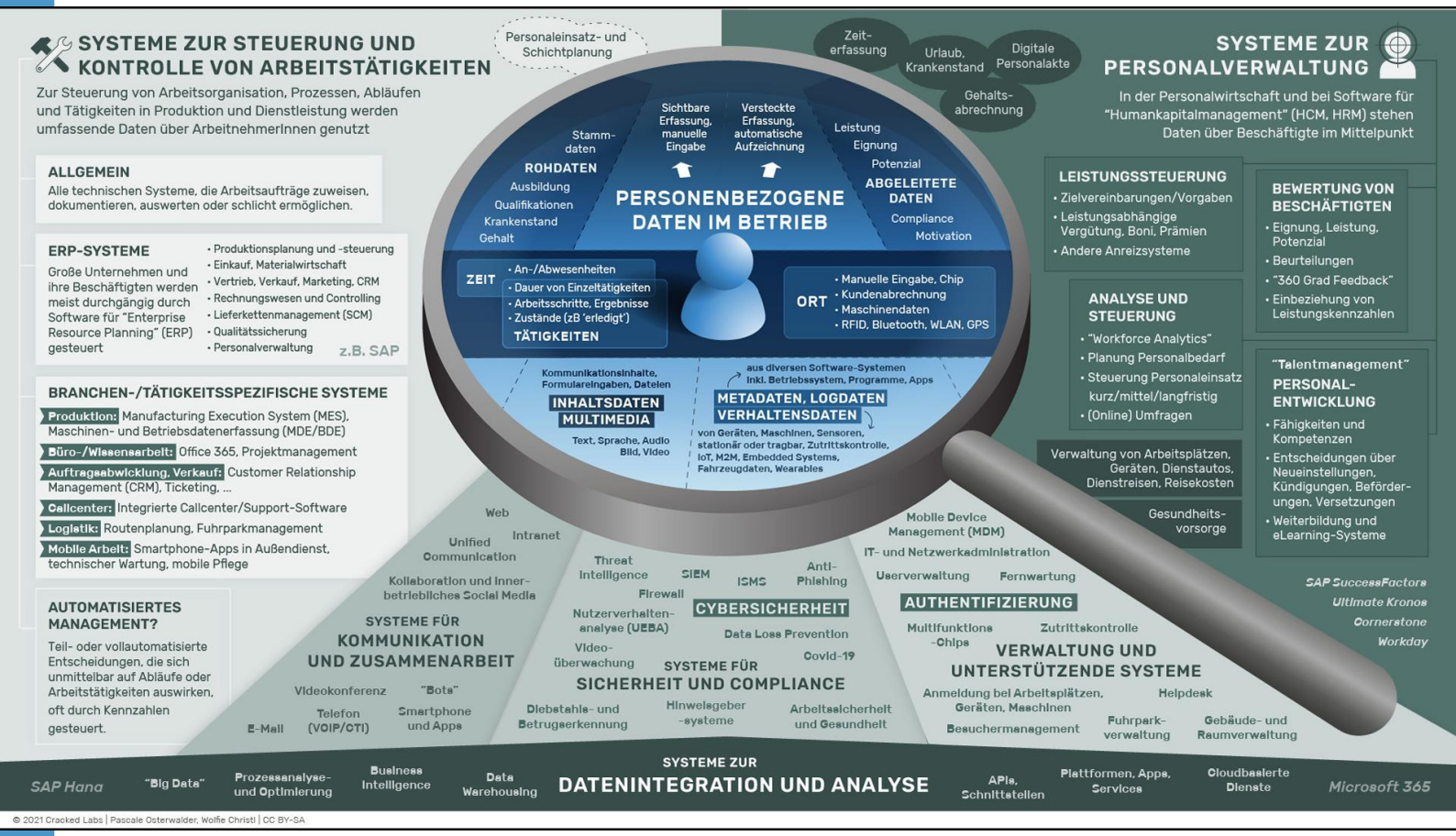


Abbildung 1: Landkarte betrieblicher Datenpraktiken und Systeme (Pascale Osterwalder, Wolfie Christl)

Die im Rahmen der Studie entwickelte Systematik datenverarbeitender Systeme ist maßgeblich von Thomas Riesenecker-Caba inspiriert (vgl. Riesenecker-Caba 2020, S. 12-14; Haslinger et al 2020, S. 36). Darauf aufbauend wurde unter Einbeziehung umfassender Literaturrecherche (siehe Kapitel 4) und Rückkopplung mit ExpertInnen aus der gewerkschaftlichen Beratungspraxis eine Systematik aus zwei Haupt- und vier Nebenkategorien entwickelt:

- **Systeme zur Steuerung und Kontrolle von Arbeitstätigkeiten** (links) umfassen alle technischen Systeme, die die eigentliche Kerntätigkeit eines Unternehmens ermöglichen. Dabei wird beiläufig oder gezielt eine Vielzahl an personenbezogenen Daten über die Beschäftigten erfasst und verarbeitet, die Betriebe potenziell zur Überwachung und Optimierung von Arbeitsleistung und andere Zwecke einsetzen.
- **Systeme zur Personalverwaltung** (rechts) könnten als Teilbereich der ersten Kategorie gefasst werden, wurden aber aus mehreren Gründen als eigene Kategorie hervorgehoben. Einerseits verarbeiten diese Systeme definitionsgemäß und gezielt Personaldaten. Andererseits werden dabei zumeist abgegrenzte Soft-

ware-Pakete eingesetzt. Zudem bildet die Trennung zwischen betrieblicher Kerntätigkeit und Personalabteilung die Organisationsstruktur der meisten Unternehmen ab. Trotzdem ist die Differenzierung unscharf. Betriebliche Steuerung und Personalwirtschaft gehen oft ineinander über.

- **Systeme zur Kommunikation und Zusammenarbeit** (links unten) wurden als eigene Kategorie hervorgehoben, weil dabei ebenfalls zumeist abgegrenzte Software-Lösungen eingesetzt werden, diese Systeme besonders sichtbar sind und weil Kommunikationsdaten grundrechtlich besonders geschützt sind.[10] In vielen Unternehmen könnten sie aber genauso als Teilbereich der ersten Kategorie gefasst werden.
- **Systeme für Sicherheit und Compliance** (unten Mitte) wurden als eigene Kategorie hervorgehoben, weil sie einerseits meist nicht die betrieblichen Kerntätigkeiten abwickeln. Andererseits lässt sich für Zwecke der Arbeitssicherheit und -gesundheit, Diebstahlsprävention, Compliance oder Cybersicherheit sehr viel leichter exzessive Datenverarbeitung rechtfertigen als für andere Zwecke. In bestimmten Branchen sind manche dieser Systeme jedoch durchaus auch näher an der Kerntätigkeit des Unternehmens – etwa Diebstahlsprävention bei Geldtransporten oder Cybersicherheit bei Banken oder kritischer Infrastruktur.
- **Unterstützende Systeme für Infrastruktur und Verwaltung** (unten rechts) bilden die betriebliche Infrastruktur oder unterstützen die Verwaltung. Dieser Kategorie wurde sowohl die Verwaltung von Gebäuden als auch die Verwaltung der IT-Infrastruktur zugeordnet, auch wenn der Übergang zu anderen Kategorien oft fließend ist. Zutrittskontrolle oder die Anmeldung bei IT-Systemen könnten etwa auch der Kategorie „Sicherheit“ zugeordnet werden. Selbstverständlich gibt es auch Unternehmen, bei denen die Verwaltung von Räumen oder von IT-Infrastruktur zur Kerntätigkeit gehört.
- **Systeme zur Datenintegration und Analyse** führen Daten aus mehreren betrieblichen Systemen zusammen, werten sie aus und helfen dabei, die zusammengeführten Daten wiederrum für betriebliche Ziele zu nutzen. Derartige Funktionen finden sich auch in Systemen der anderen Kategorien, wurden aber als eigene Kategorie herausgehoben, um den Aspekt der Zusammenführung eigens zu beleuchten.

Die Systematik ist keinesfalls universell auf jedes Unternehmen anwendbar und die Grenzziehung zwischen den Kategorien unscharf. Insbesondere die Kategorie „Datenintegration und Analyse“ wird mit zunehmender Vernetzung und Verknüpfung unterschiedlicher digitaler Dienste immer mehr zu einem Kernbestandteil betrieblicher Steuerung. Auch Systeme in Bereichen wie Cybersicherheit oder Personalverwaltung führen zunehmend Daten aus anderen Bereichen zusammen. Manche Software-Pakete decken mehrere Bereiche ab – wie etwa Microsoft 365 oder SAP. Dennoch soll die vorliegende Systematik dazu dienen, in Form einer Landkarte etwas mehr Ordnung und Überblick in die Vielfalt datenverarbeitender Systeme im Betrieb zu bringen.

5.2 Verarbeitung personenbezogener Daten über Beschäftigte

Personenbezogene Daten sind laut EU-Datenschutzgrundverordnung (DSGVO) „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen“. Als „identifizierbar“ wird eine „Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.[11] Damit definiert die DSGVO den Begriff

[10] z.B. durch das Kommunikationsgeheimnis, garantiert durch Artikel 7 der Charta der Grundrechte der Europäischen Union
[11] DSGVO Artikel 4 Z 1

sehr breit und versteht darunter bei weitem nicht nur Daten, die mit dem Namen eines Beschäftigten verknüpft sind. Beinahe jede Nutzung von Computern, Programmen, Geräten, Fahrzeugen oder Maschinen im Betrieb kann zur Verarbeitung personenbezogener Daten führen. **Pseudonymisierte Daten** – also Informationen, die etwa mit einer Kennnummer anstatt mit einem Namen verknüpft sind – zählen genauso zu den personenbezogenen Daten.[12]

Jede Verarbeitung personenbezogener Daten unterliegt den Regeln der DSGVO – sie benötigt etwa immer eine Rechtsgrundlage und darf nur für einen definierten Zweck erfolgen, der im Nachhinein nicht einfach verändert werden darf (Haslinger et al 2020, S. 61ff). Die Beschäftigten bzw. der Betriebsrat hat damit das Recht auf Mitbestimmung – in Österreich garantiert durch das Arbeitsverfassungsrecht (ebd., S. 131ff). Auch wenn die Ergebnisse einer Auswertung auf Basis personenbezogener Daten am Ende nicht mehr personenbeziehbar sein sollten, ist für die zuvor erfolgte Verarbeitung personenbezogener Daten eine Rechtsgrundlage nach der DSGVO erforderlich.

Bei der Erfassung personenbezogener Daten über Beschäftigte kann unterschieden werden zwischen:[13]

- **Transparent erfasste Daten**. Hier erfolgt die Erfassung sichtbar und im vollen Bewusstsein der Betroffenen. Beispiele dafür sind Daten, die bei der Bewerbung, Einstellung oder während des Arbeitsverhältnisses aktiv an- oder eingegeben wurden – von Stammdaten über Daten zur täglichen Arbeitszeit bis zur Eingabe eines Texts in ein Online-Formularfeld. Auch wenn etwa ein GPS-Standort nur durch eine bewusste Interaktion mit einer App gespeichert wird, könnte man dies als transparent erfasstes Datum betrachten.
- **Versteckt oder automatisch erfasste Daten**. Hier erfolgt die Erfassung unsichtbar und ohne Zutun der Betroffenen – etwa durch digitale Aufzeichnung von Verhaltensweisen bei der Nutzung von Computern, Smartphones, Maschinen oder anderen Geräten. Die Daten werden also passiv zur Verfügung gestellt.

Außerdem kann unterschieden werden zwischen:[14]

- **Rohdaten**, die direkt in der Form erfasst werden, in der sie gespeichert werden – also etwa Stammdaten, Daten zu Arbeitszeiten oder Krankenständen, der Inhalt einer Word-Datei oder einer E-Mail oder eine Logdatei, die die von einer Person besuchten Websites protokolliert. Rohdaten können sowohl transparent als auch versteckt erfasst werden.
- **Abgeleitete Daten**, die durch bestimmte Arten der Verarbeitung von Rohdaten entstehen. Dabei kann es sich um einfache Schlussfolgerungen handeln – wenn etwa aus der erfassten Uhrzeit des Arbeitsbeginns auf die Information „verspäteter Arbeitsbeginn“ geschlossen wird – oder um komplexe Einschätzungen oder Vorhersagen – etwa über Leistung, Eignung, Potenzial oder Motivation.

Zudem kann unterschieden werden zwischen:

- **Inhaltsdaten**, also die Inhalte von Kommunikationsvorgängen oder Dateien in Form von Text, Bild, Ton oder Video – etwa der Inhalt einer E-Mail oder einer Word-Datei, Suchbegriffe, digitale Formulareingaben oder das gesprochene Wort in einem Telefonat (vgl. Sánchez-Monedero und Dencik, 2019 S. 20-22).
- **Metadaten, Logdaten und Verhaltensdaten.** Inhaltsdaten sind nur die Spitze des Eisbergs. Oft viel relevanter sind Daten, deren Erfassung gleichzeitig viel weniger sichtbar ist und deren Bedeutung sich oft nicht auf den ersten Blick erschließt. Dabei handelt es sich zum Beispiel um Kommunikations-Metadaten – also

[12] DSGVO Erwägungsgrund 26
[13] Vgl. Volunteered/declared data vs. observed data, Christl und Spiekermann 2016, S. 84
[14] Vgl. Actual data vs. inferred data, Christl 2017, S. 15

etwa um Informationen über den Zeitpunkt und die EmpfängerIn einer Nachricht oder eines Anrufs. Generell speichern heute beinahe alle Software-Systeme vom Betriebssystem bis zu Programmen und Apps Logdaten, die potenziell Auskunft über Verhaltensweisen und Arbeitsalltag geben. Dies trifft oft genauso auf Geräte, Maschinen und Fahrzeuge zu. Vernetzte Sensoren, die personenbezogene Daten erfassen, können stationär sein oder sie werden am Körper getragen. Ein Zutrittskontrollsystem mit Chipkarte kann genauso Verhaltensdaten erzeugen wie Microsoft 365, das etwa die Zeitpunkte von Dateibearbeitungen und viele andere Aktivitäten protokolliert (vgl. Sánchez-Monedero und Dencik, S. 19-23; Fritsch 2021)

Aus Verhaltensdaten kann auf sensible Persönlichkeitseigenschaften und mögliche zukünftige Verhaltensweisen geschlossen werden (vgl. Christl und Spiekermann 2016, S. 11ff). Ein Betrieb kann auf Basis von Verhaltensdaten potenziell ein umfassendes Überwachungs- und Kontrollregime installieren, Arbeitstätigkeiten bis hin zu einzelnen Arbeitsschritten bewerten und kontrollieren oder einzelne Beschäftigte aussondern. Eine Überwachung von Kommunikationsinhalten ist dazu nicht nötig.[15] Verhaltensdaten verdienen daher besondere Aufmerksamkeit. In der DSGVO sind außerdem **besondere Kategorien personenbezogener Daten** definiert. Als sensibel und damit als besonders geschützt gelten Daten über Gesundheit, Gewerkschaftszugehörigkeit, politische Meinung, religiöse oder weltanschauliche Überzeugungen, rassische/ethnische Herkunft, sexuelle Orientierung sowie genetische und biometrische Daten.[16] Durch die Ausweitung der Erfassung, Verknüpfung und Analyse müssen jedoch heute viele Daten, die auf den ersten Blick als nicht sehr aussagekräftig erscheinen, als potenziell sensibel betrachtet werden.

Besondere Aufmerksamkeit verdienen folgende Arten personenbezogener Daten über Beschäftigte:

- **Zeit.** Jeder Betrieb erfasst Daten über Arbeitszeiten, Anwesenheiten (Kommen, Gehen) und Abwesenheiten (Urlaube, Krankenstand) und ist bis zu einem bestimmten Grad sogar rechtlich dazu verpflichtet (vgl. Haslinger et al 2020, S. 38). Dies kann neben der tatsächlichen Arbeitszeit auch die vereinbarte Arbeitszeit umfassen (Däubler 2017, S. 180). Sobald jedoch Zeitpunkte erfasst werden, die darüber hinausgehen, wird aus einer schlichten Zeiterfassung schnell eine Erfassung von Daten über Arbeitstätigkeiten.
- **Zeit und Arbeitstätigkeiten.** Daten über die Zeitpunkte der An- und Abmeldung an einem Computer, die Nutzung eines Kopierers oder das Betreten eines Raums mittels Chipkarte ermöglichen bereits weitergehende Auswertungen. Jede Erfassung der Zeitpunkte, zu denen Arbeitstätigkeiten beginnen oder enden, eignet sich für eine Leistungsauswertung – egal ob es sich dabei um längerfristige Arbeitspakete wie etwa Projekte oder gar um einzelne Arbeitsschritte handelt. Darunter fallen die Zeitpunkte von Zuständen (Stati) und deren Änderung – also ob etwa eine bestimmte Arbeitstätigkeit zugewiesen wurde, in Bearbeitung ist, erledigt wurde oder ob sie vielleicht erfolglos beendet wurde. Auch bei der Ankunftszeit bei einem Kunden oder beim Zeitpunkt eines Anrufs, eines Defekts an einer Maschine oder der Speicherung einer Word-Datei handelt es sich potenziell um Daten über Arbeitstätigkeiten. Der Grad an Detailinformation über eine Tätigkeit und die Zeitintervalle der Aufzeichnung können hier durchaus einen Unterschied machen (vgl. Haslinger et al 2020, S. 158). Aber auch aus rudimentären Daten über Zeitpunkte und Tätigkeiten lassen sich Schlussfolgerungen ziehen.
- **Ort.** Neben der Zeit war auch immer schon der Ort eine wesentliche Information, die das Verhalten von Beschäftigten beschreibt. Stellte sich früher nur die Frage, ob die Beschäftigten brav an der Maschine stehen oder vor dem Schreibtisch sitzen, haben sich die Möglichkeiten der automatisierten Standorterfassung

[15] Siehe z.B. die Fallstudie zu algorithmischer Kontrolle in Amazon-Verteilzentren im Abschnitt 7.1
[16] DSGVO, Artikel 9 Z 1

heute vervielfacht (vgl. Krause 2017, S. 9f). Das beginnt wiederrum beim Betreten von Räumen oder der Anmeldung bei Geräten oder Maschinen mit Chipkarte oder Passwort und endet bei der permanenten Ortung von Smartphones, Fahrzeugen oder sonstiger Geräte mittels GPS und anderer Technologien auf Basis von RFID, Bluetooth oder WLAN. Letztere ermöglichen eine im Vergleich zu GPS genauere Ortung in Innenräumen (vgl. Oguntala et al 2018; Däubler 2017, S. 209ff). Da eine permanente Ortung mittels GPS in Österreich[17] und Deutschland[18] in den meisten Fällen rechtlich problematisch ist, beschränken Unternehmen die Übertragung von Standorten immer wieder auf einzelne Zeitpunkte oder lassen die Beschäftigten manuell den Standort in eine App eintragen – etwa bei der Ankunft bei einem Kunden.[19] Auch wenn dabei kein so tiefer Eingriff in die Rechte der Beschäftigten stattfindet wie bei permanenter Ortung, lassen sich potenziell auch auf Basis punktuell eingegebener Standortdaten – etwa zum Zwecke der Abrechnung mit einem Kunden – mächtige Auswertungen durchführen.

Neben der Verarbeitung von offensichtlich sensiblen Daten – etwa über Gesundheit, biometrische Körpermerkmale, Kommunikationsinhalte oder in Form von Videoüberwachung – verdienen Daten über Zeitpunkte und Orte, die sich auf Arbeitstätigkeiten oder andere Verhaltensweisen beziehen, besondere Aufmerksamkeit. Die eigentliche Frage ist aber oft nicht, ob bestimmte Daten erfasst werden, sondern für welche Zweck sie verarbeitet werden. Was für einen Zweck zulässig oder gar rechtlich erforderlich sein kann, kann für andere Zwecke strikt unzulässig sein. Aus Sicht der ArbeitnehmerInnen ist es wohl trotzdem manchmal geboten, schon allein die Erfassung zu verhindern oder zu minimieren. Denn das Phänomen des sogenannten „Function Creep" – also die schleichende Ausweitung der Nutzung von einmal erfassten Daten für weitere Zwecke – ist lange bekannt (Koops 2021).

International verarbeiten Unternehmen zum Teil auch personenbezogene Daten über Beschäftigte, die nicht im Rahmen des Arbeitsverhältnisses erfasst werden, sondern sich auf das private Leben außerhalb der Arbeit beziehen. Wie die Beispiele in Abschnitt 6.9 zeigen, ermöglichen mehrere US-Anbieter die Auswertung von Informationen auf Socialmedia-Plattformen und von anderen externer Quellen – etwa zur Bewertung von Qualifikationen oder zur Prognose von Kündigungsabsichten.

5.3 Systeme zur Steuerung und Kontrolle von Arbeitstätigkeiten

Unternehmen nutzen schon immer unterschiedlichste Methoden, um die Arbeitstätigkeiten von Beschäftigten systematisch zu steuern und zu kontrollieren – ob in Produktion oder Dienstleistung. Wie eine Studie des Büros für Technikfolgenabschätzung des US-Kongresses über den „elektronischen Aufseher" aus dem Jahr 1987 sehr kompakt beschreibt, wurde schon im Zeitalter des Taylorismus Anfang des 20. Jahrhunderts damit begonnen, systematisch die Zeitdauer von Arbeitsschritten zu vermessen und mit anspruchsvollen Systemen aus Kontrollzetteln und Formularen jedes Detail des Produktionsprozesses aufzuzeichnen. Das sogenannte „wissenschaftliche Management" wurde bald von der Fabrik ins Büro übertragen, wo ebenfalls Arbeitstätigkeiten zerlegt, an unterschiedliche Beschäftigte verteilt und beschleunigt wurden. Versicherungen haben damit begonnen, die gut vermessbare Bearbeitung von Anträgen und Schadensfällen in eine Art von Fließbandarbeit zu verwandeln. Die Erfassung abgeschlossener Arbeitsschritte erfolgte hauptsächlich mit Papier und Bleistift, aber es gab mechanische Hilfsmittel. Mit

[17] Sabara, Bettina (2020): Unzulässige Verwendung eines GPS-Ortungssystems im Dienstfahrzeug - Schadenersatz. ARD, LexisNexis, 1.4.2020. Online: https://lesen.lexisnexis.at/news/unzulaessiger-verwendung-eines-gps-ortungssystems-im-dienstfahrz/ard/aktuelles/2020/14/lnat_news_028843.html

[18] Die Landesbeauftragte für den Datenschutz Niedersachsen (2018): Typische Fälle im Beschäftigtendatenschutz, 16.11.2018, S. 4-5 Online: https://lfd.niedersachsen.de/download/127627

[19] Siehe Fallbeispiel Anlagenbau 8.1

durch Uhren gesteuerten Zeitstempeln wurde erfasst, wann die Büroangestellten bestimmte Arbeitspakete erhalten und fertiggestellt hatten. Sogar Geräte zur Erfassung der Tippgeschwindigkeit auf mechanischen Schreibmaschinen wurden bereits Anfang des 20. Jahrhunderts eingesetzt (vgl. Office of Technology Assessment 1987, S. 18).

Diese **Zeitstempel** zur Vermessung und Steuerung von Arbeitstätigkeiten aus dem frühen 20. Jahrhundert sind im digitalen Zeitalter allgegenwärtig. Beinahe jedes technische System, das Arbeitsaufträge zuweist, den Arbeitsfortschritt und Ergebnisse dokumentiert oder den Beschäftigten die Arbeitstätigkeit überhaupt erst ermöglicht, speichert heute Logdaten mit digitalen Zeitstempeln und anderen Metadaten. Wie im vorangehenden Abschnitt ausgeführt, kann jede Erfassung von Zeitpunkten, zu denen Arbeitstätigkeiten beginnen oder enden, für eine Überwachung, Steuerung und Kontrolle von individueller oder kollektiver Arbeitsleistung genutzt werden – ebenso die Auswertung von Daten über Arbeitsergebnisse.

5.3.1 Enterprise Resource Planning (ERP)

Mittlere bis große Unternehmen und ihre Beschäftigten werden seit den 1990er Jahren meist durch Systeme des „Enterprise Resource Planning" (ERP) gesteuert. Der Begriff wurde bereits in den 1970er Jahren geprägt. Während ERP-Systeme anfangs hauptsächlich von Industriekonzernen für Produktionsplanung und -steuerung eingesetzt wurden, werden sie seit den 2000ern auch in Finanzwirtschaft, Gesundheit, Handel, Telekommunikation und sogar im Bildungsbereich eingesetzt (vgl. Shehab et al 2004). ERP-Systeme decken heute viele Unternehmensbereiche ab – von Rechnungswesen, Einkauf, Material- und Lagerwirtschaft bis Vertrieb, Verkauf und Logistik, von Marketing und Kundenbeziehungsmanagement (CRM) bis Projektmanagement und Personalverwaltung (HRM/HCM). Über Unternehmensbereiche hinweg erfüllen ERP-Systeme oft vielfältige Aufgaben von Arbeitsplanung und Qualitätssicherung bis „Controlling", das der Planung, Steuerung und Kontrolle von Unternehmenstätigkeiten dient (vgl. Gronau 2010). Globaler Marktführer ist der deutsche Konzern SAP, gefolgt von Oracle, Infor und Microsoft.[20]

ERP-Systeme strukturieren Arbeitsabläufe und haben darum erhebliche Auswirkungen auf den Arbeitsalltag der Beschäftigten. Sie bieten Funktionen zur Dokumentation und Kontrolle von Arbeitsleistung (Schörpf et al 2020, S. 70) und zeichnen Daten über sämtliche Arbeitsabläufe und -schritte auf, die Gegenstand des jeweiligen Systems sind (Haslinger et al 2020, S. 46). Diese Informationen sind in Datenbanktabellen oder in sogenannten **Ereignisprotokollen** („Event Logs") gespeichert (vgl. Selig 2017). Bei SAP enthalten viele Datenbanktabellen über betriebliche Abläufe eine Spalte, die angibt, welcher Beschäftigte die jeweilige Aktivität durchgeführt hat (ebd., S. 26). Auf Basis solcher Daten lässt sich lückenlos nachvollziehen, welche Tätigkeiten an einem Tag durchgeführt wurden – wie schnell und mit welchen Ergebnissen. Das macht potenziell Leistungsbewertungen und -vergleiche möglich (Haslinger et al 2020, S. 46). Betriebe analysieren diese Daten auf unterschiedliche Art und Weise – ob mittels eingebauter Auswertungen oder mit Hilfe von Zusatzsoftware (vgl. Abschnitt 6.3). Neben der Nutzung für Analysen und Berichte für Führungskräfte wirkt die Verarbeitung personenbezogener Daten in ERP-Systemen aber vielfach direkt auf ArbeitnehmerInnen zurück.

Darüber hinaus werden betriebliche Abläufe und Beschäftigte mit **branchen- und tätigkeitsspezifischen Systemen** gesteuert und kontrolliert, die eine Vielzahl an personenbezogenen Daten verarbeiten.

[20] Beroe (2021): ERP Software Market, Supplier, Risk and Competitive Intelligence. Online: https://www.beroeinc.com/category-intelligence/erp-software-market/

5.3.2 Produktion: Fertigungsmanagement (MES)

Die seit Jahrzehnten fortschreitende Computerisierung der Produktion wurde und wird mit unterschiedlichen Schlagworten diskutiert – von rechnergestützter Fertigung („Computer-Integrated Manufacturing", CIM) bis zur „Smart Factory" in der sogenannten „Industrie 4.0". Anfang des 21. Jahrhunderts gingen die elektronischen Leitstände der 1990er Jahre in integrierten Fertigungsmanagementsystemen auf – den sogenannten „Manufacturing Execution Systems" (MES).[21]

Während die Produktion in ERP-Systemen auf grober Ebene geplant und kontrolliert wird, steuern und überwachen **MES-Systeme** die Fertigung auf Tages-, Stunden-, Minuten- oder Sekundenebene. Zu den Kernfunktionen gehört die **Betriebsdatenerfassung (BDE)** zur Aufzeichnung von Informationen über Material und gefertigte Stücke, Start- und Endzeitpunkte von Bearbeitungsschritten, Qualität, Ausschusszahlen, Zustände, Prozessparameter wie Temperatur oder Druck, Bewegungen von Gütern oder Personaldaten. Die **Maschinendatenerfassung (MDE)** zeichnet als Teil davon mit Hilfe einer Vielzahl von Sensoren laufend Daten über Betriebszustände von Maschinen auf. Auch die Anwesenheit von Personal wird erfasst – bei der Anmeldung in Räumen, an Maschinen oder an Computern mit Chipkarte, Passwort oder Fingerabdruck. Mit am Federzug hängenden oder tragbaren Geräten werden im Rahmen unterschiedlicher Arbeitsschritte laufend Barcodes gescannt. Auch neuere „smarte" Geräte wie vernetzte und mit Sensoren bestückte Handschuhe, Kopfhörer oder Brillen erfassen Daten über ihre TrägerInnen.[22]

MES-Systeme verwenden diese Daten für die laufende Steuerung und Kontrolle von Abläufen, Produktionsraten, Durchlaufzeiten, Maschinenauslastung, Personalkapazitäten und Wartungsvorgängen. Bei Störungen oder Abweichungen zwischen geplanten und realen Vorgängen erfolgen kurzfristige Anpassungen. Für Zwecke der **Qualitätssicherung** wird laufend überprüft, ob Abläufe und Resultate den Vorgaben entsprechen. Im Rahmen der sogenannten vorausschauenden Wartung („Predictive Maintainance") erfolgen Prognosen über den Zustand von Geräten, Maschinen und Komponenten.

Im Endeffekt wird im Produktionsbereich heute jeder Arbeitsschritt digital dokumentiert. Dabei werden vielfältige personenbezogene Daten über Beschäftigte verarbeitet, die direkt oder indirekt Rückschlüsse auf Verhalten und Leistung ermöglichen (vgl. Kurbel 2013, S. 189ff; Haslinger et al 2020, S. 56).

5.3.3 Warenlogistik im Versandhandel

Das Fallbeispiel der Logistikzentren des Versandhandelsgiganten Amazon in Abschnitt 7.1 zeigt, wie auf Basis von Handscanner-Daten ein umfassendes System der sekundengenauen Leistungskontrolle und automatisierten Steuerung jedes noch so kleinen Arbeitsschritts geschaffen werden kann. Die Handscanner sind dort nicht nur mobile Aufzeichnungs- und Überwachungswerkzeuge, sondern geben mittels Display vor, welches Produkt als nächstes aus einem Regal geholt, in eine Kiste gelegt oder in ein Regal gestellt werden soll – und zählen die Sekunden herunter, die dafür zur Verfügung stehen. Ist der Zähler abgelaufen, wird die restliche Zeit als „unproduktive" Zeit aufsummiert. Individuelle Leistungsauswertungen über die bearbeiteten Produkte pro Stunde oder die durchschnitt-

[21] Für eine Liste bekannter Hersteller von MES-Systemen siehe z.B.: Franzosa, Rick und Hestermann, Christian (2021): Gartner Magic Quadrant for Manufacturing Execution Systems. Gartner, 30.3.2021. Online: https://www.gartner.com/en/documents/4000002/magic-quadrant-for-manufacturing-execution-systems

[22] Vgl. Fallbespiel in Abschnitt 8.3 und Leske, Stefan (2017): Der Handschuh mit eingebautem Scanner. IT & Production, 2.8.2017. Online: https://www.it-production.com/allgemein/der-handschuh-mit-eingebautem-scanner/

liche Taktrate in Sekunden pro Produkt sind allgegenwärtig. Werden die Vorgaben nicht erfüllt, erfolgen automatisierte Verwarnungen und gar Kündigungen. Wie in Abschnitt 7.1.4 ausgeführt, dürfte zumindest ein Teil des Systems auch bei Amazon Österreich und Deutschland in Betrieb sein.

5.3.4 Büro- und Wissensarbeit: Microsoft 365, Workflow-, Projekt- und Aufgabenverwaltung

Was in der Produktion die Betriebs- und Maschinendaten, sind in der Büro- und Wissensarbeit immer öfter Ereignisprotokolle, die nahezu jede Aktivität aufzeichnen. Seit der Einführung von **Microsoft 365** speichern Word, Excel, PowerPoint und viele andere Anwendungen von Microsoft viele Daten in der Cloud. Dabei wird etwa aufgezeichnet, wer wann welche Anwendung wie lange nutzt[23] oder – in Kombination mit der Cloud-Speicherlösung OneDrive – wer wann welche Datei erstellt, geändert, geöffnet oder freigegeben hat.[24] In Kombination mit Anwendungen für Kommunikation, Zusammenarbeit und Kalenderfunktionen wie Outlook, SharePoint und Teams – die ähnliche Aktivitätsdaten speichern[25] – und in Kombination mit dem Betriebssystem Windows 10 wird daraus ein umfassendes System, das den Arbeitsalltag von Millionen von Menschen rund um den Globus dokumentiert. Abseits der Frage, wie Microsoft die Daten für eigene Zwecke verarbeitet und ob Microsoft 365 in Europa überhaupt rechtskonform eingesetzt werden kann (vgl. Fritsch 2021, S. 14f), bietet es Unternehmen mit Workplace Analytics[26], der „Produktivitätsbewertung“[27] und anderen vorgefertigten Berichtsfunktionen weitreichende Möglichkeiten zur Auswertung dieser Daten. Darüber hinaus können Firmen über die Programmierschnittstelle „Graph API“ maßgeschneidert „auf die enormen Datenmengen in Microsoft 365, Windows 10 und Enterprise Mobility + Security zugreifen“[28] und sie in Folge nahezu beliebig auswerten – auch auf individueller Ebene.[29]

Neben Microsoft 365 dokumentiert fast jede Software zur Planung, Steuerung und Kontrolle von Abläufen oder Arbeitsaufgaben in digitaler Form, wie Beschäftigte arbeiten – von Systemen für Projektmanagement und Aufgabenverwaltung bis **Workflow-Management (WFMS)**. Für Abwicklung von Workflows – also von standardisierten Arbeitsabläufen – werden sowohl vorgefertigte Branchenlösungen als auch Eigenentwicklungen eingesetzt, oft als Teil von ERP-Systemen oder auf Basis neuerer cloudbasierter Plattformen wie ServiceNow[30]. Bei der Bearbeitung von Schadenfällen bei deutschen Versicherungen werden zum Beispiel Ablauf und Abfolge der Arbeitstätigkeiten präzise inhaltlich wie zeitlich vorgegeben. Bei Auffälligkeiten werden Vorgesetzte informiert. Auf Basis der erfassten Bearbeitungszeiten kann die Produktivität vermessen werden (Frühbrodt 2018, S. 47). Ähnliches erfolgt bei einem österreichischen Finanzdienstleister (Schörpf et al 2020, S. 14).

Die Dokumentation von Projektfortschritten durch ein **Projektmanagement-System** bei einem österreichischen Logistikdienstleister hat laut einem von Schörpf et al (2020) interviewten Mitarbeiter eine starke Kontrollfunktion und werfe permanent Fragen auf wie: „Wer ist wie weit? Wer hat was gemacht? Wer ist vorne? Wer ist hinten?“. Es werde damit natürlich alles „transparenter“ (ebd., S. 15). Im Bereich hochqualifizierter Software-Entwicklung wurden Formen des **„agilen“ Projektmanagements** entwickelt, die zwar einerseits stark auf Selbstorganisation und flache Hierarchien setzen (ebd., S. 30), durch die dabei genutzten digitalen Hilfsmittel aber andererseits eine

[23] https://docs.microsoft.com/de-de/microsoft-365/admin/activity-reports/microsoft365-apps-usage-ww?view=o365-worldwide [1.6.2021]
[24] https://docs.microsoft.com/de-de/microsoft-365/admin/activity-reports/onedrive-for-business-activity-ww?view=o365-worldwide [1.6.2021]
[25] https://docs.microsoft.com/de-de/microsoft-365/admin/activity-reports/activity-reports?view=o365-worldwide [1.6.2021]
[26] https://www.microsoft.com/de-de/microsoft-365/business/workplace-analytics [1.6.2021]
[27] https://docs.microsoft.com/de-de/microsoft-365/admin/productivity/productivity-score?view=o365-worldwide [1.6.2021]
[28] https://docs.microsoft.com/de-DE/graph/overview [1.6.2021]
[29] https://docs.microsoft.com/de-de/graph/api/overview?view=graph-rest-1.0 [1.6.2021]
[30] https://www.servicenow.com/ [2.6.2021]

sehr weitgehende Nachvollziehbarkeit aller Arbeitstätigkeiten ermöglichen. Neben Versionskontrollsystemen, die jeden noch so kleinen Beitrag zum Programmcode und jede Änderung aufzeichnen und einer Person zuordnen, werden dabei oft Systeme zur **Aufgabenverwaltung** eingesetzt, die die Zuweisung von Aufgaben, Arbeitsfortschritte, benötigte Zeiten und die Zusammenarbeit in Teams akribisch dokumentieren („Issue Tracking" bzw. „Ticket System"). Diese Daten werden auf unterschiedliche Weise ausgewertet (vgl. z.B. Poncin et al 2011, Ram et al 2018). Ähnliche Methoden für Projektmanagement und Aufgabenverwaltung werden inzwischen nicht mehr nur in der Software-Entwicklung, sondern auch in anderen Feldern der Wissensarbeit genutzt. Ein bekannter Anbieter diesbezüglicher Softwarelösungen ist Atlassian mit Produkten wie Jira.[31]

5.3.5 Verkauf und Kundenbetreuung: Customer Relationship Management (CRM)

Systeme für das „Customer Relationship Management" (CRM), also für das Kundenbeziehungsmanagement, zeichnen jede Interaktion mit KundInnen eines Unternehmens auf – von der Anbahnung eines Kontakts über Beratung, Angebotslegung und Verkauf bis zur langfristigen Betreuung. Zu den globalen Marktführern gehören Salesforce, SAP, Oracle und Microsoft (Christl 2017, S. 52).

Egal ob direkt an VerbraucherInnen verkauft wird oder hochpreisige Produkte oder Dienstleistungen an andere Unternehmen – durch die Erfassung aller **Kontakte und Interaktionen mit KundInnen** entstehen gleichzeitig umfassende digitale Protokolle über die Tätigkeiten der Beschäftigten, die diese KundInnen betreuen. Salesforce hat etwa vielfältige Auswertungsfunktionen eingebaut, die Führungskräften auf der Ebene einzelner Teammitglieder anzeigen, wer an einem Tag wie viel verkauft hat, welche Aktivitäten dafür gesetzt wurden oder wie viele Kontakte dafür angebahnt werden mussten – und damit Leistungsvergleiche ermöglichen.[32] Auch die **Kundenzufriedenheit** wird oft quantitativ vermessen – etwa in Form des „Customer Satisfaction Score" (CSAT) oder des „Net Promoter Score" (NPS)[33] – und in Folge zur Bewertung von Arbeitsleistung eingesetzt.[34]

5.3.6 Callcenter-Systeme

In verschärfter Form erfolgt diese permanente Leistungskontrolle schon lange in einem Bereich, der eng verwandt ist mit den im vorigen Abschnitt beschriebenen Praktiken in Verkauf und Kundenbetreuung. Wie die Fallstudie über algorithmische Kontrolle im Callcenter in Abschnitt 6.1 zeigt, werden dort nahezu alle Arbeitstätigkeiten automatisiert zugewiesen, gesteuert und sekundengenau überwacht.

Callcenter-Systeme zeigen Führungskräften in Echtzeit eine Vielzahl an Leistungskennzahlen über einzelne ArbeitnehmerInnen an – von der Zahl der durchgeführten Gespräche und deren durchschnittlicher Dauer bis zu Reaktions- und Nachbearbeitungszeiten. Im Namen von Qualitätssicherung, Kundenzufriedenheit und Compliance werden Gespräche aufgezeichnet, automatisiert bewertet und können nach Stichwörtern durchsucht werden. Manche Callcenter-Systeme analysieren auf Basis der erwähnten Wörter, von Tonfall, Sprechgeschwindigkeit und Lautstärke gar Emotionen und Stimmung in Gesprächen und berechnen daraus Kennzahlen über Kundenzufriedenheit sowie über die Höflichkeit und Empathie-Fähigkeit der Beschäftigten – oder geben zumindest vor, dies zu tun.

---

[31] https://www.atlassian.com/de/software/jira/work-management [2.6.2021]

[32] https://www.salesforce.com/content/blogs/us/en/2019/01/sales-management-dashboards.html [2.6.2021]

[33] Van Dessel, Gert (2014): Measure customer satisfaction: CSAT, CES and NPS compared. CheckMarket, November 2014. Online: https://www.checkmarket.com/blog/csat-ces-nps-compared/

[34] Coleman, Greg (2019): Tips for Effectively Tying Staff Performance to Customer Satisfaction. Future of Field Service, 11.3.2019. Online: https://www.futureoffieldservice.com/2019/03/11/tips-for-effectively-tying-staff-performance-to-customer-satisfaction/

5.3.7 Einzelhandel und Gastronomie: Kassensysteme

Daten über Kassaaktivitäten bilden Verhalten und Arbeitsalltag der Beschäftigten in Einzelhandel und Gastronomie sehr weitgehend ab. Wie das Fallbeispiel in Abschnitt 6.2 zeigt, bieten Kassensysteme aus Deutschland und Österreich Funktionen zur Bewertung der Leistung einzelner Beschäftigter auf Basis von Kassendaten. Dabei sind für Vorgesetzte etwa Daten zu Umsätzen, bedienten Tischen, zur Zahl der ausgestellten Bons und der Zeit zwischen den Bon-Ausstellungen einsehbar – sowohl auf Einzelpersonenebene als auch im Vergleich zum Durchschnitt. Zettle, ein schwedischer Anbieter von Bezahlsystemen für Handel und Dienstleistung, zeigt ebenfalls beschäftigtenspezifische Verkaufsumsätze sowie Informationen zur Art und Anzahl der verkauften Produkte an. Auch der globale IT-Gigant Oracle stellt eine Vielzahl an Funktionen zur Überwachung und Leistungsbewertung von Kassa-MitarbeiterInnen und Verkaufspersonal auf individueller Ebene zur Verfügung.

5.3.8 Logistik und Zustellung: Fuhrparkverwaltung, Routenplanung

Moderne Fahrzeuge sind Computer auf Rädern, erfassen und speichern eine Vielzahl an Daten oder senden sie gar permanent an den Hersteller oder an andere Parteien (vgl. FIPA 2015).

Das System zur betrieblichen Flotten- bzw. Fuhrparkverwaltung des US-Telekomkonzerns Verizon wertet etwa neben Echtzeit-Standortdaten[35], zurückgelegten Distanzen, Fahrzeiten und Stopps alle möglichen Sensordaten aus – von Fahrgeschwindigkeit, Drehzahl und Kraftstoffverbrauch bis zu Reifendruck, Batteriespannung, Temperatur der Kühlflüssigkeit und diverse Warnungen und Fehlercodes. Auch die Zeiträume, in denen der Gurt nicht angelegt ist oder in denen der Motor läuft, obwohl sich das Fahrzeug nicht bewegt, werden analysiert. Der Fahrstil – etwa zu hartes Bremsen, Beschleunigen oder Lenken – wird bewertet. Aus all diesen Daten können Scores – also Punktebewertungen – für einzelne FahrerInnen berechnet sowie Ranglisten erstellt werden.[36]

Wie das Fallbeispiel in Abschnitt 6.8 zeigt, erfasst auch Easytrack, ein österreichischer Anbieter für die Fuhrparkverwaltung in Branchen wie Transport, Bau, Handwerk oder Gesundheitswesen, weitreichende Daten wie exakte GPS-Standorte, Motor-Leerläufe, plötzliche Beschleunigungen/Bremsungen, gefahrene Routen und Arbeitszeiten. Vorgesetzte können E-Mail-Benachrichtigungen bekommen, wenn ein Beschäftigter zu schnell fährt, den Motor zu lang im Stand laufen lässt, das Fahrzeug außerplanmäßig stoppt oder einen definierten Bereich verlässt. Als Zwecke der Datenverarbeitung hebt Easytrack unter anderem Ökologie und Sicherheit hervor. Manche Daten müssen gesetzlich verpflichtend aufgezeichnet werden, etwa die Lenk- und Ruhezeiten bei LKW-FahrerInnen oder das (elektronische) Fahrtenbuch für das Finanzamt. Die angebotenen Funktionen gehen jedenfalls darüber hinaus.

Automatisierte Routenplanungssysteme gehen über die Überwachung und Bewertung des Fahrverhaltens hinaus. Wie das Fallbeispiel über Routific in Abschnitt 6.8 zeigt, können damit die zu fahrenden Routen – und damit die Arbeitstätigkeiten – von ZustellerInnen auf Basis von Echtzeit-Standortdaten engmaschig und weitgehend automatisiert gesteuert werden. Das System verspricht, die Vorgaben für die Routen in Echtzeit immer wieder zu optimieren. Basis für die automatisierte Routenplanung sind nicht nur Zustelladressen, Zeitpunkte, Fahrzeugkapazitäten und Schichtpläne, sondern auch durch Führungskräfte vorgenommene Einstellungen für die Zeit, die pro Auslieferung vor Ort zur Verfügung stehen soll. Außerdem kann für jede Person eine Vorgabe für die Geschwindigkeit

[35] https://www.verizonconnect.com/solutions/gps-fleet-tracking-software/ [3.6.2021]
[36] https://fleet-help.verizonconnect.com/hc/en-us/articles/360010698879-List-of-Key-Performance-Indicators [3.6.2021]

eingestellt werden – zwischen 10% und 190% der vom Navigationsdienst berechneten Geschwindigkeit. Eine Vorgabe von 190% (!) der vom Navigationsdienst berechneten Geschwindigkeit dürfte in Bezug auf Sicherheit und Arbeitsqualität wohl kaum adäquat sein. Dazu stehen viele Auswertungen auf individueller Ebene zur Verfügung.

Derartige Systeme versprechen meist, die Effizienz zu erhöhen und Kosten zu senken. Die vorhandenen Überwachungsfunktionen werden dabei oft nur sehr selektiv im Interesse der Firmen genutzt. Eine Reportage hat kürzlich gezeigt, wie die automatisierte Routenplanung von Amazon, die 85.000 AuslieferungsfahrerInnen steuert, diese durch extrem knappe Zeitvorgaben systematisch in gefährliche Situationen bringt (vgl. Gurley 2021).

Auch ein in Österreich tätiger Plattform-Zustelldienst hat ein System mit **Echtzeit-Standortüberwachung** im Einsatz. Wie das Fallbeispiel in Abschnitt 8.5 zeigt, hängt der Verdienst zum Teil – je nach Arbeitverhältnis – von der Zahl gefahrener Kilometer oder ausgelieferter Bestellungen ab. Eine höhere Zahl ausgelieferter Bestellungen führt darüber hinaus zu Vorrechten bei der Wahl der Schichtzeiten für die Folgewoche. Da manche Schichten lukrativer sind, wirkt sich die Leistungsbewertung hier sogar mehrfach auf den Verdienst aus.

5.3.9 Mobile Arbeit von Außendienst bis Pflege

Das Smartphone ist in den letzten zehn Jahren in sehr unterschiedlichen Branchen und Tätigkeitsbereichen zur mobilen Kommando- und Kontrollzentrale für den Arbeitsalltag geworden – vom Außendienst im Verkauf über Handwerk und technische Wartung bis zur mobilen Pflege. Neben der Erfassung von Arbeitsbeginn und -ende werden dabei oft weitergehende Daten über Dauer, Inhalt und Ergebnissen von Tätigkeiten erfasst – etwa für die Abrechnung von Reparaturen gegenüber KundInnen oder für die Dokumentation eines Pflegebesuchs (vgl. Krause 2017, S. 12, 31). Sobald Dauer und Inhalt der Tätigkeiten nicht nur aufgezeichnet, sondern auch vorgegeben werden, wird die App zur Zeiterfassung schnell zu einer Art von mobilem Management per App. Die Zeiterfassungs- und Auftragsbearbeitungs-Apps des deutschen Herstellers M-SOFT bietet etwa eine tätigkeitsbezogene Auftragszeiterfassung[37] und stellt für den jeweiligen Termin die zu bearbeitenden Aufgaben dar.[38] GPS-Ortung könne genutzt werden, damit "Arbeitgeber genau sehen, bei welchen Kunden sich die Mitarbeiter befinden".[39]

Wie das Fallbeispiel über die Montage und Wartung von Anlagen in Österreich in Abschnitt 8.1 zeigt, wurde der Arbeitsalltag bei Betrieben der Interviewpartner über viele Jahre hinweg immer mehr von mobilen Geräten dominiert. Wurde anfangs nur mit rudimentären SMS-Codes mit der Zentrale kommuniziert, so werden heute Bewegungen, Zeiträume und Arbeitsschritte via Smartphone-App dokumentiert. Eine Karte in der Zentrale zeigt, wer gerade woran arbeitet. Gleichzeitig werden die durchzuführenden Arbeitsschritte immer genauer vorgegeben – unter anderem auf Basis von Daten, die Anlagen selbsttätig an die Zentrale senden. Das System ist an SAP angebunden. Auch KundInnen, die die Anlagen betreiben, haben Echtzeit-Zugriff auf Daten über die von Beschäftigten durchgeführten Wartungsarbeiten. Sie tragen durch ihr Interesse an Informationen über die durchgeführten Arbeiten zur Ausweitung der Datenerfassung über diejenigen bei, die diese Arbeiten durchführen. Laut den Interviews sei die Arbeitseinteilung nun sehr viel weniger selbstbestimmt und die für Wartungstätigkeiten zur Verfügung stehende Zeit habe sich im Lauf der Jahre auf einen Bruchteil reduziert. Bei nahezu wöchentlichen Gesprächen mit Vorgesetzten werde die Zeit für Tätigkeiten und Arbeitsschritte auf Minuten- oder gar Sekundenniveau diskutiert.

[37] https://www.msoft.de/stempeluhr-hat-als-klassischer-arbeitszeitmesser-ausgedient.html [3.6.2021]
[38] https://www.msoft.de/software/mobile-auftragsbearbeitung/shk-elektro-gebaeudetechnik/auftragsbearbeitung-mobil.html [3.6.2021]
[39] https://www.msoft.de/stempeluhr-hat-als-klassischer-arbeitszeitmesser-ausgedient.html [3.6.2021]

Eine Fallstudie aus Australien machte ähnliche Beobachtungen in der mobilen Pflege (vgl. United Workers Union 2020, S. 49ff). Jacob Metcalf (2018) hat sich damit befasst, wie durch das Begehr, die Arbeit von mobilen PflegerInnen via App genauer zu überprüfen, auch die Gepflegten genauer überwacht werden – und umgekehrt.

5.3.10 Automatisiertes „algorithmisches" Management?

In den letzten Jahren ist immer wieder vom „algorithmischen" Management die Rede. Dabei geht es oft um plattformbasierte Arbeit wie etwa beim Taxivermittlungskonzern Uber, wo nahezu alle Arbeitstätigkeiten bis ins Detail durch ein System vorgegeben und kontrolliert werden. Das macht die Smartphone-App für die Beschäftigten faktisch zum allgegenwärtigen „Chef" (vgl. Prassl 2018). Während der Begriff des „Algorithmus" in Mathematik und Informatik eine eng definierte Bedeutung hat, wird er in der Debatte über die Auswirkungen von Informationstechnologie und Datenverarbeitung auf Mensch und Gesellschaft sehr viel breiter verwendet. Die deutsche NGO Algorithmwatch spricht von Prozessen „algorithmischer Entscheidungsfindung" („Algorithmic Decision Making", ADM), bei denen auf Basis von Datenerfassung und -analyse automatisierte Entscheidungen über Menschen getroffen werden – oder menschliche Entscheidungen durch Algorithmen vorhergesagt oder vorbestimmt werden.[40]

Algorithmisches Management beschreibt laut Mateescu und Nguyen (2019b) Systeme unterschiedlicher Komplexität, die auf der Grundlage von Datenerfassung in Echtzeit automatisierte oder teilautomatisierte Entscheidungen über Beschäftigte treffen und dabei Leistungsbewertungen, Anreize oder Sanktionen einbeziehen, die Verhalten steuern sollen. In einem allgemeinen Sinn könnte wohl die gesamte Geschichte der Automatisierung im Betrieb als Geschichte einer Automatisierung von „Management" aufgefasst werden. Schon die anspruchsvollen Systeme zur Steuerung und Kontrolle von industriellen Produktionsabläufen mit Hilfe von Kontrollzetteln und Formularen Anfang des 20. Jahrhunderts stellten in einer gewissen Weise Systeme des algorithmischen Managements dar – ebenso die Anfänge der Automatisierung von Büroarbeit, wo etwa Versicherungen damit begonnen haben, die Bearbeitung von Schadenfällen mit Hilfe von Zeitstempeln für Arbeitspakete zu steuern und zu kontrollieren. In beiden Bereichen wurden zumindest teilautomatisierte Entscheidungen darüber getroffen, welche Arbeitstätigkeiten wann verrichtet werden sollen und wie lange deren Erfüllung dauern soll – auf Basis von Datenerfassung auf Papier.[41]

Zeitgenössische Technologien zur Erfassung, Zusammenführung und Analyse von Daten sowie zur Rückmeldung an Beschäftigte mittels Bildschirm, mobilen Geräten oder anderen Mechanismen sind mehr denn je von automatisierten Entscheidungen geprägt. Arbeitsabläufe werden in erheblicher Weise digital strukturiert, gesteuert und kontrolliert. Digitale Systeme weisen Tätigkeiten zu, machen automatisierte Vorgaben oder Empfehlungen für Arbeitsschritte oder üben mit Leistungsbewertungen und automatisierten „Anreizen" Druck aus. Einige Beispiele:

- Automatisierte Zuweisung von Gesprächen im Callcenter auf Basis umfassender Daten über Beschäftigte und KundInnen (vgl. Abschnitt 6.1)
- Vorgabe des nächsten zu bearbeitenden Produkts samt Zeitvorgabe in Sekunden im Amazon-Verteilzentrum mittels Handscanner (vgl. Abschnitt 7.1)
- Vorgaben für Arbeitsschritte bei der mobilen Wartung von Anlagen auf Basis von Sensordaten von Maschinen und Anlagen (vgl. Abschnitt 8.1)

[40] https://algorithmwatch.org/de/was-wir-tun/ [18.7.2021]
[41] Siehe Einleitung von Abschnitt 5.3

- Steuerung von Arbeitstätigkeiten durch Fertigungsmanagementsysteme in der Produktion anhand von Aufträgen, Durchlaufzeiten, Maschinenauslastung, Personalkapazitäten, Störungen und Wartungsvorgängen (vgl. Abschnitt 5.3.2)
- Vorgaben für Arbeitsschritte bei standardisierten Abläufen wie der Bearbeitung von Schadenfällen bei Versicherungen mit Systemen für Workflow-Management (vgl. Abschnitt 5.3.4)
- Automatisierte Erstellung, Zuweisung und Priorisierung von Arbeitsaufgaben in Form von „Tickets“ oder „Tasks“ (vgl. Abschnitte 6.3.2 und 5.3.4)
- Automatisierung von Abläufen und Tätigkeiten mit Systemen für „Robotic Process Automation“ (vgl. Abschnitt 6.3.4)
- Automatisierte Zuweisung von Tätigkeiten auf Basis von Arbeitszeiten und Erfahrungen, Fähigkeiten und Kompetenzen durch Software für Projektmanagement (vgl. Abschnitt 5.4.5)
- Ampelsysteme, die von grün auf gelb und rot umschalten, wenn zu langsam gearbeitet wird, um Druck auf Teams oder einzelne Beschäftigte auszuüben (vgl. Abschnitt 5.4.7)
- Leistungs- und Verhaltenssteuerung mit „Gamification“ in Form von Punktesammelsystemen, Wettbewerben, Ranglisten, Auszeichnungen und anderen Spielmechaniken (vgl. Abschnitt 5.4.9)
- Automatisierte Planung und dynamische Anpassung von Routen in der Zustellung (vgl. Abschnitt 6.8.1)
- Automatisierte Planung und dynamische Anpassung von Schichtplänen unter Einbeziehung von Ausfällen und tagesaktuellen Schwankungen beim zu erwartenden Arbeitsvolumen (vgl. Abschnitt 5.4.12)
- Personaleinsatzsteuerung in Form einer (teil)automatisierten Verteilung anwesender ArbeitnehmerInnen auf Maschinen, Verkaufsabteilungen oder Baustellen (ebd.)
- Priorisierung bei der Auswahl von Schichten auf Basis der Wochenleistung und automatisierte Sanktionen beim Plattform-Zustelldienst (vgl. Abschnitt 8.5)
- Automatisierte Verwarnungen und Kündigungen in Amazon-Verteilzentren bei Unterschreitung von Leistungsvorgaben oder anderen Verfehlungen (vgl. Abschnitt 6.1)
- Automatisierte Empfehlungen für betriebsintern ausgeschriebene Positionen oder Weiterbildungsmaßnahmen auf Basis von Einschätzungen über Leistung, Fähigkeiten und Kompetenzen (vgl. Abschnitt 5.4.11)
- Automatisierte Vorschläge für Entlohnung und Beförderungen (ebd.)

Bei manchen dieser Beispiele findet die Automatisierung von Management auf der Mikroebene statt und ist unmittelbar in den Arbeitsprozess integriert. Andere Beispiele betreffen die mittel- bis langfristige Steuerung des Personals und könnten damit als Automatisierung der Personalverwaltung gefasst werden.

Auf der Makroebene können viele ineinandergreifende Funktionen von Systemen für Enterprise Ressource Planning (ERP) und Supply Chain Management (SCM) – sowie noch viel allgemeiner das „Controlling“ und die Ableitung von Handlungen aus Kennzahlen – als Formen des algorithmischen Managements betrachtet werden (vgl. Abschnitt 5.3.1; Posner 2019), ebenso die unternehmensweite Personal- und Leistungssteuerung mit Hilfe von Zielvorgaben, Beurteilungen und davon abgeleiteten Maßnahmen (vgl. Abschnitt 5.4.3).

5.4 Von digitaler Personalverwaltung zur Steuerung von „Humankapital"

Während bei den im vorigen Abschnitt beschriebenen Systemen die Verarbeitung personenbezogener Daten im Zuge der Steuerung und Kontrolle betrieblicher Kerntätigkeiten im Vordergrund steht, befasst sich dieser Abschnitt mit Systemen, die in Unternehmen typischerweise von der Personalabteilung betrieben werden, und die sich somit unmittelbar auf Beschäftigte beziehen und auswirken.

Wie bei der Beschreibung der Aufgaben der Personal- bzw. HR-Abteilung eines Unternehmens unterschiedliche Begriffe von Personalwirtschaft bis Personalverwaltung bzw. Human Resource Management (HRM) verwendet werden und sich Aufgaben und Ausrichtung der Personalabteilung je nach Betrieb unterscheiden oder wandeln (vgl. Drumm 2008, S. 26), so werden auch die entsprechenden datenverarbeitenden Systeme unter verschiedenen Bezeichnungen beschrieben bzw. vermarktet. Während der Begriff des **Personalinformationssystems (PIS)** den Aspekt der Datenverarbeitung über Beschäftigte betont, gehen Bezeichnungen wie **Personalverwaltungs- bzw. HRM-System** darüber hinaus und weisen auf Aspekte der Steuerung und Kontrolle hin. Führende Hersteller wie SAP haben für diese Personalverwaltungsfunktionen lange den zynischen Begriff des **Human Capital Management (HCM)** – also der Humankapitalverwaltung – verwendet. Seit kurzem wurde der euphemistische Begriff des **Human Experience Management (HXM)** etabliert, der das „Erlebnis" von ArbeitnehmerInnen betont.[42]

Die aus den ersten EDV-gestützten Formen der Lohn- und Gehaltsabrechnung hervorgegangenen Personalinformationssysteme wurden schon vor Jahrzehnten zu wichtigen Mitteln der **Personalsteuerung und -planung**. Neben der Verarbeitung von Stammdaten und Informationen zu Arbeitszeiten, Urlauben, Krankenständen sowie zu Einstellungen, Versetzungen und Austritten weiteten sich Rolle und Funktionen von Personalverwaltungssystemen im Lauf der Jahre immer weiter aus (Däubler 2017, S. 49, Sommer 2014). Einerseits werden Personaldaten aus unterschiedlichen Unternehmensbereichen und Standorten zunehmend in globalen Systemen zusammengeführt (Haslinger et al 2020, S. 38). Andererseits wird die Personalverwaltung immer mehr an übergeordneten betrieblichen Zielen und jährlichen Planungszyklen von Unternehmen ausgerichtet. Die heute eingesetzten Personalverwaltungssysteme ermöglichen eine enge Verzahnung von Unternehmensstrategie, Personalsteuerung und -planung mit daraus folgenden Maßnahmen, die einzelne ArbeitnehmerInnen betreffen – von der Einstellung über Zielvereinbarungen, Leistungsbeurteilung und Gehaltsentscheidungen bis zu Weiterbildung und Aufstiegsmöglichkeiten (vgl. Sommer 2014, Pilarski 2016). Sie sind nicht isoliert, sondern mit anderen Informationssystemen im Betrieb verknüpft (Pilarski 2016) und beziehen immer öfter Daten über Arbeitstätigkeiten mit ein (Däubler 2017, S. 51).

Wie Katrin Sommer (2014) zusammenfasst, dienen zeitgenössische Personalverwaltungssysteme dazu, die Belegschaft zu „optimieren" und helfen Unternehmen dabei, auf Basis von **Kategorisierungen von Beschäftigten** Entscheidungen über diese zu treffen – und dabei etwa folgende Fragen zu beantworten: „Wer sind die Top-Leister? Wer sind die Potenzialträger? Wen wollen wir halten, wen nicht? Nach welchen Kriterien wählen wir Mitarbeiter aus? Wer wird gefördert? In wen investieren wir? Wen qualifizieren wir wie? Wer soll wem auf welchen Job nachfolgen? Wer bekommt welche Gehaltserhöhung? Und natürlich auch die Frage: Welcher Mitarbeiter hat keine Zukunft mehr im Unternehmen?"

[42] Klempien, Guido (2020): Die „Ressource" wird zum „Mensch": SAP HCM wird SAP HXM. Activate HR, 21.4.2020. Online: https://activate-hr.de/successfactors/die-ressource-wird-zum-mensch-sap-hcm-wird-sap-hxm/

Personalverwaltungssysteme sind manchmal Bestandteil von ERP-Software und haben sich in den letzten Jahren in die Cloud verlagert. Zu den bekannten Anbietern gehören SAP, Workday, Oracle, Ceridian, Ultimate Kronos Group, Sage oder Cornerstone.[43] Insbesondere **Workday und SuccessFactors**, das neue cloudbasierte System von SAP, werden wegen ihrer weitreichenden Datenverarbeitungsfunktionen von gewerkschaftlicher Seite oft diskutiert (vgl. Sommer 2014; Sommer 2017; Fritsch 2017).

5.4.1 Grundfunktionen: An- und Abwesenheiten, Lohn/Gehalt, digitale Personalakte

Zu den Grundfunktionen von Personalverwaltungssystemen gehören die Erfassung von Anwesenheiten (Kommen, Gehen), Abwesenheiten (Krankenstände, Urlaube) sowie von diversen Stammdaten. Neben allgemeinen Angaben zur Person (z.B. Name, Geburtsdatum, Familienstand, Wohnadresse, Kontaktinformationen) werden Daten für die Lohn- und Gehaltsabrechnung verwaltet. Auch Informationen über den zugewiesenen Arbeitsplatz oder einen etwaigen Dienstwagen können gespeichert sein.[44] Im Zuge der **Digitalisierung der Personalakte** wurden Daten über Beschäftigte zentralisierter gespeichert und leichter auswertbar. Dazu zählen Angaben aus dem Bewerbungsverfahren (z.B. Ausbildungsweg, Abschlüsse, beruflichen Qualifikationen, Zertifizierungen) genauso wie Informationen zu aktuellen und früheren Positionen im Unternehmen, zu körperlichen und gesundheitlichen Einschränkungen oder zu Fehlzeiten, Abmahnungen und anderen disziplinarischen Maßnahmen. Teile davon müssen wegen gesetzlicher Verpflichtungen erfasst werden, aber aktuelle Personalverwaltungssysteme gehen oft weit darüber hinaus (vgl. Däubler 2017, S. 49ff; Haslinger et al 2020, S. 38f und S. 149f).

Sobald die Erfassung von Stammdaten oder Arbeitszeiten über das gesetzlich geforderte Ausmaß hinausgeht, werden schnell **weitergehende Auswertungen** möglich. Die Stammdatenverwaltung von SAP SuccessFactors, die 2018 laut Eigenangabe global für über 20 Millionen ArbeitnehmerInnen eingesetzt wurde[45], bietet etwa Zugriff auf eine Vielfalt an Personaldaten[46] – darunter Einschätzungen über Fähigkeiten und Kompetenzen von Beschäftigten.[47]

SAP bietet schon lange Möglichkeiten, die **Zeiterfassung** über die Aufzeichnung von Arbeitsbeginn und –ende hinaus auszuweiten – und etwa Teile der Arbeitszeit für Abrechnungszwecke bestimmten Projekten oder KundInnen zuzuordnen.[48] Zudem können die Daten aus SuccessFactors in anderen Systemen verwendet oder umgekehrt aus anderen Systemen übernommen werden[49] – zum Beispiel aus Zeiterfassungssoftware von Drittanbietern.[50] Wie Abschnitt 5.3.9 zeigt, erfassen etwa mobile Zeiterfassungssysteme für Zwecke der Abrechnung oder Dokumentation

---

[43] Cerrato, Jason; Pang, Chris; Freyermuth, Jeff; Hanscome, Ron; Grinter, Sam; Chandra, Ranadip; Grainger, Amanda; Kostoulas, John; Poitevin, Helen (2020): Magic Quadrant for Cloud HCM Suites for 1000+ Employee Enterprises. Gartner, 9.11.2020. Online: https://www.gartner.com/en/documents/3992866/magic-quadrant-for-cloud-hcm-suites-for-1-000-employee-e, Fortune Business Insights (2020): Human Capital Management (HCM) Market Size, Share & COVID-19 Impact Analysis, By Offering (Solution and Services), By Deployment (Cloud, and On-Premises), By Enterprise Size (SMEs, and Large Enterprises), By End-use Industry (IT and Telecommunication, BFSI, Government, Retail, Healthcare, Education, Manufacturing, and Others), and Regional Forecast, 2020-2027. September 2020. Online: https://www.fortunebusinessinsights.com/industry-reports/human-capital-management-hcm-market-100240, Data Bridge (2020): Global Human Capital Management (HCM) Market – Industry Trends and Forecast to 2027. Juli 2020. Online: https://www.databridgemarketresearch.com/reports/global-human-capital-management-hcm-market

[44] https://help.sap.com/doc/ff28e153038a424de10000000a174cb4/3.6/de-DE/e9a0e0535e56424de10000000a174cb4.html [9.6.2021]

[45] https://blogs.sap.com/2018/12/27/5-years-with-sap-successfactors-employee-central/ [9.6.2021]

[46] https://api.sap.com/package/SuccessFactorsEmployeeCentral?section=Artifacts [9.6.2021]

[47] https://api.sap.com/api/ECSkillsManagement/resource [9.6.2021]

[48] Siehe z.B. „Cross-Application Time Sheet" (CATS): https://help.sap.com/doc/3394c1536ca9b54ce10000000a174cb4/3.6/en-US/frameset.htm [9.6.2021]

[49] z.B. mittels API-Schnittstellen: https://api.sap.com/package/ERPtoSuccessFactorsEmployeeCentralEmployeeandOrganizationalData?section=Overview [9.6.2021], SAP Integration Suite: https://help.sap.com/doc/e50e61e7b66c4b60ae5e88c00c01486a/sap.cp.integration.suite/en-US/FSD_IntegrationSuite.pdf [9.6.2021] oder via App Store: https://store.sap.com/dcp/en/search/?query=:relevance:category:hr-and-people-engagement [9.6.2021]

[50] https://help.sap.com/viewer/3f4d245122434203bcfab31f48aafaba/2105/en-US/239561a13f384c1db45110b744130ec4.html [9.6.2021]

oft sehr weitgehende Daten über Dauer, Inhalt und Ergebnisse von Tätigkeiten. Aber auch eine rudimentäre Zeiterfassung von Arbeitsbeginn und -ende kann ihre Tücken haben. Eine Studie aus den USA hat 2018 gezeigt, dass bei allen 13 untersuchten Zeiterfassungssystemen die erfassten Zeiten laut Voreinstellung zum Nachteil der Beschäftigten gerundet werden (Tippett 2018). Ähnliches berichten Sandra Stern et al (2010) für österreichische Callcenter. Hier wird deutlich, dass Datenerfassung am Arbeitsplatz sowohl sehr genau und detailliert als auch ungenau bis fehlerhaft erfolgen kann – je nach Unternehmensinteresse.

5.4.2 Beurteilung von Beschäftigten – Eignung, Leistung, Zielvorgaben

Die digitale Beurteilung von ArbeitnehmerInnen beginnt beim sogenannten „Recruiting", also bei der Auswahl von BewerberInnen bei einer Neueinstellung – von der Vorsortierung von Bewerbungen und Lebensläufen über Leistungs- und Persönlichkeitstests bis zur Dokumentation von Bewerbungsgesprächen (vgl. Bogen und Rieke 2018). Dies ist nicht Gegenstand der vorliegenden Studie. Die aus dem Bewerbungsprozess stammenden Daten über Ausbildung, beruflichen Vorerfahrungen, Fähigkeiten und Kompetenzen werden in zeitgenössischen Personalverwaltungssystemen aber auch für die **Beurteilung der Eignung** in laufenden Arbeitsverhältnissen eingesetzt – etwa bei der Auswahl von Beschäftigten für Projekte, Beförderungen oder betriebliche Weiterbildung.[51] In SuccessFactors können quantitative Bewertungen für Fähigkeiten und Kompetenzen von ArbeitnehmerInnen als „Ratings" gespeichert werden – sowohl auf Basis von Selbsteinschätzungen als auch von Einschätzungen durch Vorgesetzte.[52]

Zielvorgaben und Leistungsbeurteilungen. Darüber hinaus nutzen Unternehmen vielfältige Mechanismen, um die Arbeitstätigkeit von Beschäftigten zu beurteilen und damit schlussendlich zu steuern. Diese Beurteilungen erfolgen anhand definierter Kriterien – und oft anhand zuvor definierter Ziele, die entweder vorgegeben oder beim jährlichen MitarbeiterInnengespräch „vereinbart" werden – die sogenannte Zielvereinbarung. Unter dem Schlagwort „Management by Objectives" (MBO) wurden jährliche Beurteilungen anhand zuvor festgelegter Zielvorgaben schon vor Jahrzehnten eingesetzt. Dabei können quantitative oder qualitative Ziele vorgegeben werden, aber auch qualitative Ziele müssen in irgendeiner Form strukturiert und operationalisiert werden (vgl. Angerler et al 2028, S. 9, S. 22). Zielvorgaben und Beurteilungen sind inzwischen Teil von komplexen Prozessen einer unternehmensweiten Leistungssteuerung und -kontrolle. Dabei werden einzelne Beschäftigte genauso laufend bewertet wie Teams, Abteilungen, Standorte und ganze Belegschaften (vgl. Sommer 2014). Befragungen in dutzenden Ländern haben 2011 und 2013 gezeigt, dass international eine überwiegende Mehrheit der größeren Firmen individuelle Zielvorgaben und Beurteilungen von ArbeitnehmerInnen einsetzen und diese für Entscheidungen über Entlohnung, Weiterbildung und Beförderungen nutzen (Murphy 2020, S. 3).

Raten und ranken. Derartige Leistungsbeurteilungen haben eine lange Geschichte und werden oft dazu genutzt, Beschäftigte zu „raten" – also sie mit Zahlen zu bewerten – oder sie zu „ranken" – also sie zu reihen und damit untereinander zu vergleichen (vgl. Rosenkrantz 2019). Schon 2003 wurde von einer österreichischen Niederlassung eines multinationalen Konzerns berichtet, in dem ArbeitnehmerInnen durch Abteilungsleiter entlang von sieben Kriterien bewertet wurden – Fachkenntnis, Arbeitsquantität, Arbeitsqualität, Arbeitseinstellung und -leistung, Sorgfalt und Vertrauenswürdigkeit, Teamwork und (allenfalls) Führungsqualitäten, Lernbereitschaft und Anpassungsfähigkeit. Im Anschluss wurden die Beschäftigten in die Kategorien A („Top"), B („Solid"), C („Lower") und Z

[51] SAP (2014): Best Practices in Skills-Based Management. A Talent Management Component. Recommendations for Implementing a Successful Skills and Competency Management Program. Online: http://file.tuweia.cn/M00/3D/BC/CoPea1Vuoj6AEOdQAAYKgYwT9bQ061.pdf [9.6.2021]
[52] https://api.sap.com/api/ECSkillsManagement/resource [9.6.2021]

(„Lowest“) einsortiert. Für die Gruppe A waren Gehaltserhöhungen vorgesehen, für die Gruppen B und C Fördermaßnahmen bzw. Gehaltskürzungen in Form von Vertragsänderungen oder Änderungskündigungen. Die „untersten 5%“ in der Gruppe Z sollten gekündigt werden. Technisch haben dabei die Abteilungsleiter mit Hilfe von Excel Ranglisten für ihre Teams erstellt und dann via E-Mail an die Zentrale geschickt (vgl. Reissner 2003).

Zeitgenössische Personalverwaltungssysteme haben derartige Prozesse digitalisiert, vereinheitlicht und in den Dienst strategischer Unternehmensziele gestellt. Deren Module für „Performance Management“ bilden heute nicht nur jeden Schritt in diesen Prozessen digital ab und speichern dabei jedes Detail, sondern formen, strukturieren und verändern derartiger Personalprozesse in Unternehmen oft von Grund auf (vgl. Sommer 2014).

5.4.3 Umfassende Bewertungssysteme – SAP SuccessFactors, Workday, Zalando

Der Einsatz von Personalverwaltungssoftware wie SAP SuccessFactors oder Workday führt bei Unternehmen im deutschen Sprachraum oft dazu, dass zum allerersten Mal derart umfassende und integrierte digitale Bewertungssysteme eingeführt werden. Die unternehmensweite Personalsteuerung erfolgt ab diesem Zeitpunkt entlang eines jährlichen Fahrplans – bestimmt durch Kennzahlen, digital strukturierte und dokumentierte Gespräche, Zielvorgaben und Beurteilungen (vgl. Sommer 2018).

Mit Hilfe von SuccessFactors können Bewertungsprozesse umgesetzt werden, bei denen die Beurteilung sowohl durch die Beschäftigten selbst als auch durch Vorgesetzte erfolgt (ebd.). Diese Beurteilungen werden mittels Online-Fragebögen strukturiert (vgl. SAP 2018) und beziehen neben dem Grad der Erreichung vordefinierter Ziele auch die Bewertung von beruflichen Kompetenzen sowie persönlichen Stärken und Schwächen ein – etwa der „Teamfähigkeit“ oder der „Kundenorientierung“ (Sommer 2018). Vorgesetzte können auch das „Potenzial“ einschätzen – also die Frage beantworten, ob ArbeitnehmerInnen für eine höher qualifizierte Position oder eine Führungsaufgabe in Frage kommen. Dazu kann das Abwanderungsrisiko eingeschätzt werden – also die Frage, wie unproblematisch oder schwerwiegend ein Fortgang einer Person wäre und ob Maßnahmen ergriffen werden müssen, um die Person zu halten. Auch die Bereitschaft, andere Positionen im Betrieb zu übernehmen oder in eine Niederlassung im Ausland zu wechseln, kann beurteilt werden (vgl. Sommer 2014).

Gesamtnoten für Beschäftigte. Alle Einzelaspekte können am Ende zu einer Gesamtnote zusammengefasst werden, die die Belegschaft zum Beispiel auf einer fünfstufigen Skala kategorisiert und sortiert – von „bringt außergewöhnliche Leistungen“ über „erfüllt die Erwartungen“ bis „erfüllt nicht die Erwartungen“ (Sommer 2014). Diese Note kann entweder mathematisch vom System berechnet oder durch Vorgesetzte vergeben werden (vgl. Sommer 2018). Ob solche Ratings beim Einsatz von SuccessFactors in einem Betrieb überhaupt verwendet werden, wie sie benannt werden und wie der ganze Bewertungsprozess generell verläuft, ist anpassbar. Für Beschäftigte, deren Leistung als zu niedrig eingeschätzt wird, schlägt SAP selbst etwa auch Gruppenbezeichnungen wie „Struggling“, „Serious Concern“ oder „Seriously Underperforming“ vor (SAP 2017, S. 26).

SuccessFactors verspricht, Unternehmen dabei zu helfen, Leistungsbeurteilungen zu quantifizieren und damit **vergleichbar** zu machen. Führungskräfte können sich die Werte für Teams grafisch darstellen lassen (vgl. SAP 2018). Auch Beurteilungsraster, in denen ArbeitnehmerInnen entlang der zwei Achsen „Potenzial“ und „Leistung“ eingeordnet werden, stehen zur Verfügung. Beschäftigte, bei denen sowohl Potenzial als auch Leistung niedrig eingeschätzt werden, werden im Raster links unten dargestellt, die „High Performer“ mit hohem Potenzial rechts oben (Sommer 2018). Workday bietet ähnliche Funktionen (vgl. Sommer 2017). Aus Beschäftigtensicht stellen sich hier viele Fragen: Wie wirken sich diese Bewertungen auf Gehälter, Bonuszahlungen und Aufstiegsmöglichkeiten aus?

Wer bekommt welche Angebote oder Verpflichtungen für welche Schulungsmaßnahmen? Und was geschieht mit denjenigen, die niedrig bewertet werden? Wolfgang Däubler (2017, S. 284) beschreibt, wie ein derartiges System für die Gruppe der am schlechtesten bewerteten Beschäftigten empfiehlt, das Arbeitsverhältnis zu beenden.

Stacked Ranking und 360 Grad Feedback. SuccessFactors bietet auch Funktionen zum sogenannten „Stacked Ranking" (SAP 2018). Dabei bekommen Führungskräfte zum Beispiel die fixe Vorgabe, dass zwingend 10% der Beschäftigten mit dem niedrigsten Rating bewertet werden müssen und maximal 20% mit dem höchsten. Diese vielkritisierte Art der Leistungsbewertung wurde bereits in den 1980ern vom globalen Industriekonzern General Electric propagiert, der damals offen formuliert hat, dass 10% der schlechtesten „Performer" zur Kündigung vorgesehen seien (vgl. Rosenkrantz 2019). Auch das sogenannte „360 Grad Feedback" bzw. „Multi-Rater-Feedback" wird von SuccessFactors unterstützt. Dabei fließen nicht nur Selbsteinschätzungen und Beurteilungen von Führungskräften ein, sondern auch Bewertungen von „Peers" – also von KollegInnen im Team auf gleicher Hierachie-Ebene – oder von externen Parteien wie KundInnen des Unternehmens. Die Beurteilungen können dabei sowohl quantitative als auch qualitative Daten einbeziehen (SAP 2018). Ulrich Bröckling bezeichnet dieses Prinzip – mit Wurzeln im „Rundgespräch" zur Auswahl von Offiziersanwärtern in der deutschen Wehrmacht (Staab und Geschke 2019, S. 16), der Psychologie der Gruppendynamik und vielleicht auch in den „Kritik-und-Selbstkritik-Ritualen" im Realsozialismus – als „demokratisiertes Panopticon" (Bröckling 2003).

Während diese Art der Rundum-Bewertung zumindest im deutschen Sprachraum bislang hauptsächlich für Führungskräfte eingesetzt wurde, hat der Onlinehandels-Konzern Zalando die Einbeziehung von gegenseitigen Bewertungen zwischen KollegInnen auf alle Beschäftigten ausgeweitet. Wie die Zusammenfassung der Studie von Staab und Geschke (2020) in Abschnitt 7.2 zeigt, sortiert Zalando seit 2017 mehrere tausend Beschäftigte im Bürobereich auf Basis eines umfassenden Prozesses, der laufende **Peer-Ratings** zwischen KollegInnen beinhaltet, in drei Leistungsgruppen von niedrig über mittel bis hoch. Laut einem internen Handbuch wird das System für Entscheidungen über Gehaltserhöhungen und Beförderungen eingesetzt. Zudem werden ArbeitnehmerInnen darüber informiert, ob sie die „Erwartungen und Anforderungen" erfüllen oder „ob eine Leistungsverbesserung erforderlich" sei.

System der totalen Kontrolle? Beschäftigte nehmen das System bei Zalando als „System der totalen Kontrolle" wahr. Staab und Geschke sehen es als intransparentes Kontrollinstrument, das innerbetriebliche Konkurrenz und Leistungsdruck verstärke, Solidarität unterminiere, potenziell zu Willkür führe sowie negative Auswirkungen auf Betriebsklima und Arbeitsqualität haben könne. Durch die gegenseitigen Bewertungen werde betriebliche Kontrolle verschleiert. Das System würde als objektives Messverfahren dargestellt, sei aber einseitig im betrieblichen Interesse gestaltet und verzerre damit die Ergebnisse. Die systematische Verknappung positiver Bewertungen diene etwa der Kostensenkung und Lohnrepression. Auch aus betriebswirtschaftlicher Sicht gibt es Zweifel an der Effektivität und Sinnhaftigkeit derartiger Kontrollsystems – nicht nur wegen der zahlreichen Nebenwirkungen (Staab und Geschke 2020, S. 58f). In der wissenschaftlichen Literatur wird bezweifelt, ob sie das Versprechen einer Leistungssteigerung der Belegschaft überhaupt erfüllen (vgl. Murphy 2020, S. 3). Einige prominente Konzerne haben sich wieder davon wegbewegt. Bei einer Mehrheit großer Firmen werden sie jedoch weiter eingesetzt oder weiterentwickelt (ebd.). Die Berliner Datenschutzbehörde warnt davor, dass derartige Systeme einen „permanenten Überwachungsdruck und Stress" erzeugen können, da Beschäftigte jederzeit damit rechnen müssen, dass ihr Verhalten oder Begegnungen mit KollegInnen in künftige Bewertungen einfließen könnte (BInBDI 2021, S. 123-126).

Die traditionell halbjährlichen oder jährlichen Beurteilungszyklen werden seit einigen Jahren manchmal durch **hochfrequente Echtzeit-Bewertungen** ergänzt, bei denen Beschäftigte kontinuierlich die tägliche Zusammenarbeit mit KollegInnen mittels Smartphone-App bewerten sollen – oft ohne viel Kontext und in Form einer Vergabe von

einem bis fünf Sternen (Staab und Geschke 2019, Wright 2015). Laufende Echtzeit-Bewertungen sind Teil des Systems von Zalando (vgl. Abschnitt 7.2). Auch Workday[53] und SuccessFactors[54] bieten entsprechende Funktionen. Das „Continuous Performance Managment" von SuccessFactors bietet neben Echtzeit-Bewertungen weitere Funktionen, die eine laufende Steuerung, Aufzeichnung und Kontrolle von Zielen, Arbeitsaktivitäten und Ergebnissen ermöglichen[55] und wöchentliche Gespräche mit Vorgesetzten vorschlagen[56].

5.4.4 Bewertungen durch KundInnen in Plattformarbeit und darüber hinaus

Viele der im vorangehenden Abschnitt beschriebenen Beurteilungspraktiken knüpfen an die Produktbewertungen im kommerziellen Internet an. Insbesondere die Bewertung von Dienstleistungen im Netz geht schnell nahtlos in eine Bewertung der DienstleisterInnen als Person über – von VerkäuferInnen auf eBay bis zu VermieterInnen auf AirBnb. Neben Bewertungsplattformen für Restaurants werden inzwischen auch Rating-Systeme für einzelne KellnerInnen angeboten. In der **Plattformarbeit** können KundInnen fast jede Arbeitstätigkeit und damit die jeweiligen Beschäftigten bewerten. Sinkt der Score von FahrerInnen bei Uber unter einen bestimmten Wert, wird der Account deaktiviert – eine automatisierte Form der Kündigung (vgl. Besner 2018; Pasquale 2019).

Die Bewertungen durch KundInnen beschränkt sich aber nicht auf den Bereich der Plattformarbeit. Auch die VerkäuferInnen in den österreichischen Geschäften von Apple oder Nike können nach dem Einkauf von KundInnen bewertet werden (vgl. Sulzbacher 2020). **Rückmeldungen von KundInnen** spielen generell in vielen Bereichen der Arbeitswelt eine große Rolle für die Bewertung von ArbeitnehmerInnen – von der „Kundenzufriedenheit" bei Tätigkeiten in Verkauf oder Callcenter (vgl. Abschnitte 5.3.5 und 5.3.6) bis zur Einbeziehung von Bewertungen durch FirmenkundInnen beim 360 Grad Feedback (vgl. Abschnitt 5.4.3). Auch Daten, die von ERP- oder MES-Systemen im Rahmen der Qualitätssicherung erfasst werden, können potenziell zur Bewertung von Beschäftigten eingesetzt werden (vgl. Abschnitte 5.3.1 und 5.3.2).

5.4.5 Leistungsbewertung mit Daten über Verhalten und Arbeitstätigkeiten

Neben Einschätzungen über ArbeitnehmerInnen durch – mehr oder weniger subjektive – Beurteilungen durch Vorgesetzte, KollegInnen oder KundInnen können auch viele andere Daten über Arbeitstätigkeiten und Verhaltensweisen zur Leistungsbewertung eingesetzt werden. SAP schlägt in einer Broschüre zu SuccessFactors vor, „objektiv messbare" Leistungskriterien dort einzusetzen, wo es eine direkte Verbindung zwischen individuellen Arbeitstätigkeiten und „messbaren" Arbeitsergebnissen gibt und führt als Beispiele individuelle Verkaufsumsätze, produzierte Stückzahlen oder die Abwesenheit von Produktfehlern an (SAP 2017).

Viele betrieblich erfasste Daten eignen sich potenziell zur Leistungsbewertung. Einige Beispiele:

- Kassendaten in Einzelhandel und Gastronomie (siehe Abschnitt 6.2)
- Betriebs- und Maschinendaten aus Produktion und Qualitätssicherung (Abschnitt 5.3.2)
- Daten von Handscannern oder anderen tragbaren Geräten (Abschnitt 7.1)
- Daten über gefahrene Routen in Logistik und Zustellung (Abschnitt 5.3.8)
- Mobile Daten in Außendienst, Handwerk, technischer Wartung oder Pflege (Abschnitt 5.3.9)

[53] https://www.workday.com/content/dam/web/uk/documents/datasheets/datasheet-workday-talent-management-uk.pdf [14.6.2021]
[54] https://news.sap.com/2019/02/sap-successfactors-customers-employee-performance-management-approach/ [14.6.2021]
[55] https://www.sap.com/products/performance-goals/features.html [14.6.2021]
[56] https://blogs.sap.com/2017/04/26/test-the-continuous-performance-management-waters-before-you-take-the-plunge/ [14.6.2021]

- Protokolldaten von MS Office bis Dateibearbeitung bis Kommunikation in Microsoft 365 (Abschnitt 5.3.4)
- Daten aus Systemen für Projektmanagement und Aufgabenverwaltung (ebd.)
- Daten über Verkäufe und Kundenkontakte aus CRM-Systemen (Abschnitt 5.3.5)
- Daten über Gesprächsdauer, Anrufzahlen oder gar Gesprächsinhalte in Callcentern (Abschnitt 6.1)
- Daten über die Anmeldung in Räumen, an Maschinen oder Arbeitsplätzen (Abschnitt 5.5.1)
- Protokoll- und Ereignisdaten aus ERP- oder Workflow-Systemen (Abschnitte 5.3.1, 5.3.4, 5.8.1)
- Daten aus invasiven neueren Systemen wie zur Vermessung von Arbeitsplatzbelegung mit Bewegungssensoren (Abschnitt 6.5.1), von Bewegungen und Interaktionen im Büro mit tragbaren Geräten (Abschnitt 6.6), von Tippverhalten und Mausbewegungen (Abschnitt 6.7.3) oder von Bewegungsmustern und Kundenkontakten mittels automatisierter Videoanalyse im Einzelhandel (Abschnitt 6.2.3)

Alle diese Daten können potenziell in Personalverwaltungssystemen eingesetzt, aber auch unabhängig davon zur Leistungs- und Verhaltenskontrolle genutzt werden. Wolfgang Däubler (2017, S. 51) spricht von **„verdeckten" Personalinformationssystemen**, die Daten über Arbeitsprozesse verarbeiten.

Wie das Fallbeispiel über die Logistikzentren von Amazon zeigt, geben manche dieser Systeme nicht nur Leistungsziele vor und ermöglichen weitreichende Auswertungen, sondern steuern und kontrollieren unmittelbar jeden einzelnen Arbeitsschritt und dessen vorgesehene Dauer in Sekunden (siehe Abschnitt 7.1). In den USA hat Disney in den Wäschereien eine Wandanzeige eingesetzt, die die Namen aller ArbeitnehmerInnen darstellt. Die Namen der Beschäftigten, die die vorgegebene Rate bewältigen, wurden in grün angezeigt. Wurde jemand langsamer, wechselte die Farbe auf gelb. War jemand zu langsam, wurde der Name in blinkendem Rot dargestellt. Auch dabei handelt es sich um ein System, das die Arbeitsleistung unmittelbar steuert und kontrolliert. Die Beschäftigten nannten es laut einer Gewerkschafterin die „elektronische Peitsche" (vgl. Gabrielle 2018).

Systeme zur Personalverwaltung sowie zur Steuerung und Kontrolle von Arbeitstätigkeiten können auch direkt miteinander verbunden sein. Das **Projektmanagement-Modul von Workday** verspricht etwa, die Erfüllung von Arbeitsaufgaben zu überwachen und die Qualität der Ergebnisse zu bewerten. Dabei können „Beschäftigtenprofile" über Erfahrungen, Fähigkeiten und Kompetenzen sowie Daten über Arbeitszeiten und Abwesenheiten aus der Personalverwaltung direkt im Projektmanagement-System genutzt werden, um Beschäftigte miteinander zu vergleichen, für Tätigkeiten auszuwählen oder sie gar automatisiert zuzuweisen.[57]

5.4.6 Negativbeurteilungen, Risiko-Scores und unerwünschte Verhaltensweisen

Neben der Beurteilung von Fähigkeiten, Kompetenzen und Leistung erfassen Personalverwaltungssysteme auch Informationen über Verfehlungen, Abmahnungen und andere disziplinarische Maßnahmen (vgl. Däubler 2017, S. 50). Dabei handelt es sich um Beurteilungen, die diejenigen Beschäftigte aussondern sollen, die mit sehr verschiedenen Arten von unerwünschtem Verhalten auffallen – von Fehlzeiten oder Verstößen gegen Unternehmensregeln bis zu kriminellen Handlungen. **Verfehlungen** können dabei zu Sanktionen bis hin zur Kündigung führen. Während Personalverwaltungssoftware meist nur Informationen über tatsächliche Verfehlungen dokumentiert, haben sich abseits davon in Bereichen wie Betrugserkennung oder IT-Sicherheit umfassende Bewertungssysteme entwickelt, die unerwünschtes Verhalten von ArbeitnehmerInnen erkennen oder verhindern sollen.

[57] https://www.workday.com/content/dam/web/se/documents/datasheets/datasheet-workday-projects-se.pdf [14.6.2021]

Beschäftigte unter Pauschalverdacht. Das Fallbeispiel über Betrugsprävention im Handel zeigt, wie für Kassa-MitarbeiterInnen, deren Verhalten auf Basis von Kassendaten als verdächtig eingeschätzt wird, automatisiert Risiko-Scores berechnet werden (vgl. Abschnitt 6.2). Manche Systeme im Bereich IT-Sicherheit gehen noch viel weiter und werten exzessive Daten über den gesamten Arbeitsalltag aus, um permanent Risiko-Scores über Beschäftigte zu berechnen und möglichst schon im Vorhinein zu erkennen, ob sich eine Person möglicherweise in Zukunft unerwünscht verhalten wird. Ein führendes IT-Sicherheitssystem wertet nicht nur Daten über „negatives" Verhalten, mangelnde Kommunikation, Kündigungsabsichten oder finanzielle Schwierigkeiten aus, sondern verspricht sogar, verringerte Produktivität zu erkennen. Dabei können auch Daten aus der Zeiterfassung, Personalbeurteilungen und andere Daten aus Personalverwaltungssystemen wie Workday einbezogen werden (vgl. Abschnitt 6.4).

Auch andere datenschutz- und arbeitsrechtlich sensible Informationen werden manchmal als Negativbeurteilungen eingesetzt, wenn Beschäftigte etwa mit Auswertungslisten über Krankenstände unter Druck gesetzt werden – wie das interviewbasierte Fallbeispiel aus dem Sozial- und Gesundheitsbereich in Österreich zeigt (Abschnitt 8.2).

5.4.7 Belohnen und bestrafen – Steuerung mit Bewertungen und „Anreizen"

Beurteilungen und Bewertungen von Beschäftigten werden für unterschiedliche Zwecke eingesetzt und können unterschiedliche Auswirkungen auf einzelne ArbeitnehmerInnen, Gruppen und ganze Belegschaften haben. Sowohl die Bewertungsprozesse als auch die daraus folgenden betrieblichen Steuerungsmaßnahmen können heute über Personalverwaltungssysteme organisiert werden. Wie in den vorangehenden Abschnitten beschrieben, werden Bewertungen etwa für Entscheidungen über die Entlohnung oder zur Auswahl von Beschäftigten für Beförderungen, Versetzungen, Projekte, Weiterbildungs- und Fördermaßnahmen oder gar Kündigungen genutzt. Eine Kündigung der „untersten 10%" wurde früher offen propagiert – und wird das zum Teil noch immer, wie die automatisierten Verwarnungen und Kündigungen in den Logistikzentren von Amazon zeigen (vgl. Abschnitt 7.1).

Der Hinweis auf **Bestrafungen, Lohnkürzungen oder Kündigungen** wird heute aber zumeist vermieden. Es werden eher die positiven Aspekte hervorgehoben – von der Ermöglichung persönlicher Entwicklung, innerbetrieblicher Karriere und Weiterbildung bis zur Steigerung von „Motivation", „Engagement" und „Mitarbeitererlebnis".[58] Nichtsdestotrotz kann mit negativen bzw. nicht vollständig positiven Beurteilungen gezielt Druck ausgeübt werden – sogar ohne tatsächliche oder in Aussicht gestellte Maßnahmen. Um Druck auszuüben, kann schon der persönliche Hinweis eines Vorgesetzten ausreichen, nicht ganz „den Erwartungen" zu entsprechen. Dies geht bis hin zu unternehmensweiten Kampagnen gegen „Low Performer".

Der Druck verstärkt sich, wenn Leistungsbewertungen oder Ranglisten einer betriebsinternen Öffentlichkeit zugänglich gemacht werden – wenn also etwa Zahlen über individuelle Verkaufsumsätze, erledigte Anrufe im Callcenter oder Einstufungen aus dem Personalverwaltungssystem für Gruppen von ArbeitnehmerInnen oder gar für ganze Belegschaften sichtbar gemacht werden (vgl. Angerler et al 2018, S. 14). Das Ampelsystem in den Wäschereien von Disney in den USA, wo die individuelle Arbeitsleistung der Beschäftigten für alle sichtbar in der Farbe grün – oder bei zu langsamer Arbeit in gelb oder rot – dargestellt wurde, galt in den USA als „elektronische Peitsche" (vgl. Abschnitt 5.4.5). Ein Ampelsystem in einem österreichischen Callcenter stellt zwar nicht die Arbeitsleistung einzelner Beschäftigte dar, aber übt Druck auf das ganze Team aus. Wie alle im Team wissen, droht dem Callcenter-Betreiber eine Vertragsstrafe, wenn die Ampel die Farbe „rot" zeigt (siehe Abschnitt 7.1.4).

[58] Siehe z.B. https://www.sap.com/austria/products/human-resources-hcm/employee-experience-management.html [14.6.2021]

Im Rahmen der sogenannten **indirekten Steuerung** können auch Bewertungen und Beurteilungen, die sich nicht auf individuelle ArbeitnehmerInnen beziehen, sondern auf Teams, Abteilungen oder anderen Gruppen, zur Ausübung von Druck eingesetzt werden. Indirekte Steuerung setzt auf Eigenverantwortung und darauf, dass etwa ein Team selbstständig unter gegebenen Bedingungen bestimmte Ziele erreicht. Ein Beispiel dafür wären Beschäftigte auf einer rund um die Uhr zu besetzenden Station in einem Krankenhaus, die als Team selbstständig für Ersatz sorgen müssen, wenn ein Teammitglied krank wird, und sich dadurch gegenseitig unter Druck setzen, jederzeit einzuspringen. Auch in einem Team in der Softwareentwicklung, dass sich unternehmensintern zur Umsetzung eines Projekts mit einem bestimmten Budget, bestimmten Qualitätsstandards und einem bestimmten Fertigstellungstermin verpflichtet hat, werden sich die Teammitglieder gegenseitig unter Druck setzen, die vorgegebenen Ziele unter allen Umständen zu erreichen (vgl. Angerler et al 2018, S. 16ff). Digitale **Bewertungen von Teams oder anderen Gruppen** sind darum keineswegs grundsätzlich unproblematisch, sondern können Gruppendruck erzeugen und sich damit entscheidend auf die Machtverhältnisse zwischen Betrieb und Beschäftigten auswirken. Auch Bewertungen auf Gruppenebene sind deshalb ein Thema im betrieblichen Datenschutz. Wie Wolfgang Däubler (2017, S. 484f) ausführt, kann ein technisch geschaffener „Überwachungsdruck" bei Gruppen von ArbeitnehmerInnen, die gemeinschaftlich für Verhalten und Leistung verantwortlich sind, auf einzelne Mitglieder der Gruppe „durchschlagen".

Direkte und indirekte Formen der Steuerung können auch kombiniert werden. Ebenso können Bewertungen von individuellen Beschäftigten mit Bewertungen auf Gruppenebene kombiniert werden. Zudem können diese Prozesse sowohl im Personalverwaltungssystem als abseits davon stattfinden – oder systemübergreifend. Neben mittelfristig angelegten jährlichen oder halbjährlichen Zyklen mit Zielvereinbarungen, Beurteilungen und Maßnahmen können Leistungsvorgaben und -bewertungen auch direkt in den Arbeitsalltag integriert sein und laufend dazu genutzt werden, Arbeitstätigkeiten unmittelbar zu steuern zu kontrollieren (siehe Abschnitte 5.4.5 und 6.1).

Direkte **materielle Anreizmechanismen** in Form leistungs- oder erfolgsorientierter Vergütung zählen zu den klassischen Instrumenten „marktorientierter" betrieblicher Steuerung, bei der gezielt Konkurrenz zwischen den Beschäftigten geschaffen wird. Dabei hängt die Entlohnung zum Beispiel von Beurteilungen der Arbeitsleistung oder dem Erreichen vorab definierte Ziele ab. Neben individuellen Komponenten können dabei auch die von Teams, Abteilungen oder dem gesamten Unternehmen erreichten Ziele einfließen (vgl. Angerler et al 2018, S. 25). Eine Belohnung von Beschäftigten mit hoher Leistung kann natürlich umgekehrt immer auch als Benachteiligung derjenigen verstanden werden, die diese Vorteile nicht erhalten. Wenn ein Bewertungsschema mit Auswirkungen auf die Entlohnung so gestaltet ist, das gute Beurteilungen systematisch verknappt werden und damit eine Mehrheit der Beschäftigten stagnierende Löhne in Kauf nehmen müssen, kann es sogar als Instrument der systematischen Kostensenkung verstanden werden – wie die in Abschnitt 7.2 zusammengefasste Studie von Staab und Geschke (2020) herausgearbeitet hat. Der Anreizcharakter eines Leistungslohns kann durch weitere Belohnungsmechanismen ergänzt werden. Wie das Fallbeispiel in Abschnitt 8.5 zeigt, hängt der Verdienst der FahrerInnen bei einem Plattform-Zustelldienst zum Teil von den bewältigten Zustellaufträgen und Strecken ab. Beschäftigte, deren Arbeitsleistung am höchsten bewertet wird, bekommen Vorrechte bei der Auswahl der Schichten für die Folgewoche und können damit die Schichten mit den höchsten Bestellfrequenzen und damit den höchsten Verdienstmöglichkeiten wählen.

Neben direkten materiellen Anreizmechanismen wie Leistungslohn oder Erfolgs- und Vermögensbeteiligungen und indirekten materiellen Anreizmechanismen wie das Versprechen einer Beförderung oder die Drohung mit der Kündigung setzen Betriebe auch eine Vielfalt an **immateriellen Anreizmechanismen** ein, um Verhalten zu steuern, die Motivation zu verbessern und die Leistung zu steigern – von Anerkennung und Würdigung über die Verleihung von

Status bis zur Art, wie mit Beschäftigten umgegangen wird (vgl. Drumm 2008, S. 388f). Auch immaterielle Belohnungen können an Bewertungsprozesse gekoppelt werden. Bei der Übertragung von Spielmechaniken auf die Arbeitswelt, die seit einigen Jahren unter dem Schlagwort **Gamification** diskutiert wird, werden oft hauptsächlich immaterielle Anreizmechanismen eingesetzt (siehe Abschnitt 5.4.9).

5.4.8 „Talentmanagement" und betriebliche Weiterbildung

Das SAP-Personalverwaltungssystem SuccessFactors deckt unter dem Schlagwort „Talentmanagement" viele der im vorangehenden Abschnitt beschriebenen Maßnahmen ab, die Bewertungen mit Anreizmechanismen kombinieren. Neben Modulen für die Suche und Neueinstellung von Personal bietet SuccessFactors umfangreiche Funktionen für das „Leistungsmanagement" – von Zielvereinbarungen über Leistungsbeurteilungen bis zur Planung der Maßnahmen, die auf die Beurteilungen folgen – sowie für das „Vergütungsmanagement", das leistungsorientierte Gehaltsanpassungen und Bonusprogramme verwaltet. Im Rahmen des Moduls für Nachfolgeplanung und Personalentwicklung werden die Beurteilungen für Entscheidungen über Beförderungen und Versetzungen genutzt. Ein weiteres Modul deckt innerbetriebliche Weiterbildung und Qualifizierung ab.[59] Für die Entscheidung, wer welche Weiterbildungs- und Qualifizierungsmaßnahmen absolvieren darf oder muss, werden neben der Beurteilung von Leistung und Zielerreichung auch die umfassenden Datenbestände und Funktionen zur Einschätzung von Erfahrungen, Fähigkeiten und Kompetenzen von ArbeitnehmerInnen aus dem „**Skills Management**" von SuccessFactors genutzt. Auch für die Auswahl von Beschäftigten für Beförderungen, Versetzungen oder Projekte kann auf diese Beschäftigtenprofile zurückgegriffen werden.[60]

Betriebliche Aus- und Weiterbildung kann viele unterschiedliche Maßnahmen umfassen – vom Lernen am Arbeitsplatz und Wissenstransfer durch KollegInnen über Coaching durch Vorgesetzte oder externe BeraterInnen bis zu Seminaren, Kursen, fachspezifischen Zertifizierungen oder ganzen Ausbildungslehrgängen. Dabei kommen zunehmend Webinare, Videos, eLearning und interaktive digitale Formate zum Einsatz (vgl. Fritsch 2017, S. 8ff). Manchmal werden vollständige digitale Lernplattformen genutzt – sogenannte „Learning Management Systems" (LMS). Digitale Lernplattformen, die an Schulen und Universitäten eingesetzt werden, zeichnen heute oft jede Interaktion auf und bieten umfassende Analysemöglichkeiten – von der Beurteilung der Persönlichkeit und von Lernerfolgen bis zur Vorhersage zukünftiger Leistung (vgl. Sin und Muthu 2015). Im Betrieb können derartige Daten potenziell zur weiteren Beurteilung und Bewertung von Beschäftigten genutzt werden.

Personalverwaltungssysteme wie SuccessFactors oder Workday bieten umfangreiche **digitale Lernplattformen**, die verschiedene digitale Schulungsformate sowie Möglichkeiten der Beurteilung und Auswertung unterstützen. Neben personalisierten Schulungsangeboten oder der automatisierten Zuordnung zu Schulungen auf Basis von Beschäftigtenprofilen werden auch Funktionen zur Einbettung von Schulungs- und Weiterbildungsmaßnahmen in den laufenden Arbeitsalltag zur Verfügung gestellt.[61] Auch andere Hersteller wie etwa Centrical bieten Systeme für „Microlearning" an, die kontinuierlich kurze personalisierte Lerneinheiten in den Arbeitsalltag einbetten und dabei sogar Leistungsdaten einbeziehen.[62] Callcenter-Systeme integrieren regelmäßige Evaluierungen von Gesprächen

[59] https://www.sap.com/austria/products/human-resources-hcm/talent-management.html [14.6.2021]
[60] SAP (2014): Best Practices in Skills-Based Management. A Talent Management Component. Recommendations for Implementing a Successful Skills and Competency Management Program. Online: http://file.tuweia.cn/M00/3D/BC/CoPea1Vuoj6AEOdQAAYKgYwT9bQ061.pdf [9.6.2021]
[61] https://www.sap.com/austria/products/corporate-lms.html [14.6.2021], https://www.sap.com/austria/products/corporate-lms/features.html [14.6.2021], https://www.workday.com/en-us/products/talent-management/learning.html [14.6.2021]
[62] https://centrical.com/platform/personalized-microlearning/ [14.6.2021]

und laufende Schulungen in den Arbeitsalltag (siehe Abschnitt 6.1.4). In diesen Fällen verschwimmt die Grenze zwischen betrieblicher Weiterbildung und der Steuerung und Kontrolle von Arbeitstätigkeiten fast vollständig.

5.4.9 Verhaltenssteuerung und Leistungssteigerung mit „Gamification"

Unter dem Schlagwort „Gamification" wird seit einigen Jahren die Übertragung von Spielmechaniken auf die Arbeitswelt und andere Lebensbereiche diskutiert. In den meisten Fällen erinnern diese Mechaniken nicht direkt an das, was die meisten Menschen als Spiel kennen. Auf Grundlage bestimmter Regeln und kleiner Belohnungen oder Bestrafungen sollen Beschäftigte motiviert und deren Verhalten in eine bestimmte Richtung beeinflusst werden. Die Bandbreite dieser Mechaniken reicht von Wettbewerben, Punktesammelsystemen, Ranglisten und Bestenlisten über die Vergabe von Auszeichnungen oder Abzeichen („Badges") bis zu virtuellen Ökonomien, in denen erreichte Punkte, Erfolge oder sonstige Ziele in andere Belohnungen getauscht werden können. Die Ausnutzung der menschlichen Psychologie spielt dabei eine große Rolle (vgl. Ferreira et al 2017; Christl und Spiekermann 2016, S. 60f).

Leistungsvergleich mit Gamification. Wie das Fallbeispiel in Abschnitt 6.1.4 zeigt, bietet das Callcenter-System Genesys einige der oben beschriebenen Funktionen. Die Beschäftigten erhalten über den Arbeitstag hinweg für bestimmte Verhaltensweisen Punkte, unter anderem wenn sie die durchschnittliche Gesprächsdauer und Nachbearbeitungszeiten für Anrufe möglichst gering halten und dabei möglichst selten ein Gespräch an KollegInnen weiterleiten. Die Punktewerte werden im Vergleich zu den täglichen, wöchentlichen und monatlichen Bestwerten von KollegInnen dargestellt. Dazu gibt es Ranglisten und „Badges". Im Endeffekt handelt es sich dabei um einen permanenten Leistungsvergleich auf Basis von Kennzahlen. Schörpf et al (2018) berichten vom Einsatz eines Systems bei einem österreichischen Finanzdienstleistungsunternehmen, mit dem die Beschäftigten für jede abgeschlossene Fallbearbeitung Punkte bekommen – ein Punkt für schnell zu bearbeitende Fälle, drei Punkte für mittelschwere Fälle und sechs Punkte für jeden umständlichen Fall. Es gab eine zu erreichende Mindestpunktezahl. Der Betriebsrat ließ diese Form der Leistungskontrolle kurz nach der Einführung stoppen.

SuccessFactors bieten Funktionen, mit denen Beschäftigte Badges wie „Großartige Arbeit", „Teamplayer" oder schlicht „Danke" an KollegInnen, Vorgesetzte oder Untergebene vergeben können, die dann auf deren Beschäftigtenprofil sichtbar sind.[63] Andere Systeme wie Centrical bieten umfassende Funktionen für Gamification im Betrieb.[64] Dabei können kontinuierliche Ziele gesetzt werden, die auf Echtzeit-Leistungsdaten von ArbeitnehmerInnen zurückgreifen.[65] Auch im Bereich der betrieblichen Weiterbildung[66] oder zur Verbesserung von Arbeitssicherheit und –gesundheit (vgl. Abschnitt 6.7.1) gibt es Angebote, die derartige Spielmechanismen nutzen.

Neuer Begriff für alte Mechanismen? Aus einem etwas breiteren Blickwinkel könnten aber ohnehin viele Mechanismen am Arbeitplatz mit dem Begriff „Gamification" beschrieben werden – von Zielvereinbarungen mit Koppelung an die Entlohnung bis hin zu ganzen innerbetrieblichen Karrieren, die als Wettbewerb mit Anreizen und Belohnungen verstanden werden könnten. Auch ein Steuerungs- und Kontrollmechanismus wie das Ampelsystem, das in Echtzeit die Arbeitsleistung der Beschäftigten in den Wäschereien von Disney in den USA visualisiert (vgl. Abschnitt 5.4.5), könnte als „Gamification" gefasst werden. Ebenso die Punktebewertungen, die den MitarbeiterInnen der US-Supermarktkette Target die Geschwindigkeit ihrer Arbeitstätigkeit an der Kasse angezeigt haben (vgl.

[63] https://education.jhu.edu/wp-content/uploads/2020/02/Badges-in-Success-Factors.pdf [23.6.2021]
[64] https://centrical.com/platform/gamification/ [23.6.2021]
[65] https://centrical.com/platform/performance-management/ [23.6.2021]
[66] Siehe z.B. https://blogs.sap.com/2020/08/20/benefits-of-gamification-with-sap-successfactors-lms-make-learning-a-game/ [23.6.2021], https://centrical.com/platform/personalized-microlearning/ [23.6.2021]

Gabrielle 2018) oder die herabzählenden Sekunden, die Beschäftigten in den Logistikzentren von Amazon die noch zur Verfügung stehende Zeit für den aktuellen Arbeitsschritt anzeigen.

Spiele, die auch wie Spiele aussehen. Um diesem „Spiel" in den Lagerhallen von Amazon, das bei jedem Arbeitsschritt maximalen Druck ausübt, ein etwas freundlicheres Gesicht zu geben, bietet der Konzern den Beschäftigten in den USA seit kurzem an, mit Arbeitstätigkeiten wie dem holen, sortieren und ablegen von Produkten tatsächlich ein klassisches Computerspiel zu steuern (vgl. Abschnitt 7.1.5). Tatsächliche Spiele, die auch wie Spiele aussehen, werden im Betrieb darüber hinaus bei Persönlichkeitstests zur Beurteilung von bestehendem oder neu einzustellenden Personal eingesetzt.[67]

5.4.10 Umfragesoftware zwischen Personalbefragung und Leistungsbewertung

Meinungsumfragen im Betrieb sind eine weitere Funktion, die oft direkt in Personalverwaltungssoftware angesiedelt ist – oder in dessen Umfeld. Bei Mitarbeiterumfragen geht es zum Beispiel um die Analyse von Arbeitszufriedenheit, von Einstellungen, Werthaltungen oder persönlichen Zielen von Beschäftigten – oder um die Erfüllung gesetzlicher Verpflichtungen wie die Evaluierung psychischer Belastungen am Arbeitsplatz (vgl. Haslinger et al 2020, S. 58; Drumm 2018, S. 96f). Klassische Fragebögen auf Papier wurden längst durch Online-Formulare ergänzt, die jährliche MitarbeiterInnenbefragung durch kleinere Umfragen und hochfrequente „Feedback"-Mechanismen. Sobald die Eingaben bei Umfragen nicht vollständig anonymisiert sind, sondern einzelnen Personen zugerechnet werden können, können damit potenziell Beschäftigtenprofile erstellt werden. Eine mangelnde Freiwilligkeit der Teilnahme kann derartige Befragungen ebenfalls problematisch machen (Däubler 2017, S. 182f).

Qualtrics und Peakon. Die SAP-Tochterfirma Qualtrics bietet eine Plattform, die unzählige Funktionen für die Durchführung und Auswertung von Umfragen versammelt – und die an Personalverwaltungssysteme wie SAP SuccessFactors, Workday oder Oracle PeopleSoft angebunden werden kann.[68] Neben sogenannten „Pulse Surveys" für oftmalige schnelle Online-Befragungen stehen Umfragefunktionen für Schlüsselereignisse im Laufe einer Beschäftigung zur Verfügung – etwa anlässlich einer Neueinstellung, Weiterbildung, Gehaltsänderung oder bei der Auflösung des Dienstverhältnisses.[69] Auswertungsmöglichkeiten von der Analyse von Emotionen in Texteingabefeldern bis zur Verknüpfung der Umfragedaten mit betrieblichen Kennzahlen sollen Unternehmen dabei helfen, zu verstehen, was „ein Mitarbeiter über seinen Arbeitgeber und seine Rolle denkt" und mit „welchen Maßnahmen sie die Leistung der Mitarbeiter steigern können".[70] Die Software von Peakon, einer Tochterfirma von Workday, bietet ähnliche Funktionen.[71]

Derartige Anwendungen sind Beispiele für Systeme, die nicht mehr isoliert einem einzigen Zweck dienen, sondern die Nutzung der erfassten Daten und Auswertungsmöglichkeiten für viele verwandte Zwecke ermöglichen. Sowohl Qualtrics als auch Peakon beschränken sich nicht auf anonymisierte Umfragen, sondern bieten Funktionen zur „kontinuierlichen" **Leistungsbeurteilung**[b] bis zur Umsetzung von umfassenden Bewertungssystemen mit „360 Grad Feedback"[72] (siehe Abschnitt 5.4.3). Peakon berechnet für die Untergebenen einer Führungskraft einen „Engagement Score" und andere Kennzahlen, die sich sowohl auf die Leistung der Beschäftigten als auch auf die Leistung

[67] Siehe z.B. https://www.pymetrics.ai/ [23.6.2021]
[68] https://www.qualtrics.com/employee-experience/exit-interviews/ [23.6.2021]
[69] https://www.qualtrics.com/employee-experience/ [23.6.2021]
[70] https://www.qualtrics.com/de/employee-experience/einbindung-der-mitarbeiter [23.6.2021]
[71] https://peakon.com/solutions/employee-engagement/ [23.6.2021]
[72] https://www.qualtrics.com/uk/employee-experience/360-degree-feedback/ [23.6.2021]

der Führungskraft beziehen. Führungskräfte werden in Folge dazu angehalten, diese Kennzahlen zu verbessern. Sie sehen nicht nur, wie ihr Team im Vergleich zu anderen Teams im Unternehmen abschneidet, sondern auch Vergleichszahlen zu Teams in ähnlichen Branchen und Tätigkeitsbereichen. Zu diesem Zweck wertet Peakon **Beschäftigtendaten über Betriebe hinweg** aus.[73] Man bewirbt das Produkt als „weltweit größte[n] standardisierte[n] Datensatz aus Mitarbeiterfeedback", der auf fast 180 Millionen beantworteten Umfragen in Betrieben basiere.[74] Qualtrics wird nicht nur im Personalbereich eingesetzt, sondern auch für Umfragen in Vertrieb und Marketing. Unternehmen können damit „Daten aller […] Kunden und Mitarbeiter aus sämtlichen Interaktionen in einem zentralen System" erfassen.[75] Das Produkt dient also der Erfassung und Auswertung von Daten über Beschäftigte, aber auch über KundInnen des Betriebs – und damit **über mehrere Gruppen hinweg**. Qualtrics spricht von drei Milliarden Menschen, die jährlich mit Hilfe des Systems an Umfragen teilnehmen oder „Feedback" geben.[76]

Im Gegensatz zu Auswertungen auf Basis versteckt erfasster Daten über Kommunikation oder Verhalten ist bei Software für Online-Umfragen für ArbeitnehmerInnen klar ersichtlich, dass Daten erfasst werden. Nicht zwingend ersichtlich ist, ob die Eingaben einzelnen Personen zugeordnet werden, ob sie mit anderen personenbezogenen Daten im Betrieb verknüpft werden und welche Auswertungen durchgeführt werden.

Sowohl die die Workday-Umfragesoftware Peakon als auch das SAP-System Qualtrics bieten fortgeschrittene **KI-basierte Analysen** wie etwa die Prognose von Kündigungen „in Echtzeit"[77] oder die Benachrichtigung von Führungskräften, wenn für Beschäftigte Kündigungsabsichten vorhergesagt werden.[78]

5.4.11 Analysen mit KI? Vorhersage von Leistung, Eignung oder Kündigung

Neben vorwiegend auf menschlichen Beurteilungen beruhenden Einschätzungen durch Vorgesetzte oder andere Beschäftigte bieten Personalverwaltungssysteme immer öfter Funktionen, die große Personaldatenbestände analysieren und mit statistischen Modellen und anderen Methoden der künstlichen Intelligenz (KI) die künftige Leistung von Beschäftigten, deren Eignung für bestimmte Positionen oder deren Abwanderungsrisiko vorhersagen. Auch wer für Gehaltserhöhungen oder innerbetriebliche Fortbildung in Frage kommt, wird auf diese Weise bestimmt.

IBM behauptet, die **künftige Leistung** von ArbeitnehmerInnen mit Hilfe von KI mit einer Zuverlässigkeit von 96% vorhersagen zu können – und **Kündigungsabsichten** mit einer Zuverlässigkeit von 95%. Auch Fähigkeiten und Kompetenzen von Beschäftigten würden mittels KI eingeschätzt und deren künftige Entwicklung vorhergesagt, unter anderem auf Basis von Daten über erledigte Arbeitsaufgaben, absolvierte Schulungen und vergangene Beurteilungen. Führungskräfte nutzen diese Einschätzungen für Entscheidungen über Bonuszahlungen, Gehaltserhöhungen und Beförderungen. Dazu bietet IBM virtuelle Assistenten, die den Beschäftigten auf dieser Grundlage Schulungen und interne Jobausschreibungen empfehlen. IBM sagt, man habe die Technologie zur Vorhersage künftiger Leistung genutzt, um jene zehn Prozent der Belegschaft zu identifizieren, die unbedingt im Unternehmen gehalten werden müsse – und die darum neben Gehaltserhöhungen von spezieller Betreuung und gezieltem Rotieren durch unterschiedliche Arbeitsbereiche profitiere. Wenn als künftige HochleisterInnen eingeschätzte Personen speziell

[73] https://peakon.com/products/engage/bespoke-benchmarking/ [23.6.2021]
[74] https://peakon.com/de/ [23.6.2021]
[75] https://www.qualtrics.com/de/ [23.6.2021]
[76] https://www.qualtrics.com/de/offentlicher-sektor/ [23.6.2021]
[77] https://peakon.com/de/solutions/experience-and-retention/ [23.6.2021]
[78] https://www.qualtrics.com/employee-experience/exit-interviews/ [23.6.2021]

gefördert werden, könnte das natürlich eine selbsterfüllende Prophezeiung darstellen. IBM verkauft diese Analysetechnologien zum Teil auch an andere Unternehmen (vgl. Greenfield 2018; Rosenbaum 2019).

Für die von IBM behaupteten Prozentzahlen zur Zuverlässigkeit der Prognosen gibt es keine Belege. Die Bewerbung erfolgt offensichtlich im Rahmen des Marketings für Watson[79], der KI-Plattform von IBM, deren Versprechungen immer wieder umstritten waren.[80] Ein von IBM veröffentlichter Datensatz mit fiktiven Beschäftigtenprofilen[81] liefert Hinweise darauf, welche Daten das Unternehmen zur Vorhersage von Kündigungen und anderer Verhaltensweisen von ArbeitnehmerInnen nutzen könnte. Neben Alter, Geschlecht, Familienstand, Ausbildung, Position und Einkommen zählen dazu Variablen wie vergangene Leistungsbeurteilungen, die Dauer des Dienstverhältnisses, die Zahl der vorangegangenen Dienstverhältnisse oder die Entfernung zwischen Wohn- und Arbeitsort.

Das Personalverwaltungssystem **UltiPro** von Ultimate Kronos berechnet seit 2016 für einzelne ArbeitnehmerInnen Vorhersagen darüber, ob sie zukünftig zu den „High Performern" zählen könnten und ob sie das Unternehmen in den nächsten 12 Monaten verlassen werden. Die Prognosen werden auf Basis unterschiedlicher Personaldaten und statistischer Methoden monatlich neu berechnet und in Form von Scores, die Wahrscheinlichkeitswerte angeben, im Beschäftigtenprofil angezeigt. Sie werden auch für viele Jahre rückwirkend berechnet. Führungskräfte können benachrichtigt werden, wenn die Scores unter oder über bestimmte Werte fallen. Die datenbasierte Leistungsprognose soll laut Hersteller die jährliche Leistungsbeurteilung durch Vorgesetzte ergänzen und kann für Entscheidungen über Boni, Gehaltserhöhungen, Beförderungen, Versetzungen oder Förderungs- und Schulungsangebote genutzt werden. Auch das sogenannte „Engagement" von Beschäftigten wird individuell mit einem Score bewertet. Der Hersteller bewirbt diese Prognosefunktionen mit Schlagwörtern wie „Big Data", „Predictive Analytics" und künstlicher Intelligenz, macht aber keine näheren Angaben über Methodik und genutzte Daten.[82]

Auch **Workday** ermöglicht die Vorhersage von „Kündigungsrisiken", des künftigen Potenzials von Beschäftigten und die Identifikation von „at-risk performers" – also von ArbeitnehmerInnen, deren Leistung als ungenügend eingeschätzt wird – auf Basis umfassender Datenauswertungen mit Hilfe von „Machine Learning", also mit Technologien der künstlichen Intelligenz.[83] Darüber zeigt Workday Beschäftigten individuell zugeschnittene Empfehlungen für unternehmensintern ausgeschriebene Positionen sowie für zu entwickelnde Fähigkeiten und Kompetenzen an. Die Einschätzungen darüber, ob eine ausgeschriebene Position im Unternehmen zu einer Person passt, erfolgen ebenfalls mittels Machine Learning.[84] Viele dieser Funktionen haben potenziell weitreichende Auswirkungen auf ganze Erwerbsbiografien.

Wie das Fallbeispiel in Abschnitt 6.4 zeigt, treffen auch zeitgenössische **IT-Sicherheitssysteme** Einschätzungen über einzelne Beschäftigte mit Hilfe von KI. Auf Basis umfassender Daten über Datenzugriffe, Suchvorgänge, Website-Aufrufe, Kommunikation und andere Aktivitäten – und damit einer fast vollständigen Überwachung des Arbeitsalltags – sollen als ungewöhnlich oder riskant eingeschätzte Verhaltensweisen erkannt werden. Neben der

[79] https://www.ibm.com/watson/uk-en/talent/insights/ [23.6.2021]
[80] Siehe z.B. Strickland, Eliza (2019): How IBM Watson Overpromised and Underdelivered on AI Health Care. IEEE Spectrum, 2.4.2019. Online: https://spectrum.ieee.org/biomedical/diagnostics/how-ibm-watson-overpromised-and-underdelivered-on-ai-health-care
[81] http://inseaddataanalytics.github.io/INSEADAnalytics/groupprojects/January2018FBL/IBM_Attrition_VSS.html [23.6.2021]
[82] https://www.ultimatesoftware.com/Digital-Whitepaper/workforce-intelligence-at-your-fingertips [3.7.2021], http://ultimarketingweb.blob.core.windows.net/static/pdf/releasehighlights/ENT_UltiPro_2016_FYE_Highlights_FINAL.pdf [3.7.2021]
[83] https://www.workday.com/content/dam/web/en-us/documents/datasheets/datasheet-workday-talent-management.pdf [3.7.2021], https://www.workday.com/content/dam/web/en-us/documents/datasheets/datasheet-workday-professional-services-automation.pdf [3.7.2021]
[84] https://www.workday.com/en-us/products/talent-management/performance-optimization.html [3.7.2021], https://www.workday.com/content/dam/web/en-us/documents/datasheets/datasheet-workday-talent-management.pdf [3.7.2021]

Vorhersage möglicher Kündigungsabsichten wird versucht, zu erkennen, ob sich die „Produktivität“ von ArbeitnehmerInnen verringert hat, ob sie weniger als zuvor mit KollegInnen kommunizieren oder gar, ob sie privat in finanziellen Schwierigkeiten stecken. Wer sich ungewöhnlich verhält, landet auf einer Liste riskanter und speziell zu beobachtender Personen.

Einige US-Anbieter gehen über die im Betrieb erfasste Beschäftigtendaten hinaus und beziehen bei der Vorhersage von Kündigungsabsichten oder der Bewertung von Qualifikationen Informationen über **Socialmedia-Aktivitäten** und aus anderen Datenquellen außerhalb des Unternehmens mit ein – wie die Fallbeispiele in Abschnitt 6.9 zeigen.

5.4.12 Personalanalyse, Personalbedarfsplanung und Personaleinsatzplanung

Im Rahmen der Personalwirtschaft setzen Unternehmen unterschiedliche Methoden der Personalanalyse und -planung ein. Dabei werden Kosten ins Verhältnis zu betrieblichen Zielen, Erfordernissen und Ergebnissen gesetzt. Aus einer Analyse des **Personalbestands** – also von Kenntnissen, Fähigkeiten und Arbeitsleistungen der aktuellen Belegschaft – folgt die Planung des künftigen **Personalbedarfs** und Nicht-Bedarfs. Künftiger Bedarf soll durch die **Personalbeschaffung** – also durch Neueinstellungen – abgedeckt werden, die aus betrieblicher Sicht überflüssigen Stellen durch die sogenannte **Personalfreisetzung** abgebaut werden. Gleichzeitig wird im Rahmen der **Personalzuweisung** analysiert und geplant, welche Beschäftigten welche Arbeit verrichten sollen – mit sehr unterschiedlichen zeitlichen Horizonten. Dies reicht von der langfristigen Planung der Zuweisung zu bestimmten Positionen im Unternehmen oder zu Projekttätigkeiten bis zur tagesaktuellen Verteilung anwesender Beschäftigten auf Arbeitsbereiche – etwa auf Maschinen, Verkaufsabteilungen oder Baustellen (vgl. Drumm 2008, S. 195ff). Die Personalzuweisung wird auch unter dem Begriff des **Personaleinsatzes** diskutiert (vgl. Pilarski 2016). Alle diese Analyse- und Planungsvorgänge sowie die Entscheidungen, die in Folge getroffen werden, haben erhebliche Auswirkungen auf ArbeitnehmerInnen – auf deren Arbeitsalltag oder gar auf ganze Erwerbsbiografien.

Viele Funktionen der Personalanalyse und -planung werden von Personalverwaltungssystemen oder Software im Umfeld abgedeckt. Beschäftigtendaten spielen dabei eine wichtige Rolle. Eine zentrale Grundlage sind die in den vorangehenden Abschnitten beschriebenen Praktiken der Bewertung von Erfahrungen, Fähigkeiten und Kompetenzen von ArbeitnehmerInnen – von deren Arbeitsleistung, dem Grad der Zielerreichung oder dem eingeschätzten Potenzial. Auch mit den in Abschnitt 5.4.10 beschriebenen Systemen für Personalbefragungen werden Daten für die Analyse gesammelt. Die in Abschnitt 5.4.11 beschriebenen neuen Methoden zur Einschätzung und Vorhersage von Arbeitsleistung oder Eignung mittels künstlicher Intelligenz sind im Endeffekt nur die Fortsetzung einer langen Geschichte der Nutzung statistischer Methoden in der Personalplanung (vgl. Drumm 2008, S. 203). Heute wird Personalanalyse unter Schlagwörtern wie **Workforce Analytics, People Analytics** oder **HR Analytics** vermarket (vgl. Huselid 2018). Kennzahlen spielen dabei eine große Rolle – von Leistungskennzahlen, Umsätzen und Kosten pro MitarbeiterIn (vgl. Kavanagh und Johnson 2018, S. 553ff) bis zur Stimmung im Betrieb (vgl. Abschnitt 5.4.10). Das SAP-Personalverwaltungssystem SuccessFactors bietet umfassende Funktionen zur Personalanalyse[85] und Planung[86]. Workday bietet neben Auswertungs- und Analysemöglichkeiten[87] Funktionen zur Personalplanung, die Szenarien simulieren und deren mögliche Auswirkungen vorhersagen.[88]

[85] https://www.sap.com/austria/products/workforce-analytics.html [6.7.2021]
[86] https://www.sap.com/austria/products/human-resources-hcm/workforce-planning-hr-analytics.html [6.7.2021]
[87] https://www.workday.com/de-de/products/human-capital-management/analytics-reporting.html [6.7.2021]
[88] https://www.workday.com/de-de/products/enterprise-planning/workforce-planning.html [6.7.2021]

Die Beschreibung eines Systems für Zeiterfassung und „Workforce Management" des deutschen Anbieters ATOSS zeigt, wie die strategische, taktische und operative Analyse und Planung des Personaleinsatzes ineinandergreifen – von langfristiger Personalplanung bis zur tagesaktuellen Schichtplanung. Das Modul zur **Personalbedarfsermittlung** soll dabei helfen, zu bestimmen, „welche Mitarbeiter mit welchen Qualifikationen zu welchen Kosten wo und wann zum Einsatz kommen sollen – pro Tag, pro Stunde oder im Idealfall minutengenau berechnet". Grundlage dafür sind „Prognosen des zukünftigen Arbeitsvolumens" auf Basis vergangener Daten wie „Umsätze, Kassenbons, Auftragsvolumen, Belegungsquote[n] im Krankenhaus oder getätigte Anrufe im Call Center". Ergebnis sei eine „minutengenaue bedarfsoptimierte **Personaleinsatzplanung**" mit dem Ziel einer „Optimierung der Personalkosten" und einer „Steigerung der Produktivität".[89] Mit Hilfe der **Kapazitätsplanung** soll der mittelfristige Personalbedarf bestimmt werden – unter Einbeziehung von Beschäftigtendaten über Qualifikationen und über „Abwesenheits- und Krankheitsraten".[90] Langfristig soll die **Personalstrukturoptimierung** dabei helfen, pro „Standort, Filiale oder Abteilung" eine „optimale Anzahl von Vollzeit-, Teilzeit- und Aushilfskräften mit unterschiedlichen Verfügbarkeiten, Arbeitszeitmodellen und Qualifikationen" zu bestimmen.[91]

Mit dem Modul zur **Personaleinsatzsteuerung** sollen hingegen tagesaktuelle Schwankungen beim Personalbedarf berücksichtigt und sowohl Personalengpässe als auch „unproduktive[n] Arbeitszeiten" vermieden werden. Für die kurzfristige Einsatzplanung werden Informationen zu Arbeitszeiten, Qualifikationen und andere Beschäftigtendaten einbezogen. Bei krankheitsbedingten Ausfällen werden automatisch „verfügbare und geeignete" MitarbeiterInnen als Ersatz vorgeschlagen. Diese erhalten „Schichtangebote" via Smartphone. Das System unterstützt auch „das Verleihen von Mitarbeitern sowie den Einsatz von Springern und Poolmitarbeitern".[92]

Man könnte Systeme, die anhand von Vorhersagen zur erwarteten Arbeitsauslastung teil- oder vollautomatisierte Dienst- und Schichtpläne erstellen, wohl als eine Form des **automatisierten Managements** fassen. Bei Einzelhandelsketten international seit den 1990er Jahren üblich haben sich derartige Technologien in unterschiedlichste Branchen ausgebreitet. Sie können dazu genutzt werden, für jeden Zeitabschnitt am Tag das minimal benötigte Personal einzusetzen oder etwas weniger – oder zur Steuerung einer großen Zahl an flexibel verfügbaren Arbeitskräften (vgl. Dzieza 2020; Williams et al 2018). Hier geht Personalanalyse und -planung nahtlos in die im Abschnitt 5.3 beschriebenen Methoden zur Steuerung und Kontrolle von Arbeitstätigkeiten über. Die kurz- und längerfristige Koordination von Personaleinsatz mit dem anfallenden oder zu erwartenden Arbeitsvolumen erfolgt dabei nicht unbedingt durch die Personalabteilung. In der Produktion wird diese Aufgabe von Fertigungsmanagementsystemen übernommen (vgl. Abschnitt 5.3.2; Kurbel 2013, S. 194ff), in vielen Branchen ganz allgemein von ERP-Systemen (vgl. Abschnitt 5.3.1). Auch Projektmanagementsoftware (siehe Abschnitt 5.3.4) und andere branchen- und tätigkeitsspezifische Systeme koordinieren Personaleinsatz und Arbeitsvolumen.

Workday hingegen verbindet Personalverwaltung mit dem Finanz- und Projektmanagement. Dabei können im gleichen System sowohl Projekte geplant und gesteuert als auch sämtliche Funktionen des Personalverwaltungssystems

[89] https://www.atoss.com/de-de/workforce-management/personalbedarfsermittlung [6.7.2021]
[90] https://www.atoss.com/de-de/workforce-management/kapazitaetsplanung [6.7.2021]
[91] https://www.atoss.com/de-de/workforce-management/personalstrukturoptimierung [6.7.2021]
[92] https://www.atoss.com/de-de/workforce-management/personalsteuerung [6.7.2021]

genutzt werden. Die Zuweisung von Beschäftigten zu Arbeitstätigkeiten erfolgt auf Grundlage von Daten zu Verfügbarkeit, Kompetenzen und Leistung sowie von Vorhersagen zur Arbeitsauslastung im Projektverlauf.[93]

5.4.13 Weitere Funktionen von Personalverwaltungssystemen

Viele weitere Funktionen können in der Personalverwaltung und in entsprechenden datenverarbeitenden Systemen angesiedelt oder eng an diese angebunden sein. Dazu zählt etwa die Verwaltung und Überwachung von **Dienstreisen, Reisekosten** und anderen Ausgaben mit MitarbeiterInnen durch Software wie SAP Concur.[94]

Ein anderes Beispiel sind betriebliche **Gesundheitsprogramme** unter Einbeziehung von Fitness-Armbändern, die Schritte und andere Körperdaten erfassen. In den USA haben derartige Programme ganz massive Auswirkungen, da ArbeitgeberInnen oft direkt für die Krankenversicherung der Beschäftigten zuständig sind (vgl. Christl und Spiekermann 2016, S. 65ff). Dies ist im deutschsprachigen Raum nicht der Fall. Dennoch stellen sich auch hier Fragen in Bezug auf die Verarbeitung sensibler Gesundheitsdaten und Verhaltenssteuerung durch Unternehmen.[95]

5.5 Unterstützende Systeme für Infrastruktur und Verwaltung

Neben Software, die explizit Daten über Beschäftigte und ihre Arbeitstätigkeiten verarbeitet, sind in Betrieben viele Systeme zu finden, die zur Infrastruktur gehören und die Verwaltung unterstützen, dabei aber ebenfalls umfangreiche Daten erfassen, die potenziell auch für andere Zwecke genutzt können. Einige der in den folgenden Abschnitten beschriebenen Systeme wie die Flotten- und Fuhrparkverwaltung können natürlich genauso zur Kerntätigkeit eines Unternehmens gehören.

5.5.1 Zutrittskontrolle und Anmeldung bei Arbeitsplätzen, Geräten und Maschinen

Zutrittssysteme mit Schranken, Schleusen oder anderen Türsperren wie elektronische Schlösser sichern heute nicht nur den Haupteingang von betrieblichen Gebäuden ab, sondern oft auch den Zugang zu Innenräumen – von Liftanlagen, Büros und Besprechungsräumen bis zum Zutritt zu besonderen Bereichen wie Produktionshallen, Labors oder Rechenzentren. Mit der maschinenlesbaren **Magnet- oder Chipkarte**, auf denen Kennungen für einzelne Beschäftigte gespeichert sind, können die elektronischen Lesegeräte an Schleusen oder Türen erkennen, ob eine Person zutrittsberechtigt ist oder nicht (vgl. Haslinger et al 2020, S. 44; Frühbrodt 2018, S. 6).

Zutrittssysteme sollen einerseits sicherstellen, dass nur berechtigte Personen Zugang zu Gebäuden oder Räumlichkeiten haben. Für diesen Zweck ist es leicht möglich, das technisch so zu lösen, dass nur überprüft wird, *ob* eine Person zutrittsberechtigt ist, dabei aber nicht zu erfassen oder zu speichern, wer diese Person ist oder wann der Zutritt erfolgt. Daten über die Identität und den Zeitpunkt der Kartennutzung werden aber oft zumindest für die **elektronische Zeiterfassung** verwendet – also um Arbeitsbeginn und -ende aufzuzeichnen. Sind viele Bereiche im Innenraum mit Lesegeräten ausgestattet, können aus den Protokolldaten potenziell Profile über Bewegungen oder Arbeitsabläufe abgeleitet werden (ebd.). Wenn für Pausen ein durch das Zutrittssystem geschützter Bereich betreten

[93] https://www.workday.com/content/dam/web/en-us/documents/datasheets/datasheet-workday-professional-services-automation.pdf [6.7.2021], https://www.workday.com/content/dam/web/en-us/documents/datasheets/datasheet-workday-projects.pdf [6.7.2021]
[94] https://www.concur.de/ [6.7.2021]
[95] Urgancioglu, Kemal (2016): Betriebliches Gesundheitsmanagement mit Wearables, 7.1.2016. Online: https://wirtschaftsrecht-news.de/2016/01/betriebliches-gesundheitsmanagement-mit-wearables/

oder verlassen werden muss oder die gleiche Karte auch für die Essensabrechnung in der Kantine genutzt wird, fallen potenziell auch Verhaltensdaten an, die sich nicht auf die Arbeit beziehen (vgl. Däubler 2017, S. 480).

Neben dem Zutritt zu Räumlichkeiten wird oft die **Anmeldung an genutzten Geräten** erfasst – vom Rechner am Arbeitsplatz über Drucker, Scanner und Kopierer (vgl. Haslinger et al 2020, S. 48) bis zu Maschinen in der Produktion (vgl. Kurbel 2013, S. 200ff). **Ausgabeautomaten** für Schutzausrüstung, Werkzeuge und viele andere Ge- und Verbrauchsartikel erfassen bisweilen jede Entnahme personenbezogen und mit Zeitpunkt.[96] Daten zur Anmeldung an Geräten oder zur Materialverwendung eignen sich für weitergehende Auswertungen über Arbeitstätigkeiten.

Neben Magnet- oder Chipkarten können für die Authentifizierung oder Identifikation auch Passwörter genutzt werden – oder **biometrische Merkmale** wie Fingerabdrücke, Gesicht, Iris oder Stimme (vgl. Frühbrodt 2018, S. 6f).

5.5.2 Verwaltung von Gebäuden, Räumen, Fahrzeugen und anderen Betriebsmitteln

Betriebliche Gebäude und Räume werden zunehmend zu digital vernetzten Umgebungen. Eine große Bandbreite an Technologien unterstützt deren Verwaltung und die Optimierung der Kosten für deren Nutzung. Im Rahmen des **Facility Managements** werden unterschiedlichste Vorgänge und Zustände gesteuert und überwacht – von Instandhaltung, Reinigung und Müllentsorgung über Klimatisierung, Temperatur, Luftfeuchtigkeit, Beleuchtung und andere Umgebungsbedingungen bis zu Sicherheitsmaßnahmen wie Rauch- und Feuermelder, Alarmanlagen, Bewegungsmelder oder Überwachungskameras. Neben der Zuweisung und Verwaltung von Arbeitsplätzen, Besprechungsräumen oder Parkplätzen wird die Anschaffung und Nutzung von Einrichtungsgegenständen, Büromöbeln, Maschinen, Geräten, Werkzeugen, Fahrzeugen und anderer Betriebsmittel überwacht – von Kaffeemaschinen, Druckern, Laborutensilien oder Gabelstaplern bis hin zur „Smart Factory“[97], in der beinahe jede Aktivität in der Produktionshalle erfasst wird (vgl. de Barros Lima 2020).

Auch Systeme für die **Buchung von Besprechungsräumen**[98] und Arbeitsplätzen[99] oder für die Betreuung und Überwachung externer BesucherInnen[100] zeichnen umfassende Verhaltensdaten auf.

Neben der im vorangehenden Abschnitt beschriebenen Erfassung von Verhaltensweisen durch Zutrittskontrollsysteme oder durch die aktive Anmeldung an Geräten können Verhaltensdaten auch **passiv und versteckt aufgezeichnet** werden. Abschnitt 6.5.1 beschreibt ein besonders invasives Fallbeispiel eines Systems, das mit unter Tischen montierten vernetzten Bewegungsmeldern die Anwesenheit auf Arbeitsplätzen überwacht. In die Geräte eingebaute Sensoren messen außerdem Raumtemperatur, Luftqualität, Luftdruck, Geräuschpegel, Lichtintensität und Feuchtigkeit. Als Ziele werden Energieeinsparung, effizientere Raumnutzung und Kostensenkung hervorgehoben. Gleichzeitig kann die Anwesenheit von Beschäftigten an Tischen auf individueller Ebene dargestellt und ausgewertet werden. Ein weiteres Produkt geht über die Nutzung stationärer Sensoren hinaus und ortet die Laptops, Tablets und Smartphones von Beschäftigten mit Hilfe von WLAN-Daten (vgl. Abschnitt 6.5.2).

[96] Siehe z.B. https://www.wuerth-industrie.com/web/de/wuerthindustrie/cteile_management/materialwirtschaft_automatenversorgung/warum_automatenversorgung.php [6.7.2021]
[97] Siehe auch Abschnitte 5.3.2 und 8.3
[98] Siehe z.B. https://envoy.com/products/conference-room-scheduling-software/ [6.7.2021]
[99] Siehe z.B. https://envoy.com/products/hot-desk-booking-software/ [6.7.2021]
[100] Siehe z.B. https://envoy.com/products/visitor-management-system/ [6.7.2021]

Die Nutzung – und bisweilen auch der Standort – beweglicher Betriebsmittel wird mit dem sogenannten **Asset Tracking** überwacht – von Reinigungsgeräten[101] oder Servierwagen in Hotels[102] über Baumaschinen und Schuttcontainer[103] bis zu medizinischen Geräten in Krankenhäusern.[104] Wie Abschnitt 5.3.8 zeigt, zeichnen auch Systeme für die **Flotten- oder Fuhrparkverwaltung** oder **elektronische Fahrtenbücher** eine Vielzahl von Daten über die Nutzung und die Standorte von Fahrzeugen auf.

5.5.3 IT-Infrastruktur und Verwaltung, Fernwartung, Authentifizierung und Berechtigungen

Welche IT-Infrastruktur ein Unternehmen betreibt und wie diese verwaltet und gewartet wird, variiert je nach Branche und betrieblichen Gegebenheiten. In vielen Fällen ist die IT-Infrastruktur heute entscheidende Grundlage für beinahe jegliche Aktivität im Unternehmen. Verwaltet werden Netzwerkinfrastruktur und Rechenzentren, Basisdienste wie Internetzugang, Telefonie und E-Mail, die Software auf den stationären und mobilen Geräten der Beschäftigten sowie alle in der vorliegenden Studie beschriebenen Softwaresysteme – egal ob diese vor Ort, in der Zentrale oder in der Cloud betrieben werden. Auch viele anderen vernetzten Geräte werden von der IT-Abteilung betrieben, gewartet und überwacht – von Gebäudetechnologie und Fuhrpark bis zu Produktionsanlagen.[105]

Rein technisch ermöglicht die betriebliche IT-Infrastruktur einen weitreichenden Zugriff auf Daten über Arbeitsalltag und Verhaltensweisen von ArbeitnehmerInnen. Wer Zugang zum gesamten Datenverkehr auf Netzwerkebene hat, hat umfassende Kontrolle über **Web-Nutzung, E-Mail-Kommunikation und andere Online-Dienste**. Viele dieser Daten werden protokolliert. Selbst wenn der Datenverkehr verschlüsselt erfolgt, kann er von zeitgenössischen **IT-Sicherheitssystemen** ausgewertet werden. Diese haben oft auch Zugriff auf die Endgeräte und die darauf genutzte Software (siehe Abschnitt 5.6.3).

Betrieblich genutzte Endgeräte wie PCs, Laptops, Smartphones oder Tablets und die darauf installierte Software werden meist vollständig via **Fernwartung** von der IT-Abteilung kontrolliert. Da die Geräte mittels Kennnummern einzelnen Beschäftigten zugeordnet sind, entsteht dabei eine Vielzahl an personenbezogenen Daten (vgl. Simpson und Foltz 2018). Dies betrifft selbstverständlich auch viele andere vernetzte Geräte von der Supermarktkasse bis zur Maschine in der Produktion.[106] Software für **Mobile Device Management (MDM)** oder **Enterprise Mobility Management (EMM)** verwaltet neben Firmengeräten auch private Laptops oder Smartphones, die betrieblich genutzt werden – Stichwort „Bring your own Device“ (BYOD). Zu den möglichen Funktionen dieser Systeme zählt die Installation von Programmen und Apps aus der Ferne, der Zugriff auf die auf dem Gerät gespeicherte Dateien oder gar auf den Standort des Geräts (vgl. Yamin und Katt 2019).

Wer tatsächlich die faktische Kontrolle über diese Systeme hat, hängt davon ab, ob sie von der unternehmensinternen IT-Abteilung, von einer zentralisierten Konzern-IT oder etwa von externen IT-Dienstleistungsfirmen betreut

[101] Dax, Patrick (2016): Internet der Dinge: Wie sich Kärcher neu erfunden hat. Futurezone, 7.6.2016. Online: https://futurezone.at/b2b/internet-der-dinge-wie-sich-kaercher-neu-erfunden-hat/202.474.483
[102] https://www.axxind.com/smarthotel/traytracker/ [6.7.2021]
[103] https://www.verizonconnect.com/solutions/gps-asset-tracking/ [6.7.2021]
[104] https://www.telekom-healthcare.com/en/e-health/internet-of-medical-things/asset-tracking-hospital [6.7.2021]
[105] Für einen Überblick über betriebliche IT-Infrastruktur und deren Verwaltung siehe z.B. Paula dos Santos, Carlos Raniery & Famaey, Jeroen & Schönwälder, Jürgen & Granville, Lisandro & Pras, Aiko & De Turck, Filip (2016): Taxonomy for the Network and Service Management Research Field. Journal of Network and Systems Management. 24. 764–787. 10.1007/s10922-015-9363-7
[106] Tedeschi, Stefano; Emmanouilidis, Christos; Mehnen, Jorn; Roy, Rajkumar (2019): A Design Approach to IoT Endpoint Security for Production Machinery Monitoring. Sensors. 19. 2355. 10.3390/s19102355

werden. Aus Beschäftigtensicht ist die Verwaltung der IT-Infrastruktur höchst sensibel. Die Minimierung der gespeicherten Daten, die strikte Einhaltung der Zweckbindung und die Kontrolle dieser Umstände durch den Betriebsrat sind hier darum besonders wichtig. Bei cloudbasierten Diensten oder einer Verwaltung durch externe Dienstleister hat das Unternehmen unter Umständen weniger direkten Zugriff als bei selbstverwalteten Systemen. Andererseits ist die Kontrolle der Datenverarbeitung für den Betriebsrat manchmal schwierig bis unmöglich.[107]

Ein entscheidender Bestandteil der betrieblichen IT-Infrastruktur ist die Verwaltung von Nutzeraccounts und Berechtigungen, die im digitalen Raum die gleiche Rolle erfüllen wie Zutrittssysteme im physischen Raum (vgl. Abschnitt 5.5.1). Im Rahmen des **Identity and Access Management (IAM)** werden Nutzeraccounts für ArbeitnehmerInnen angelegt und festgelegt, auf welche Systeme und Daten sie zugreifen dürfen. In Folge können sie sich an ihrem Rechner oder in bestimmten Programmen einloggen oder haben die Berechtigung, bestimmte Daten einzusehen oder zu ändern. Während die **Authentifizierung** überprüft, welche Berechtigungen mit welchen Zugangsdaten verbunden sind, verknüpft das Identitätsmanagement den Nutzeraccount mit den Stammdaten und der Rolle der Beschäftigten im Betrieb (vgl. Sharma et al 2015). Eine wichtige Rolle spielen dabei **Verzeichnisdienste** wie LDAP oder Microsoft's Active Directory.[108] Sobald ein Login erfolgt ist, kann prinzipiell jede erfasste oder protokollierte Aktivität einer bestimmten Person zugeordnet werden.

Neben der eigentlichen Verwaltung der IT-Infrastruktur wird mit **Helpdesk-Systemen** die Unterstützung von NutzerInnen bei technischen Problemen abgewickelt. Dabei werden meist Daten über alle Arbeitsschritte der Helpdesk-MitarbeiterInnen gespeichert. Gleichzeitig lassen sich Rückschlüsse über Beschäftigte ziehen, die sich an den Helpdesk wenden (vgl. Haslinger et al 2020, S. 53).

5.6 Systeme für Sicherheit und Compliance

Die in den folgenden Abschnitten beschriebenen Systeme verarbeiten Beschäftigtendaten für Zwecke der Arbeitssicherheit und -gesundheit, der Diebstahl- und Betrugsprävention oder der Cybersicherheit. Sie sollen das Eigentum des Unternehmens schützen, aber auch die Einhaltung gesetzlicher oder vertraglicher Verpflichtungen sicherstellen – darunter die Sicherheit und Gesundheit der Beschäftigten. Ihnen ist gemeinsam, dass sich die Datenverarbeitung dafür oft leichter rechtfertigen lässt als für andere Zwecke – sowohl rechtlich als auch vor der Belegschaft.

Die DSGVO erleichtert etwa die Verarbeitung personenbezogener Daten im öffentlichen Interesse, zum Schutz lebenswichtiger Interessen oder zur Erfüllung rechtlicher Verpflichtungen.[109] Die Verhinderung von Betrug oder die Gewährleistung der Netz- und Informationssicherheit können ein „berechtigten Interesse" des Unternehmens darstellen.[110] Die Bandbreite möglicher vertraglicher und rechtlicher Verpflichtungen, die als Begründung dienen können, ist groß (vgl. Haslinger et al 2020, S. 186). Auch gegenüber der Belegschaft sind diese Systeme oft leichter zu rechtfertigen – und der Einsatz kann selbstverständlich auch durchaus im Interesse der Beschäftigten sein. Gleichzeitig verarbeiten sie manchmal in exzessiver Weise hochsensible Daten, stellen ArbeitnehmerInnen unter Pauschalverdacht und können leicht für andere Zwecke missbraucht werden. Manchmal dienen invasive datenverarbeitende Systeme von Anfang an mehreren Zwecken. So kann der Einsatz einer Überwachungskamera etwa sowohl der Verhinderung von Diebstählen als auch der Qualitätssicherung dienen. Manche dieser Maßnahmen sind

[107] Bei prominenten cloudbasierten Systemen wie Microsoft 365 ist nicht nur teilweise undurchsichtig, welche Daten verarbeitet werden, sondern es stellt sich überhaupt die Frage, ob sie DSGVO-konform eingesetzt werden können. Siehe z.B. Fritsch 2021, S. 12ff

[108] https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview [6.7.2021]

[109] DSGVO Artikel 6 (1)

[110] DSGVO Erwägungsgründe (47) und (49)

in bestimmten Branchen näher an den Kerntätigkeiten des Unternehmens als bei anderen – etwa Systeme zur Gewährleistung der Cybersicherheit und der Verhinderung von Diebstahl und Insiderhandel bei Banken.

5.6.1 Diebstahl, Betrug, Korruption und „Compliance"

Zu den klassischen Überwachungs- und Kontrollmaßnahmen, die mit der Verhinderung von Diebstahl oder Vandalismus argumentiert werden, gehören Torkontrolle und Videoüberwachung. Während die **Torkontrolle** – also die Durchsuchung von Taschen beim Verlassen des Betriebsgeländes – keine technische Maßnahme im engeren Sinn darstellt, so greift sie doch wesentlich in die Persönlichkeitssphäre der Beschäftigten ein (vgl. Däubler 2017, S. 180). Die im Abschnitt 5.5.1 beschriebenen Systeme für die Kontrolle des Zutritts zum Betriebsgelände oder zu einzelnen Räumlichkeiten dienen unter anderem dazu, den Zutritt durch Unbefugte zu verhindern – und damit ebenfalls der „Sicherheit". **Überwachungskameras** im Betrieb werden seit langer Zeit immer wieder problematisiert. Je nach System und Positionierung der Kamera werden dabei Bilder von Aktivitäten verarbeitet oder archiviert. Dabei können Daten über Arbeitstätigkeiten anfallen, aber auch über Verhalten, das sich nicht auf die Arbeit bezieht.

Videoüberwachung greift besonders tief in die Persönlichkeitsrechte von ArbeitnehmerInnen ein. Selbst eine Kameraattrappe kann „Überwachungsdruck" erzeugen. Neben dem Einsatz zur Verhinderung von Diebstahl, Vandalismus, Raubüberfällen oder sonstigen Sicherheitszwecken werden Kameras bisweilen auch für die Qualitätssicherung oder für andere Zwecke der Steuerung betrieblicher Abläufe genutzt (vgl. Haslinger et al 2020, S. 44 und S. 186; Däubler 2017, S. 197ff). Hier droht die Grenze zum Einsatz für die Leistungs- und Verhaltenskontrolle zu verschwimmen. Diese Gefahr droht umso mehr bei Systemen, die Kamerabilder automatisiert auswerten, um Verhaltensweisen zu analysieren oder die abgebildeten Personen mittels **Gesichtserkennung** zu identifizieren.[111] Der Chiphersteller Intel hat die Kameras in den Betriebsräumlichkeiten im US-Bundesstaat Oregon 2020 mit Gesichtserkennungstechnologie ausgestattet. Seither werden täglich tausende Beschäftigte und BesucherInnen automatisiert mit Kameras überwacht. Dies soll laut Intel verhindern, dass die Räumlichkeiten von nicht näher definierten „Hochrisikopersonen" betreten werden, die eine Bedrohung für den Konzern darstellen (vgl. Rogoway 2020).

Schon länger im Einsatz sind Systeme für **Betrugserkennung im Handel**, die auf Basis einer laufenden Auswertung von Kassendaten verdächtige Verhaltensweisen wie etwa ungewöhnliche Rückerstattungen, Rabatte oder Stornos erkennen. Wie das Fallbeispiel in Abschnitt 6.2 zeigt, sind bei den Produkten von Oracle und RetailNext für Führungskräfte Listen einsehbar, die Kassa-MitarbeiterInnen mit namentlicher Nennung nach einer Risikobewertung gereiht darstellen. Manche Beschäftigte werden als besonders riskant hervorgehoben und stehen in Folge unter spezieller Beobachtung. Für als verdächtig eingestufte Kassentransaktionen sind zeitlich passende Ausschnitte aus aufgezeichneten Überwachungsvideos einsehbar. Daten über Bezahlvorgänge oder die mit dem Barcode-Lesegerät erfassten Produkte an der Supermarktkasse bilden sehr weitgehend die Arbeitstätigkeiten der Beschäftigten ab. Eine laufende Auswertung dieser Daten stellt damit eine laufende Kontrolle des ganzen Arbeitsalltags dar. Kassendaten werden auch im Dienstleistungsbereich oder in der Gastronomie eingesetzt, um mögliches Fehlverhalten von Beschäftigten aufzudecken. Manche dieser Systeme nutzen die gleichen Daten für ganz andere Zwecke – etwa zur Leistungsbewertung.

Darüber hinaus analysieren mittlere und große Unternehmen umfassende Datenbestände über betriebliche Abläufe aus Finanzbuchhaltung und ERP-Systemen[112], um **Korruption, Betrug und kriminelles Verhalten** aufzudecken

[111] Siehe z.B. https://www.identiv.com/3vr/ [13.7.2021]
[112] ERP-Systeme siehe Abschnitt 5.3.1

und etwa zu verhindern, dass betriebliche Ausgaben durch gefälschte Belege abgeschöpft werden oder dass bestechliche Beschäftigte überhöhte Rechnungen ausstellen oder Angebote manipulieren. Im Banken- und Finanzbereich beinhaltet dies auch die Verhinderung von **Insiderhandel und Geldwäsche** (vgl. Baader 2019, S. 48ff). Derartige Analysen beinhalten meist die Verarbeitung umfangreicher Beschäftigtendaten. Sie wurden lange hauptsächlich im Nachhinein durchgeführt – in Form einer regelmäßigen Durchsuchung geschäftlicher Transaktionsdaten nach Auffälligkeiten. Heute kommen Systeme zum Einsatz, die diese Daten laufend auswerten und versprechen, wirtschaftskriminelles oder betrügerisches Verhalten nicht nur zu entdecken, sondern schon im Vorhinein zu verhindern. Dabei kommen Methoden der Statistik und der künstlichen Intelligenz zum Einsatz, die Auffälligkeiten erkennen sollen (ebd., S. 59ff). Auch Software zur Prozessanalyse wie Celonis[113] kann dazu genutzt werden (ebd., S. 78).

Beim sogenannten „Red Flags"-Ansatz zur Betrugserkennung werden bestimmte **Aktivitäten und Verhaltensweisen** als ungewöhnlich definiert und als Regeln im System hinterlegt. Als mögliche „Red Flags" werden in der Literatur neben klar betrieblichen Aktivitäten wie dem übermäßigen Einkauf bei bestimmten LieferantInnen oder die Überbezahlung von Waren auch Lebenssituationen und Verhaltensweisen wie familiäre Krisen oder ein „ausschweifender Lebensstil" genannt (ebd., S. 82, S. 91). Während die laufende Einbeziehung derart persönlicher Informationen in Auswertungen zur Betrugserkennung durch Unternehmen datenschutzrechtlich kaum denkbar ist, stellt eine Reihe internationaler Anbieter sehr weitreichende Überwachungsfunktionen zur Verfügung, die persönliche Lebensverhältnisse (vgl. Abschnitt 6.4) oder Socialmedia-Aktivitäten (vgl. Abschnitt 6.9) einbeziehen. Derartige Funktionen sind heute oft bei Systemen im Umfeld der IT-Sicherheit zu finden, zum Beispiel bei Software für die Erkennung von **Insider Threats** – also von Bedrohungen durch Beschäftigte eines Betriebs (vgl. Abschnitt 5.6.3). Auch Software für **eDiscovery**, die die digitalen Archive des Betriebs nach Indizien und Beweisen für Fehlverhalten von Beschäftigten durchsucht, wertet umfangreiche Datenbestände aus.[114]

Derartige Systeme werden ebenso im staatlichen Bereich eingesetzt – von **Strafverfolgung bis zu geheimdienstlicher Überwachung** – und können potenziell missbraucht werden, zum Beispiel um unliebsame MitarbeiterInnen loszuwerden. Palantir, eine Datenanalysefirma, deren Aufstieg zum Teil mit Geldern des CIA-Investmentsfonds In-Q-Tel[115] finanziert wurde, hat für die Großbank JPMorgan Daten ausgewertet, um mögliches Fehlverhalten von Beschäftigten zu identifizieren. Ausgewertet wurde dabei E-Mail-Kommunikation, automatisch transkribierte Telefonate, Daten über Website-Zugriffe und Druckvorgänge, GPS-Standorte von Smartphones und Daten vom Zutrittskontrollsystem.[116] Laut Medienberichten hat Palantir auch dabei geholfen, kritische JournalistInnen und Gewerkschaften auszuspionieren (vgl. Christl und Spiekermann S. 108f). Die eDiscovery-Lösung von Microsoft wird damit beworben, dass sie zum Beispiel für die Auswertung betrieblicher Daten im Rahmen von Rechtsstreitigkeiten mit Beschäftigten genutzt werden könne.[117]

Auch Systeme, mit denen ArbeitnehmerInnen unternehmensintern Hinweise über Missstände an Vorgesetzte, Aufsichtsgremien oder Stabstellen senden können, kommen vermehrt zum Einsatz – unter Bezeichnungen wie **Hinweisgebersystem**, „Whistleblower-System", „Meldestelle wie Missstände" oder „Compliance-Hotline" (vgl. Fritsch 2020b). Während dieses interne „Whistleblowing" typischerweise von der Unternehmensführung unterstützt

[113] Siehe Fallbeispiel in Abschnitt 6.3

[114] Marktüberblick siehe z.B.: https://www.mordorintelligence.com/industry-reports/electronic-discovery-market

[115] https://www.iqt.org/portfolio/?search=palantir [13.7.2021]

[116] Mak, Aaron (2018): Report: Palantir Helped JPMorgan Spy on Employees. Slate, 19.4.2018. Online: https://slate.com/technology/2018/04/jpmorgan-used-palantir-tools-monitor-employee-activity-bloomberg-report.html

[117] https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-legal-investigations?view=o365-worldwide [13.7.2021]

wird, wird die Kommunikation von Missständen nach außen – etwa an Medien oder staatliche Behörden – als Bedrohung des Unternehmens eingestuft und unterbunden (vgl. Däubler 2017, S. 307).

Generell versuchen Unternehmen unter dem Schlagwort **Compliance** vermehrt, die Einhaltung von Gesetzen und betriebsinterner Regeln sicherzustellen. Dies geht über die Verhinderung von Gesetzesverstößen hinaus und kann als Vorwand für invasive Überwachungsmaßnahmen dienen (vgl. Däubler 2017, S. 278ff). Für die Aufzeichnung und automatisierte Auswertung von Gesprächen und jeglicher Bildschirmaktivitäten in Callcentern wird „Compliance" als Rechtfertigung genannt (vgl. Abschnitt 6.1.2) – ebenso für Systeme, die die Socialmedia-Kommunikation von Beschäftigten auswerten (vgl. Abschnitt 6.9). Auch die Gewährleistung von Arbeitssicherheit und -gesundheit wird unter diesem Schlagwort diskutiert.

5.6.2 Arbeitssicherheit und -gesundheit

Unternehmen sind durch eine Vielzahl gesetzlicher Vorschriften dazu verpflichtet, die Sicherheit und Gesundheit von ArbeitnehmerInnen zu gewährleisten.[118] Die Verarbeitung personenbezogener Daten für diese Zwecke ist in vielen Fällen gerechtfertigt und sinnvoll. Da die dabei erfassten Daten sehr umfassend oder sensibel sein können, sind Transparenz und eine strikte Einhaltung des Datenschutzes entscheidend. Eine Nutzung für andere Zwecke muss ausgeschlossen sein. Neben der Gefahr der Nutzung der Daten für andere Zwecke sind betriebliche Maßnahmen denkbar, die zwar vorgeben, der Arbeitssicherheit und -gesundheit zu dienen, tatsächlich aber andere Ziele verfolgen – oder zumindest eine gewisse Ambivalenz aufweisen.

Schon Anfang des 20. Jahrhunderts wurde etwa im Umfeld des von **Frederick Taylor** (1911) begründeten „wissenschaftlichen Managements" untersucht, wie sich körperliche Arbeitsbelastung und „Ermüdung" von Arbeitskräften verringern lassen könnte. Gilbreth und Gilbreth (1919) haben in ihrer „Ermüdungsstudie" akribisch jede Bewegung von BauarbeiterInnen aufgezeichnet und vermessen. Ziel war aber nicht nur die Bestimmung und Verringerung „unnötiger" Ermüdung, sondern auch die Bestimmung „nötiger" Ermüdung. In der Praxis könnte ein Unternehmen auf dieser Grundlage genau an das Limit dessen gehen, was körperlich möglich ist – oder auch etwas darüber hinaus. Heute wäre denkbar, dass die digital vermessene und in Kennzahlen gegossene „Ermüdung" der Belegschaft so lange in Kauf genommen wird wie andere betriebliche Kennzahlen in die richtige Richtung zeigen. Es wäre auch vorstellbar, dass Systeme, die vorgeblich für Zwecke der Arbeitssicherheit und -gesundheit invasive Beschäftigtendaten erfassen, am Ende nur zur Vortäuschung der Erfüllung arbeitsrechtlicher Vorgaben dienen, oder gar der Disziplinierung von Beschäftigten.

Als Beispiel für manche dieser Praktiken kann wie so oft **Amazon** dienen. Der Konzern ist dafür bekannt, das Arbeitsverhalten sehr umfassend zu überwachen und in Kennzahlen zu gießen (vgl. Abschnitt 7.1). Laut einem internen Dokument gibt es sogar eine Zahl für die Kalorien, die Beschäftigte in den Verteilzentrum im Schnitt verbrennen. Um Ermüdung und damit Verletzungen zu vermeiden, müssten sie sich laut Amazon so ernähren, dass sie stündlich 400 Kalorien verbrauchen können (vgl. Ongweso Jr 2021). Gleichzeitig ist die Verletzungsrate in den Verteilzentren von Amazon überdurchschnittlich hoch (vgl. Evens 2019). AuslieferungsfahrerInnen des Konzerns

[118] Für Österreich und Deutschland siehe z.B.: Heider, Alexander und Schneeberger, Karl (2018): ArbeitnehmerInnenschutzgesetz. 7. Auflage, 2017, ÖGB Verlag. Pieper, Ralf (2017): ArbSchR - Arbeitsschutzrecht. Arbeitsschutzgesetz, Arbeitssicherheitsgesetz und andere Arbeitsschutzvorschriften. 6. Auflage, 2017, Bund Verlag.

wurden dazu angehalten, ein vorhandenes System für die Fahrsicherheit zu deaktivieren, um die geforderten Zustellraten einzuhalten (vgl. Gurley 2021). Außerdem hat Amazon einen gewerkschaftlich aktiven Beschäftigten, der entwürdigende Arbeitsbedingungen und mangelnde Arbeitssicherheit kritisiert hat, mit der Begründung gekündigt, man habe Belege, dass er Regeln der Arbeitssicherheit verletzt habe.[119]

In den letzten Jahren vermarkten immer mehr Anbieter Systeme, die versprechen, die Sicherheit und -gesundheit von ArbeitnehmerInnen mittels invasiver Datenerfassung zu verbessern. Wie das Fallbeispiel in Abschnitt 6.7.1 zeigt, verspricht die Firma Kinetic, mit einem am Gürtel getragenen Gerät **gesundheitsschädliche Bewegungen** wie etwa falsches Bücken oder exzessive Drehungen zu erkennen, damit das Verletzungsrisiko von ArbeiterInnen in Logistikzentren oder Fabriken zu senken und die Produktivität zu erhöhen. Das Gerät warnt bei falschen Bewegungen mit Vibrationen. Gleichzeitig können Vorgesetzte die tägliche Zahl der „Hochrisiko-Bewegungen" von Einzelpersonen einsehen.

Ein ausführlicher Artikel über ähnliche Systeme zitiert einen Manager des globalen Logistikkonzerns Geodis, der offen darüber spricht, „Ergonomiedaten" einzusetzen, um den Arbeitsprozess effizienter zu machen, ihn „auf die Sekunde herunterzubrechen" und dann kleine Wartezeiten zwischen Tätigkeitsschritten zu eliminieren. Er möchte Daten über „Arbeitssicherheit" und „Effizienz" zusammenführen und bezeichnet Bedenken wegen einer derartigen Verknüpfung als „emotionale Sorgen". Ein ebenfalls im Artikel zitierter Gewerkschafter stimmt ihm im Grunde zu und sagt, **Ergonomiedaten** seien tatsächlich mit Leistungsdaten gleichzusetzen – zumindest bei körperlicher Arbeit. Er befürchtet, dass die Erfassung und Auswertung von Bewegungsdaten zur Verbesserung von Ergonomie und Arbeitssicherheit schlussendlich dazu genutzt werden würde, die Produktivität zu erhöhen und Arbeit zu beschleunigen (Brustein 2019).

Wie das Fallbeispiel in Abschnitt 6.7.2 zeigt, verkauft auch IBM ein umfassendes System, das mit am Körper getragenen Geräten und Sensoren in Schuhen und Helmen die **Arbeitssicherheit und -gesundheit bei manuellen Tätigkeiten** auf Baustellen oder in der Industrie verbessern soll. Neben der Überwachung von Verstößen gegen Sicherheitsregeln wie dem Abnehmen des Helms oder dem Betreten unerlaubter Areale verspricht es, mit Hilfe von Standort- und Sensordaten Stürze, Unfälle, schlechte Luftqualität oder zu große Hitze genauso zu erkennen wie eine zu hohe Herzfrequenz, Dehydrierung, Überanstrengung oder Übermüdung. Bei Problemen erhalten Beschäftigte visuelle oder akustische Warnungen. Führungskräfte haben Zugriff auf eine Live-Kartenansicht und auf Statistiken.

Auch wenn der Einsatz einzelner Funktionen des Systems insbesondere bei gefährlichen Arbeitstätigkeiten sinnvoll sein mag, führt die sehr weitgehende Überwachung von Körperdaten und Verhaltensweisen über den gesamten Arbeitstag hinweg zu einer umfassenden digitalen Verhaltenskontrolle. Dies birgt ein hohes Missbrauchspotenzial. Dass ArbeitnehmerInnen bei Schichtbeginn in der App sogar gefragt werden, wie viele Stunden sie in der vergangenen Nacht geschlafen haben und wie sie die Schlafqualität einschätzen, dehnt diese Verhaltenskontrolle sogar auf die Freizeit aus. Ob derartige selbsterklärte Angabe über die Schlafqualität Sinn machen sind und wie zuverlässig Zustände wie Überanstrengung oder Übermüdung überhaupt digital eingeschätzt werden können, bleibt unklar.

Abseits rein körperlicher Arbeit verspricht die Software „Performetric", durch eine Auswertung von Daten über Tippverhalten und Mausbewegungen den **Grad der mentalen Müdigkeit** von Callcenter-MitarbeiterInnen zu berechnen, wie das Fallbeispiel in Abschnitt 6.7.3 zeigt. Vorgesetzte sehen Auswertungen, die den berechneten

[119] Picchi, Aimee (2019): Amazon accused of firing warehouse worker who criticized "robot"-like treatment. CBS News, 21.3.2019. Online: https://www.cbsnews.com/news/amazon-accused-of-firing-warehouse-worker-who-criticized-robot-like-treatment/

Müdigkeitsgrad ins Verhältnis zu Leistungskennzahlen wie der Zahl der bearbeiteten Telefonate und deren Länge setzt. Diese können auch für Einzelpersonen erstellt werden. Durch die permanente Überwachung von Tippverhalten und Mausbewegungen greift das System tief in die Autonomie von Beschäftigten ein, während völlig unklar bleibt, wie valide die Auswertungen überhaupt sind.

5.6.3 IT-, Netzwerk-, System- und Cybersicherheit

Im Gegensatz zum Beschäftigtendatenschutz und anderen Regelungen und Maßnahmen zum Schutz der Rechte und Freiheiten von ArbeitnehmerInnen hat die IT-Sicherheit hauptsächlich das Ziel, das Unternehmen, dessen Infrastruktur und die betrieblichen Werte zu schützen (vgl. Eckert 2013, S. 1). Insbesondere soll die Verfügbarkeit, Integrität und Vertraulichkeit der geschäftlich verarbeiteten Informationen geschützt werden (vgl. Fried 1994). Auch wenn die Informationssicherheit ein Teilbereich des Datenschutzes ist, sind ihre Ziele keineswegs zwingend immer an den Interessen der Beschäftigten ausgerichtet. In den letzten Jahren setzen Unternehmen im Gegenteil immer mehr Systeme ein, die zur Gewährleistung betrieblicher Informations- und IT-Sicherheit tief in die Rechte und Freiheiten von ArbeitnehmerInnen eingreifen – bis hin zur Totalüberwachung des gesamten Arbeitsalltags.

Betriebliche IT-Infrastruktur ist unbestreitbar vielen Bedrohungen ausgesetzt. Die möglichen Schäden sind groß und können nicht nur ganze Unternehmen lahmlegen, sondern indirekt auch massive Auswirkungen auf viele andere Menschen haben – wenn etwa betriebliche Daten in falsche Hände geraten oder kritische Infrastruktur ausfällt. Neben höherer Gewalt und technischem oder organisatorischem Versagen entstehen Gefährdungen durch Fahrlässigkeit oder Vorsatz, durch Computerviren und Trojaner oder durch gezielte Cyberangriffe durch Kriminelle oder zum Zweck der Industriespionage (vgl. Eckert 2013, S. 16ff und S. 45ff; Vacca 2017, S. 1011ff). Maßnahmen zur IT-Sicherheit sind im Optimalfall integraler Bestandteil jeglichen IT-Systems. Alle in Abschnitt 5.5.3 beschriebenen Bereiche der Verwaltung und Wartung betrieblicher IT-Infrastruktur erfüllen darum auch Funktionen der IT-Sicherheit. Diese ist ein breites Feld. Für diverse Systeme wird eine Vielzahl an Bezeichnungen und Abkürzungen verwendet, die manchmal verwandte oder einander überschneidende Aufgaben erfüllen.

Eine wichtige Grundlage für betriebliche IT-Sicherheit ist die Verwaltung von Nutzeraccounts und Berechtigungen im Rahmen des **Identity and Access Management (IAM)**[120], die festlegt, wer auf welche Anwendungen, Programme, Funktionen und Daten in welcher Form zugreifen darf. Mittels **Single Sign-on (SSO)**[121] und **Cloud Access Security Broker (CASB)**[122] werden Zugangsberechtigungen und Sicherheitsrichtlinien zwischen unterschiedlichen Systemen vor Ort und in der Cloud miteinander verknüpft und gespiegelt (vgl. Vacca 2017, S. 409).

Betriebliche Endgeräte wie Desktop-Computer, Laptops, Smartphones oder Tablets und die darauf installierte Software werden meist vollständig aus der Ferne gewartet und kontrolliert. Dies betrifft zum Teil auch private Geräte, die betrieblich genutzt werden, sowie eine Fülle von anderen vernetzten Geräten im Betrieb – von Kassenterminals bis zu Maschinen in der Produktion (vgl. Abschnitt 5.3.2). Die dazu genutzten Systeme enthalten Funktionen für **Endpoint Security** bzw. **Endpoint Protection**[123], die oft weit über klassische **Antivirus-Software** hinausgehen[124] und jegliche Nutzung von Programmen und sonstige Aktivitäten am Gerät überwachen (vgl. Vacca 2017, S. 1049).

[120] https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam
[121] https://www.gartner.com/en/information-technology/glossary/sso-single-sign-on
[122] https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs
[123] https://www.gartner.com/en/information-technology/glossary/endpoint-protection-platform-epp
[124] Gartner (2021): Magic Quadrant for Endpoint Protection Platforms. Gartner, 5.5.2021

Auf der Ebene des Netzwerks überwachen **Firewalls**[125] jeglichen Datenverkehr zwischen betrieblichen Systemen und der Außenwelt und filtern Datenverkehr, der als Bedrohung eingeschätzt wird. Sie können damit zum Beispiel den Zugriff auf bestimmte Websites blockieren (ebd., S. 1253ff). Sogenannte **Next-Generation Firewalls (NGFW)**[126] sind in der Lage, auch verschlüsselten Datenverkehr zu überwachen und identifizieren dabei NutzerInnen und genutzte Anwendungen (vgl. Neupane et al 2018). Umgekehrt stellen **Virtual Private Networks (VPNs)**[127] verschlüsselte Netzwerkverbindungen zwischen betrieblich genutzten Geräten über das Internet her, können dabei aber potenziell erst recht auf den kompletten Datenverkehr zugreifen (vgl. Eckert 2013, S. 765ff).

Sogenannte **Intrusion Prevention Systems (IPS)** überwachen sowohl Geräte als auch Datenverkehr und versuchen, Virenbefall, gezielte Cyberangriffe und andere Sicherheitsbedrohungen zu entdecken bzw. zu verhindern (vgl. Vacca 2017, S. 159ff). Auf den Endgeräten der Beschäftigten kann die laufende Überwachung der genutzten Programme und erstellter, geänderter und geöffneter Dateien genauso erfolgen wie die Erkennung oder Beschränkung der Nutzung von Zusatzgeräten wie USB-Sticks oder von eingebauten Mikrofonen und Kameras (ebd., S. 145). Lösungen für **E-Mail-Sicherheit** überwachen versandte und empfangene E-Mail-Nachrichten. Funktionen wie das Filtern von Spam-Nachrichten und der Schutz vor Viren gehen dabei nahtlos in eine sehr weitreichende Auswertung von Kommunikationsinhalten über, die versucht, auf Basis künstlicher Intelligenz Muster zu erkennen, die die Übernahme von E-Mail-Konten durch Kriminelle durch „Phishing" genauso verhindern soll wie die Preisgabe von Geschäftsgeheimnissen oder andere unerwünschte Verhaltensweisen von Beschäftigten[128] (vgl. Eckert 2013, S. 80ff; Vacca 2017, S. 157). Ähnliches gilt für **Chats und Instant Messaging** (vgl. Vacca 2017, S. 726ff).

Systeme für **Unified Threat Management (UTM)**[129] vereinen viele der bereits genannten Funktionen, oft in Form physischer Geräte, die Funktionen einer Next-Generation Firewall, zur Filterung von Website-Zugriffen und E-Mail-Nachrichten sowie zur Erkennung und Verhinderung von Virenbefall und Cyberangriffen abdecken (vgl. Vacca 2017, S. e277ff). Unter dem Begriff **Data Loss Protection (DLP)**[130] wird Software vermarket, die nicht die Bedrohung von außen als Ausgangspunkt nimmt, sondern umgekehrt versucht, den Verlust betrieblicher Informationen zu verhindern. Dabei werden ebenfalls die meisten der genannten Funktionen abgedeckt. Der Blickwinkel verschiebt sich aber auf Bedrohungen, die aus dem Unternehmen selbst kommen und damit auf Beschäftigte, die Fehler machen, durch Unwissenheit oder Fahrlässigkeit Opfer von Cyberangriffen werden oder aber dem Unternehmen absichtlich schaden wollen (vgl. Vacca 2017, S. 1155). Ausschließlich auf Beschäftigte als interne Bedrohung konzentrieren sich Funktionen zur Erkennung von **Insider Threats** (ebd., S. 529ff). Hier geht Cyber-Sicherheit nahtlos in die in Abschnitt 5.6.1 beschriebenen Praktiken der Erkennung von Diebstahl, Betrug und Korruption über. Insbesondere bei Systemen zur Verhinderung von Datenverlust und Bedrohungen durch „Insider" werden oft sehr vielfältige Verhaltensdaten einer großen Zahl von ArbeitnehmerInnen über lange Zeiträume ausgewertet. Nach Vorfällen werden mit Software für **eDiscovery** und **Cyber Forensics** große betriebliche Datenbestände nach Hinweisen durchsucht und Beweise gesichert – unter anderem über Aktivitäten von Beschäftigten (ebd., S. 571ff).

Besondere Aufmerksamkeit verdienen zwei neuere Systemtypen, die im Hintergrund weitreichende Daten über Verhaltensweisen im Arbeitsalltag auswerten. Plattformen für **Security Information and Event Management"**

[125] https://www.gartner.com/en/information-technology/glossary/firewall
[126] https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws
[127] https://www.gartner.com/en/information-technology/glossary/vpn-virtual-private-network
[128] Gartner (2020): Market Guide for Email Security. Gartner, 8.9.2020
[129] https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm
[130] https://www.gartner.com/en/information-technology/glossary/data-loss-protection-dlp

(SIEM)[131] führen Log- und Ereignisdaten aus bestehenden IT-Systemen im Betrieb zusammen. Software für **User and Entity Behavior Analytics (UEBA)** überwacht Nutzerverhalten, um als verdächtig eingeschätzte Verhaltensweisen zu erkennen. Diese Systeme „lernen" laufend, wie sich Beschäftigte „normalerweise" verhalten und versuchen, außergewöhnliches Verhalten zu erkennen und das damit verbundene Risiko zu bewerten. Dabei werden viele Datenquellen einbezogen – vom Netzwerkdatenverkehr und der Nutzung von Geräten und Programmen über die Ablage und Bearbeitung von Dateien und jeglicher Kommunikation bis hin zu Personal- oder gar Leistungsdaten. Mehrere Produkte werten Tastatureingaben aus und zeichnen auf, was bei ArbeitnehmerInnen am Bildschirm zu sehen ist. Zu den bekannten Anbietern in den Bereichen SIEM und UEBA zählen unter anderem IBM, Microsoft, Forcepoint, Splunk, Exabeam, Securonix, LogRhythm, Rapid7 oder Micro Focus (vgl. Abschnitt 6.4.1).

Wie das Fallbeispiel im Abschnitt 6.4.2 zeigt, werten die Produkte für UEBA, DLP und gegen Bedrohungen durch „Insider" des US-Herstellers **Forcepoint** laufend Daten über den ganzen Arbeitsalltag von Beschäftigten aus. Überwacht werden Login-Vorgänge, auf dem Rechner genutzte Programme, das Öffnen, Ändern und Kopieren von Dateien, Zugriffe auf Websites, Suchvorgänge, Kommunikation via E-Mail, Chat und Telefon sowie Daten über den physischen Zutritt zu Räumlichkeiten. Neben Logdaten aus Systemen von Microsoft, Salesforce, SAP oder Cisco können auch GPS-Standorte, Druckerdaten oder Mitarbeiterbeurteilungen aus der Personalverwaltung einbezogen werden. Forcepoint berechnet daraus laufend **Risikobewertungen für Beschäftigte**. Durch die Auswertung von Kommunikationsinhalten und anderer Daten wird eingeschätzt, ob ArbeitnehmerInnen in finanziellen Schwierigkeiten stecken, ob sich ihre „Produktivität" verringert hat, ob sie Kündigungsabsichten haben, wieviel sie mit KollegInnen kommunizieren, ob sie „obszöne" Inhalte aufrufen oder ob eine „negative" Stimmung herrscht. Das System gegen Bedrohungen durch „Insider" wertet darüber hinaus Aktivitäten wie Tastatureingaben, Kopiervorgänge über die Zwischenablage oder die Anfertigung von Screenshots aus und ermöglicht es, die für Beschäftigte sichtbaren Bildschirminhalte im Nachhinein als Video einzusehen.

Selbst wenn die exzessiven Funktionen zur Verhaltensüberwachung von Forcepoint und ähnlichen Anbietern nur in Hochsicherheitsbranchen und nur für ArbeitnehmerInnen in sensiblen Arbeitsbereichen eingesetzt würden, greifen sie tief in die Autonomie der Beschäftigten ein und bieten ein hohes Missbrauchspotenzial. Als mögliche Bedrohungen nennt Forcepoint etwa auch „unzufriedene" ArbeitnehmerInnen, die einen „großen Streit mit dem Chef" hatten, und „interne Aktivisten", die Informationen an Medien geben könnten. Außerdem ist zu befürchten, dass derart invasive Funktionen im Lauf der Zeit in immer mehr Bereichen eingesetzt werden. Viele Anbieter von IT-Sicherheitslösungen haben enge **Verbindungen zu Militär und Geheimdiensten**. Forcepoint war etwa bis vor kurzem Teil des US-Rüstungsgiganten Raytheon. Der 2019 übernommene Anbieter RedOwl, der nun die UEBA-Funktionen von Forcepoint abdeckt, wurde mit Risikokapital der CIA aufgebaut. Der Gründer von RedOwl ist ehemaliger NSA-Offizier und hatte zuvor ein Unternehmen gegründet, das an einem 2011 aufgedeckten Plan zur großangelegten Diskreditierung von gewerkschaftlichen Gruppen in den USA beteiligt war (vgl. Abschnitt 6.4.1).

Wie dieser Abschnitt zeigt, verschwimmen die Grenzen zwischen IT-Sicherheit, Betrugs- und Diebstahlsprävention, dem Schutz von Kundendaten und Geschäftsgeheimnissen („Data Loss Protection") oder etwa der Gewährleistung der Einhaltung von Gesetzen und sonstiger Verhaltensregeln im Unternehmen („Compliance") zunehmend. Systeme für die Abwehr von Cyberangriffen, für die Überwachung von Netzwerken oder für die Fernwartung von

[131] https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

Geräten und greifen ineinander und werden dazu genutzt, Fehlverhalten zu verhindern – ob fahrlässig, absichtlich oder in anderer Weise unerwünscht.

5.7 Systeme für Kommunikation und Zusammenarbeit

Zwischenmenschliche Kommunikation genoss in der Geschichte der Grundrechte immer schon einen besonderen Schutz. Das Kommunikationsgeheimnis zählt zu den Wurzeln rechtlicher Garantien für Privatheit und Privatsphäre (vgl. Peissl 2007, S. 279) und ist heute neben dem Recht auf den Schutz personenbezogener Daten in der EU als Grundrecht verankert.[132]

Technische Systeme, die Kommunikation und damit Koordination und Zusammenarbeit ermöglichen, sind darum besonders sensibel. Dabei werden einerseits Inhaltsdaten verarbeitet, also Informationen über Kommunikationsinhalte wie etwa das gesprochene oder geschriebene Wort. Andererseits fallen Metadaten an, also zum Beispiel Informationen darüber, wer mit wem zu welchen Zeitpunkten in welcher Form wie lange kommuniziert (vgl. Abschnitt 5.2). Damit sind auch Metadaten über Kommunikationsvorgänge – in österreichischen und deutschen Telekommunikationsgesetzen „Verkehrsdaten“[133] genannt – sensibel, da sie Aufschluss über Kommunikationsmuster und menschliches Verhalten geben können. Die Existenz dieser Systeme ist für die Beschäftigten offensichtlich und sehr sichtbar. Deren Nutzung bildet bei vielen Arbeitstätigkeiten einen Großteil des Arbeitsalltags ab, in manchen Fällen wie etwa im Callcenter beinahe die gesamte Arbeitszeit. Andererseits können ArbeitnehmerInnen meist kaum überprüfen, wie und zu welchen Zwecken Unternehmen Kommunikationsdaten im Hintergrund verarbeiten.

5.7.1 Web, E-Mail, Telefon, VOIP, Smartphone, Videokommunikation

Fast jeder betriebliche Kommunikationsvorgang wird heute über das öffentliche Internet oder andere digitale Netzwerke übertragen. Wer Kommunikationsdienste wie E-Mail oder die zu Grunde liegenden Netzwerke betreibt und wartet, hat potenziell Zugriff auf die übertragenen Informationen (vgl. Abschnitt 5.5.3). Auch Telefonie wird in Unternehmen heute über **„Voice over Internet Protocol“ (VoIP)** abgewickelt (vgl. Frühbrodt 2018, S. 8ff). Dabei wird Sprache digital über das Internet oder andere digitale Netzwerke übertragen und kann damit potenziell ebenfalls ausgewertet werden.

Zur Gewährleistung von **Cybersicherheit** werden Aktivitäten wie Website-Zugriffe oder E-Mail-Kommunikation oft laufend protokolliert, überwacht und gefiltert – um den Zugriff auf nicht vertrauenswürdige Websites zu unterbinden, Spam-Nachrichten auszusondern, Trojaner und Viren zu erkennen und Cyberangriffe zu verhindern. Zeitgenössische IT-Sicherheitssysteme können den Netzwerkdatenverkehr selbst dann auswerten, wenn die Übertragung verschlüsselt erfolgt. Die Verarbeitung von Kommunikationsdaten zur Gewährleistung des laufenden Betriebs und der IT-Sicherheit kann fließend in die Überwachung der Kommunikation zur Erkennung von „interne Bedrohungen“, Betrug, Korruption und anderen im Betrieb unerwünschten Verhaltensweisen übergehen. Dazu stehen Systeme zur Verfügung, die jegliche digitale Kommunikation inklusive der Inhalte auswerten und damit den Charakter einer Totalüberwachung aufweisen. Diese haben meist auch Zugriff auf die Endgeräte und die darauf genutzte Software (vgl. Abschnitt 5.6.3).

[132] Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union: https://fra.europa.eu/de/eu-charter/article/7-achtung-des-privat-und-familienlebens, https://fra.europa.eu/de/eu-charter/article/8-schutz-personenbezogener-daten

[133] Österreich: Telekommunikationsgesetz 2003, § 99. Deutschland: Telekommunikationsgesetz § 96

Sobald Endgeräte wie **Smartphone** vom Betrieb gewartet und kontrolliert werden, können Kommunikationsdaten potenziell direkt vom Gerät aus ausgewertet werden. Ähnliches ist der Fall, wenn der Netzwerkdatenverkehr – zum Beispiel über eine VPN-Verbindung – über die digitale Infrastruktur des Unternehmens umgeleitet wird (ebd.). Seit der globalen Pandemie 2020 erlebte Software für **Videokommunikation** einen signifikanten Aufstieg. Zu den bekannten Anbietern gehören neben Microsoft Skype und Teams beispielsweise Cisco WebEx und Zoom.[134]

Werden derartige Systeme – oder Teile davon – nicht von der IT-Abteilung eines Betriebs selbst betrieben, sondern extern betreut oder in der Cloud betrieben, hängen die Zugriffsmöglichkeiten auf Kommunikationsdaten vom Dienstleister oder Hersteller der genutzten Produkte ab.

5.7.2 Unified Communications, Kollaborationssysteme und betriebliche soziale Netzwerke

Neben Diensten für einzelne Kommunikationsarten wie Telefonie oder E-Mail hat sich in den letzten Jahren eine Vielfalt an Systemen entwickelt, die unterschiedliche Formen der betrieblichen Kommunikation und Zusammenarbeit vereinen. Unter Schlagwörtern wie **Unified Messaging** oder **Unified Communications**[135] werden Produkte vermarket, die Sprachtelefonie und Videokommunikation mit „Messaging“ verbinden – also mit dem schnellen Versand von Nachrichten an Einzelne oder Gruppen in Chat-Umgebungen. Mit dem Schlagwort „Unified Communications and Collaboration“[136] werden Dienste beworben, die neben der Abwicklung von Kommunikation weitergehende Funktionen für die Zusammenarbeit in Teams bieten. Microsoft und Cisco gehören zu den Marktführern in diesen Bereichen.[137]

Einen rasanten Aufstieg erlebte das erst seit 2014 für den Einsatz in Unternehmen verfügbare Kollaborationssystem **Slack**, das betriebliche Kommunikation und Zusammenarbeit in Form von Echtzeit-Chats organisiert, die manchmal den gesamten Arbeitsalltag der Beschäftigten begleiten (vgl. Silverman 2016). Neben Chat-Kanälen bietet Slack auch Funktionen zum Dateiaustausch sowie für Sprach- und Videokommunikation.[138] Mit Hilfe sogenannter Bots[139], einer Vielzahl an Apps[140] und Anbindungen an andere betriebliche Software von vielen Drittherstellern[141] können Kommunikationsvorgänge digital strukturiert oder automatisiert werden. Damit kann aus Slack etwa ein System zur Verwaltung von Arbeitsaufgaben[142] und -abläufen[143] werden. Slack bietet Lösungen, die Kommunikation und Arbeitsabläufe in Bereichen wie Software-Entwicklung, Projektmanagement, IT-Support, Kundenservice, Marketing oder Verkauf strukturieren und steuern.[144] Das Produkt wurde lange damit beworben, dass „alles in Slack“ automatisch „indiziert und archiviert“ werde und damit später bei Bedarf jederzeit zur Verfügung stünde. Der Name „Slack“ selbst steht für „Searchable Log of All Conversation and Knowledge” – also für ein “durchsuchbares Protokoll aller Konversationen und allen Wissens“ im Unternehmen (vgl. Silverman 2016). Das Produkt

[134] Gartner (2020): Gartner Magic Quadrant for Meeting Solutions. Gartner, 12.10.2020. Online: https://www.gartner.com/en/documents/3991618/magic-quadrant-for-meeting-solutions
[135] https://www.gartner.com/en/information-technology/glossary/unified-communications-uc
[136] https://www.gartner.com/en/information-technology/glossary/unified-communications-and-collaboration-ucc
[137] Forrester (2019): The Forrester Wave™: Unified-Communications-As-A-Service (UCaaS) Providers, Q3 2019. Forrester, 27.8.2019
[138] https://slack.com/intl/en-at/help/categories/200111606 [9.8.2021]
[139] https://api.slack.com/bot-users [9.8.2021]
[140] https://slack.com/apps [9.8.2021]
[141] https://slack.com/intl/en-at/integrations [9.8.2021]
[142] https://slack.com/intl/en-au/solutions/task-management [9.8.2021]
[143] https://slack.com/intl/en-at/features/workflow-automation [9.8.2021]
[144] https://slack.com/intl/en-at/solutions [9.8.2021]

selbst[145] und Erweiterungen von Drittherstellern[146] ermöglichen viele Arten der Auswertung von Kommunikationsdaten. Auch Erweiterungen für die Personalverwaltung stehen zur Verfügung.[147] Slack wurde 2021 an den CRM-Giganten Salesforce verkauft.[148]

Manche Systeme für Kommunikation und Zusammenarbeit werden gar als **innerbetriebliche soziale Netzwerke** vermarket – also als betriebliche Äquivalente zu Plattformen wie Facebook. Sie bieten neben Dokumentenverwaltung und Organisation von Teamarbeit etwa für alle einsehbare Nutzerprofile und Möglichkeiten, Nachrichten und Kommentare zu posten, sie zu bewerten oder zu teilen, anderen zu „folgen" und im eigenen „News Feed" über die neuesten Inhalte und Interaktionen informiert zu werden (vgl. Höller und Wedde 2018). Facebook vermarket mit „Workplace" selbst ein derartiges Systeme für Unternehmen.[149] Salesforce Chatter[150], HCL Connections[151] oder Microsoft-Produkte wie Sharepoint oder Yammer bieten ähnliche Funktionen (vgl. Hölle und Wedde 2018). Viele dieser und der oben genannten Systeme erfüllen Teile dessen, was früher das sogenannte **Intranet** war – von interner Kommunikation in Richtung Belegschaft über Zusammenarbeit und Wissensmanagement bis zum Zugang zu digitalen Anwendungen für ArbeitnehmerInnen, etwa zur Selbstverwaltung der eigenen Beschäftigtendaten.[152] Zeitgenössische Intranet-Systeme[153] werden als Plattformen für „Employee Communication"[154], „Employee Experience"[155] oder als „digitaler Arbeitsplatz"[156] vermarket – und bieten manchmal viele Funktionen eines innerbetrieblichen sozialen Netzwerks.[157]

Die Produkte von Microsoft decken beinahe alle genannten Bereiche ab und verbinden sie mit den anderen Microsoft-Angeboten, die nun im cloudbasierten System **Microsoft 365** zusammengefasst sind. Während **Outlook und Exchange** die Kommunikation via E-Mail, Kontakte, Termine und Aufgaben abdecken, bietet **SharePoint** diverse Funktionen für das Intranet und die Zusammenarbeit in Teams (vgl. Fritsch 2021). Skype für Unternehmen wird in Microsoft Teams aufgehen, ähnliches wird für Yammer erwartet, das Chat-Funktionen mit einem innerbetrieblichen sozialen Netzwerk vereint. **Microsoft Teams** bietet neben Sprachtelefonie, Videokommunikation, Chats und Kanälen[158] vorgefertigte Zusatzfunktionen zur Strukturierung, Steuerung und Kontrolle von Arbeitsaufgaben[159] und -abläufen, Funktionen für gegenseitige Positivbewertungen zwischen Beschäftigten in Form von „Badges"[160] und Funktionen zur Kommunikation über die Organisation von Arbeitsschichten.[161] Außerdem können ähnlich wie bei Slack Apps von Drittanbietern eingebunden werden[162], die Arbeitstätigkeiten und -abläufe strukturieren – für un-

[145] https://slack.com/intl/en-at/help/articles/360057638533-Understand-the-data-in-your-Slack-analytics-dashboard [9.8.2021]
[146] https://slack.com/apps/category/At0G5YTKU2-analytics [9.8.2021]
[147] https://slack.com/apps/category/At0EFT6893-hr-team-culture [9.8.2021]
[148] https://slack.com/intl/en-at/blog/news/salesforce-completes-acquisition-of-slack [9.8.2021]
[149] https://www.workplace.com/ [9.8.2021]
[150] https://www.salesforce.com/eu/products/chatter/features/ [9.8.2021]
[151] https://www.hcltechsw.com/connections [9.8.2021]
[152] https://www.gartner.com/en/information-technology/glossary/intranet
[153] Forrester (2020): The Forrester Wave™: Intranet Platforms, Q2 2020. Forrester, 16.6.2020
[154] https://www.simpplr.com/ [9.8.2021]
[155] https://www.unily.com/ [9.8.2021]
[156] https://www.lumapps.com/de/ [9.8.2021]
[157] https://www.jivesoftware.com/solutions/enterprise-social-network/ [9.8.2021]
[158] https://docs.microsoft.com/en-us/office365/servicedescriptions/teams-service-description [9.8.2021]
[159] https://docs.microsoft.com/en-us/microsoftteams/manage-tasks-app [9.8.2021]
[160] https://docs.microsoft.com/en-us/microsoftteams/manage-praise-app [9.8.2021]
[161] https://docs.microsoft.com/en-us/microsoftteams/expand-teams-across-your-org/shifts/manage-the-shifts-app-for-your-organization-in-teams [9.8.2021]
[162] https://appsource.microsoft.com/en-us/marketplace/apps?product=teams [9.8.2021]

terschiedliche Branchen und Unternehmensbereiche. Unternehmen können auch selbst „Bots“ und andere Zusatzfunktionen für die weitergehende Strukturierung, Steuerung, Automatisierung und Kontrolle von Arbeitstätigkeiten in Microsoft Teams entwickeln.[163]

Darüber hinaus ist Teams mit vielen anderen Funktionen von Microsoft 365 integriert – von den Office-Anwendungen Word, Excel und PowerPoint bis zur Ablage von Dateien. Viele Aktivitäten in Teams oder Office sowie Informationen darüber, wer wann welche Datei erstellt, geändert, geöffnet oder freigegeben hat, werden gespeichert und können über verschiedene Analyse-Anwendungen oder über die Programmierschnittstelle „Graph API“ ausgewertet werden (vgl. Abschnitt 5.3.4). Für Microsoft Teams kann angezeigt werden, an wie vielen Besprechungen individuelle Beschäftigte teilgenommen haben, wie viele Nachrichten in Chats oder Kanälen hinterlassen wurden oder welche Zeitdauer eine Person mit Audio- oder Videokommunikation verbracht hat.[164] Für über Teams durchgeführte Telefonate können für jeden eingehenden und ausgehenden Anruf die Telefonnummer des Gegenübers, die Gesprächsdauer und viele andere Informationen ausgewertet werden.[165] Wie der nachfolgende Abschnitt zeigt, können Aktivitätsdaten aus Teams mit Hilfe von Microsoft Workplace Analytics und andere Funktionen auf viele weitere Arten ausgewertet werden.

5.7.3 Auswertung von Daten über Kommunikation und Zusammenarbeit

Neben der Überwachung für Zwecke der IT-Sicherheit, Betrugserkennung oder zur Abwehr von Bedrohungen durch Beschäftigte werden Kommunikationsdaten auch für andere Zwecke analysiert oder betrieblich genutzt. Zeitgenössische Callcenter-Systeme bieten weitreichende Funktionen zur Auswertung von Kommunikationsinhalten im Namen von Qualitätssicherung, Kundenzufriedenheit und „Compliance“ bis hin zur Analyse von Stimmung und Emotionen in Gesprächen (siehe Abschnitt 6.1). Im Bereich hochqualifizierter Wissensarbeit vermarket eine US-Firma ein Produkt zur Vermessung von Kommunikationsmustern mit Hilfe kleiner Geräte mit eingebautem Mikrofon, die am Körper getragen werden, und wertet dabei sogar sprachliche Kommunikation zwischen Beschäftigten im Büro aus. Auch Kommunikationsdaten aus Systemen von Microsoft, Slack oder Zoom können einbezogen werden (siehe Abschnitt 6.6).

Microsoft „Workplace Analytics“. Auch Microsoft bietet inzwischen Produkte an, die das Kommunikationsverhalten der Belegschaft analysieren. Mit Hilfe von Workplace Analytics erhalten Führungskräfte Einblicke in das Kommunikationsverhalten der Belegschaft und in Zusammenarbeit und Beziehungen zwischen Beschäftigten. Dazu wird die gesamte betriebliche Kommunikation via E-Mail, Anrufe, Videokonferenzen und Chats aus Microsoft-365-Anwendungen wie Outlook/Exchange und Teams analysiert. Außerdem werden Kalendereinträge sowie Personaldaten über Positionen und Rollen der Beschäftigten einbezogen. Neben Metadaten über die Zeitpunkte und TeilnehmerInnen der jeweiligen Kommunikationsvorgänge und Besprechungen werden „Betreffzeilen“ im Volltext ausgewertet.[166] Workplace Analytics stellt zum Beispiel folgende Auswertungen zur Verfügung:

- Anzahl der Stunden, die Beschäftigte in Besprechungen verbringen.
- Anzahl der Stunden, die sie mit dem Lesen und Versenden von E-Mails verbringen.[167]

[163] https://www.microsoft.com/en-us/microsoft-teams/apps-and-workflows [9.8.2021]
[164] https://docs.microsoft.com/en-us/microsoftteams/teams-analytics-and-reports/user-activity-report [9.8.2021]
[165] https://docs.microsoft.com/en-us/microsoftteams/teams-analytics-and-reports/pstn-usage-report [9.8.2021]
[166] https://docs.microsoft.com/de-de/workplace-analytics/privacy/privacy-and-data-access [12.8.2021]
[167] https://docs.microsoft.com/de-de/workplace-analytics/use/explore-metrics-week-in-the-life [12.8.2021]

- Anzahl der „Fokusstunden“, in denen keine Besprechungen stattgefunden haben.[168]
- Anzahl der Stunden für E-Mail-Kommunikation und Besprechungen außerhalb der definierten Geschäftszeiten. Microsoft selbst bezeichnet dies als „Überwachung der Aktivitäten nach Feierabend“.[169]
- Anzahl der Stunden interner Zusammenarbeit (Besprechungen und E-Mail-Kommunikation mit Personen innerhalb des Unternehmens) und Anzahl der Stunden externer Zusammenarbeit (Besprechungen und E-Mail-Kommunikation mit mindestens einer Person außerhalb des Unternehmens).[170]
- Besprechungsstunden, die von Microsoft als Besprechungen „niederer Qualität“ einstuft werden, aufgeschlüsselt nach „redundanten“ Besprechungsstunden (Besprechungen, bei denen Personen aus mindestens drei Organisationsebenen teilnehmen), „Multitasking-Besprechungsstunden“ (Besprechungen, bei denen TeilnehmerInnen zwei oder mehr E-Mails pro Besprechungsstunde versandt haben) und „in Konflikt stehenden“ Besprechungen (mehr als eine Besprechung zum gleichen Zeitpunkt im Kalender).[171]
- Besprechungsstunden, die Beschäftigte mit direkten und indirekten Vorgesetzten verbringen.[172]
- Analysen der internen[173] und externen[174] kommunikativen „Netzwerke“ der Beschäftigten, aufgeschlüsselt nach „Größe“ des Netzwerks (durchschnittliche Zahl der Personen, mit denen eine Person mindestens zwei von Microsoft als „sinnvoll“ definierte[175] Kontakte hatte) und „Breite“ des Netzwerks (durchschnittliche Zahl der Teams bzw. externen Unternehmen, mit denen eine Person mindestens zwei als „sinnvoll“ definierte Kontakte hatte).

Neben den vorgefertigten Berichten können Unternehmen eigene Auswertungen definieren und durchführen:

- Mit sogenannten „Peeranalysen“ kann zum Beispiel untersucht werden, wie die „effektivsten“ MitarbeiterInnen kommunizieren und zusammenarbeiten.[176]
- Unternehmen können Schlüsselwörter definieren und damit Auswertungen über Kommunikation und Zusammenarbeit durchführen, bei denen die Betreffzeilen nach diesen Schlüsselwörtern durchsucht werden. So können etwa nur Daten zu E-Mail-Kommunikation und Besprechungen analysiert werden, die Begriffe wie „Kauf“, „Budget“, „Genehmigung“ oder „Lizenz“ enthalten. Microsoft schlägt vor, diese Funktionen zur Analyse betrieblicher Abläufe zu nutzen.[177]
- Generell können eigene Abfragen definiert werden, dabei können weitere Daten einbezogen werden.[178]

Viele der Berichte zeigen aggregierte Ergebnisse für Teams, Abteilungen oder den ganzen Betrieb. Es stehen aber auch Auswertungen zur Verfügung, die sich auf Einzelpersonen beziehen. Die Namen der Beschäftigten werden dabei durch Pseudonyme ersetzt.[179] Microsoft gibt viele Hinweise und Empfehlungen zu Datenschutz und ist der Ansicht, Workplace Analytics könne „problemlos“ in „Übereinstimmung mit der DSGVO“ verwendet werden.[180]

---

[168] Ebd.
[169] Ebd.
[170] Ebd.
[171] https://docs.microsoft.com/de-de/workplace-analytics/use/explore-metrics-meetings-overview [12.8.2021]
[172] https://docs.microsoft.com/de-de/workplace-analytics/use/explore-metrics-management-and-coaching [12.8.2021]
[173] https://docs.microsoft.com/de-de/workplace-analytics/use/explore-metrics-internal-networks [12.8.2021]
[174] https://docs.microsoft.com/de-de/workplace-analytics/use/explore-metrics-external-collaboration [12.8.2021]
[175] https://docs.microsoft.com/de-de/workplace-analytics/use/glossary#meaningful-interaction-define [12.8.2021]
[176] https://docs.microsoft.com/de-de/workplace-analytics/use/peer-analysis [12.8.2021]
[177] https://docs.microsoft.com/de-de/workplace-analytics/tutorials/analyze-business-processes [12.8.2021]
[178] https://docs.microsoft.com/de-de/workplace-analytics/tutorials/query-designer [12.8.2021]
[179] https://docs.microsoft.com/de-de/workplace-analytics/tutorials/person-queries [12.8.2021]
[180] https://docs.microsoft.com/de-de/workplace-analytics/privacy/data-protection-intro [12.8.2021]

Österreichische Gewerkschaften empfehlen BetriebsrätInnen hingegen, sich gegen den Einsatz des Produkts auszusprechen (vgl. Fritsch 2021, S. 41). Als Grundlage für die Auswertungen werden jedenfalls exzessive personenbezogene Daten über das Kommunikationsverhalten der gesamten Belegschaft verarbeitet. Sogar Daten über unternehmensexterne Personen – etwa KundInnen, GeschäftspartnerInnen oder LieferantInnen – werden einbezogen.[181]

Microsoft legt Betrieben nahe, mit Workplace Analytics die Effektivität von Kommunikation und Zusammenarbeit zu vermessen. Die Sinnhaftigkeit der Auswertungen ist zumindest teilweise fragwürdig (vgl. Fritsch 2021, S. 11). Es darf zum Beispiel bezweifelt werden, dass Beschäftigte und Teams, die nur mit wenigen anderen im Betrieb regelmäßig kommunizieren, zwangsläufig ineffektiv sind. Die im Produkt definieren Kriterien – etwa für Besprechungsstunden „niederer Qualität" – sind willkürlich. Das hindert Microsoft aber nicht daran, sogar die hypothetischen Kosten für als negativ eingeschätzte Verhaltensweisen wie Besprechungsstunden „niederer Qualität" darzustellen. Damit prägt das Produkt potenziell betriebliche Entscheidungen über den Arbeitsalltag. Heinz-Peter Höller und Peter Wedde (2018) haben sich in ihrer Publikation „Die Vermessung der Belegschaft. Mining the Enterprise Social Graph" mit derartigen Systemen und ihren Auswirkungen auseinandergesetzt. Während sie „lückenlos" die „direkten und indirekten Beziehungen zwischen den Beschäftigten in vielfältiger Weise auf Vorrat" festhalten, sei den Betroffenen oft nicht einmal „die bloße Existenz dieser umfassenden Datensammlungen" bekannt.

Microsoft „Productivity Score". Noch weiter als Workplace Analytics geht „Productivity Score" – auf Deutsch „Produktivitätsbewertung".[182] Dieses Produkt wird unabhängig von Workplace Analytics angeboten und bezieht neben Daten über Kommunikation und Besprechungen aus Outlook/Exchange und Teams auch Daten über die Nutzung von Word, Excel und PowerPoint sowie über die Handhabung von Dateien aus OneDrive mit ein. Neben dem Kommunikationsverhalten wird bewertet, wie Beschäftigte gemeinsam an Dateien arbeiten, sie erstellen, ändern, kopieren, teilen oder auf sie zugreifen.[183] Am Ende wird eine Punktebewertung für den Betrieb berechnet und mit Durchschnittswerten ähnlicher Unternehmen verglichen.[184] Das bedeutet, dass Microsoft diese Daten über Betriebe hinweg verarbeitet. Damit werden Beschäftigtendaten zum Produkt.

Der Verfasser der vorliegenden Studie hat das Produkt „Productivity Score" im November 2020 öffentlich scharf kritisiert, es als „vollwertiges Werkzeug zur Arbeitsplatz-Überwachung" bezeichnet – und die zur Verfügung gestellten Auswertungen und Metriken als „esoterisch".[185] Die darauf folgende umfassende globale Medienberichterstattung hat Microsoft dazu bewogen, einige besonders invasive Funktionen aus „Productivity Score" zu entfernen und sich dabei sogar öffentlich beim Verfasser zu bedanken.[186] Dies ändert allerdings wenig daran, dass Microsoft 365 weiterhin viele Aktivitäten von Beschäftigten aufzeichnet und Unternehmen vielfältige Zugriffsmöglichkeiten auf diese Daten bietet (siehe Abschnitt 5.3.4).

Direkte Nutzung von Kommunikationsdaten durch Clutter und Delve. Neben Auswertungen für Führungskräfte verarbeiten andere Produkte von Microsoft personenbezogene Daten über Kommunikation und Zusammenarbeit im Betrieb in einer Form, die bestimmte Funktionen erfüllen soll und unmittelbar auf die Beschäftigten zurückwirkt. Die Funktion „Clutter" in Outlook „lernt" etwa mittels kontinuierlicher Datenanalyse, welche E-Mails

[181] https://docs.microsoft.com/de-de/workplace-analytics/use/explore-metrics-external-collaboration [12.8.2021]
[182] https://docs.microsoft.com/de-de/microsoft-365/admin/productivity/productivity-score?view=o365-worldwide [14.8.2021]
[183] https://docs.microsoft.com/de-de/microsoft-365/admin/productivity/content-collaboration?view=o365-worldwide [14.8.2021]
[184] https://docs.microsoft.com/de-de/microsoft-365/admin/productivity/productivity-score?view=o365-worldwide [14.8.2021]
[185] https://twitter.com/WolfieChristl/status/1331221942850949121 [14.8.2021]
[186] Hern, Alex (2020): Microsoft apologises for feature criticised as workplace surveillance. The Guardian, 2.12.2020. Online: https://www.theguardian.com/technology/2020/dec/02/microsoft-apologises-productivity-score-critics-derided-workplace-surveillance

Beschäftigte als wichtig und prioritär behandeln sollen.[187] Delve wertet noch sehr viel weitreichendere Daten aus Microsoft 365 darüber aus, wer welche Dateien wann aufgerufen, bearbeitet oder per E-Mail-Anhang verschickt hat, um zu entscheiden, wie relevant eine Datei für eine bestimmte Person im Rahmen personalisierter Suchergebnisse ist. Die angezeigten Ergebnisse hängen davon ab, woran Beschäftigte „zuletzt gearbeitet haben, mit wem Sie zusammengearbeitet haben und an welchen Dokumenten diese Person gearbeitet hat".[188] Delve wertet damit Daten über Tätigkeiten und Kommunikation von ArbeitnehmerInnen aus – sowie über deren Beziehungen untereinander (vgl. Höller und Wedde 2018, S. 27; Fritsch 2021, S. 37).

5.8 Systeme zur Datenintegration und Analyse

Das digitale Zeitalter brachte eine massive Ausweitung der Erfassung und Auswertung personenbezogener Daten in vielen Lebensbereichen mit sich. Mit dem Schlagwort **Big Data** wird heute nicht nur die Speicherung und Zusammenführung großer Datenmengen beschrieben, sondern auch deren Analyse. Für das Auffinden verwertbarer Informationen in vorhandenen Datenbeständen wird oft der Begriff **Data Mining** verwendet – eine Analogie zur Gewinnung wertvollen Materials aus einer Mine (vgl. Christl und Spiekermann 2016). Derartige Begriffe mögen viel und gleichzeitig wenig aussagen, deuten jedoch auf Entwicklungen hin, die auch vor der Arbeitswelt nicht haltmachen. Daten über betriebliche Aktivitäten und damit oft über Beschäftigte und deren Tätigkeiten werden immer mehr zum Gegenstand digitaler Analyse. Die in einzelnen Systemen für bestimmte Zwecke verarbeiteten Daten bleiben dabei immer öfter nicht isoliert, sondern werden zusammengeführt, verknüpft und integriert. Aus Beschäftigtensicht ist diese Zusammenführung besonders unübersichtlich und heikel, weil damit potenziell mächtige Auswertungen für Zwecke möglich werden, die sehr weit von den Zwecken abweichen, für die die Daten ursprünglich erfasst wurden.

5.8.1 Ereignisprotokolle, Data Warehousing, Business Intelligence, Prozessanalyse

Für zentrale betriebliche Datenbanken, die nicht nur Informationen aus unterschiedlichen Unternehmensbereichen zusammenführen, sondern auch Funktionen zur Analyse und Auswertung bieten, wird seit einigen Jahrzehnten der Begriff des **Data Warehouse** verwendet – also des Daten-Warenlagers (vgl. Sen und Sinha 2005). Auch der Begriff der **Business Intelligence** wird schon länger verwendet, um Systeme zu beschreiben, die Daten aus dem Unternehmen in einer Form auswerten, die schlussendlich Entscheidungen des Managements unterstützen sollen.[189] Zu den bekannten Anbietern in diesem Bereich zählen SAP, Oracle und Microsoft.[190]

Am Ende zeigen derartige Auswertungen oft quantitative **Kennzahlen**, die darstellen, zu welchem Grad ein Unternehmen die Ziele erreicht, die erreicht werden sollen. Solche Kennzahlen können finanzielle Kriterien beschreiben, die zeitliche Dauer bestimmter Abläufe, Pünktlichkeit, Qualität, Kundenzufriedenheit oder beliebige andere Aspekte. Sie können sich auf das gesamte Unternehmen beziehen, auf bestimmte Abläufe, Standorte, Abteilungen oder Teams – oder gar nur auf einzelne Beschäftigte. Synonym werden Begriffe wie **Metrics** oder **Key Performance Indicators (KPIs)** verwendet.[191] Inwieweit diese Kennzahlen immer das aussagen, was sie vorgeben, auszusagen,

[187] https://support.microsoft.com/de-de/office/verwenden-der-funktion-clutter-zum-sortieren-von-nachrichten-mit-niedriger-priorität-in-outlook-7b50c5db-7704-4e55-8a1b-dfc7bf1eafa0 [14.8.2021]

[188] https://support.microsoft.com/de-de/office/wie-kann-delve-wissen-was-f%c3%bcr-mich-relevant-ist-048d502e-80a7-4f77-ac5c-f9d81733c385?ui=de-DE&rs=de-DE&ad=DE

[189] Kompakt-Lexikon Wirtschaftsinformatik. Springer Fachmedien Wiesbaden, Wiesbaden 2013

[190] Gartner (2021): Magic Quadrant for Analytics and Business Intelligence Platforms. Gartner, 15.2.2021

[191] Vgl. z.B. Ishaq Bhatti, M., Awan, H.M. & Razaq, Z. (2014): The key performance indicators (KPIs) and their impact on overall organizational performance. Qual Quant 48, 3127–3143, 2014. https://doi.org/10.1007/s11135-013-9945-y

sei an dieser Stelle dahingestellt. In jedem Fall werde sie verwendet und haben in Folge potenziell Auswirkungen auf Beschäftigte – insbesondere dann, wenn personenbezogene Daten mit einfließen. Auswertungen können entweder einmalig durchgeführt werden oder aber jederzeit aktuell verfügbar sein. Oft haben Führungskräfte Zugriff auf sogenannte **Dashboards**, die in der Optik eines Kontrollpults einen Überblick über den Stand der Dinge geben oder zumindest vorgeben, dies zu tun (vgl. Sánchez-Monedero und Dencik 2019, S. 31ff).

Eine wesentliche Grundlage für derartige Auswertungen sind die **Log-, Protokoll- und Ereignisdaten** aus unterschiedlichen betrieblichen Systemen, die meist sehr detaillierte Informationen über einzelne Arbeitsschritte enthalten. Ein Eintrag in einem Ereignisprotokoll („Event Log“) kann Informationen über eine bestimmte Aktivität enthalten – zum Beispiel „Bestellung erstellt“, „Kunde fordert Informationen an“, „E-Mail an den Kunden verschickt“, „Produkt ausgeliefert“, „Rechnung versandt“ und „Rechnung bezahlt“. Dazu werden Daten über die Person gespeichert, die die Aktivität durchgeführt hat oder die dafür verantwortlich ist – und natürlich ein Zeitstempel. Viele andere Attribute können enthalten sein – in diesem Fall etwa Kundennummern, Produktinformationen oder Rechnungsbeträge. SAP und viele andere Systeme zeichnen solche Daten auf (vgl. Claes und Poels 2014).

Wie derartige Ereignisprotokolle ausgewertet werden können, zeigt das Fallbeispiel in Abschnitt 6.3. **Celonis** verspricht unter dem Schlagwort **Process Mining**, betriebliche Abläufe zu analysieren und effizienter zu machen und stellt 80 vorgefertigte Module zur Verfügung, mit denen Ereignisprotokolle aus ERP-, HRM- oder CRM-Systemen von SAP, Oracle, Microsoft, Salesforce und anderen Herstellern in Echtzeit in Auswertungen einbezogen werden können. Beliebige andere Datenquellen können hinzugefügt werden. Celonis transformiert diese Rohdaten in Informationen über betriebliche Aktivitäten, Tätigkeiten und Arbeitsschritte, stellt verschiedene Varianten betrieblicher Abläufe dar und identifiziert „unerwünschte Aktivitäten“, die als ineffizient bewertet werden. Eine Produktdemonstration von Celonis zeigt, um welches Volumen an Aktivitäten es geht. Darin werden Daten über jeweils etwa eine Million aufgenommene Bestellungen, gescannte Rechnungen sowie gebuchte Rechnungen analysiert.

Während sich die Auswertungen meistens nicht direkt auf Einzelpersonen beziehen, werden umfassende personenbezogene Daten über Arbeitstätigkeiten verarbeitet. Außerdem können sich auch Auswertungen über Gruppen auf einzelne Beschäftigte auswirken – und auf ganze Belegschaften (vgl. Abschnitt 5.4.7). Wie klein der Schritt von der Auswertung auf Gruppenebene zur Leistungsbewertung einzelner ArbeitnehmerInnen ist, zeigt sich zudem darin, dass Celonis auch mit „Dashboards“ wirbt, die zum Beispiel Ranglisten namentlich genannter Beschäftigter anzeigen, gereiht nach dem Grad der Pünktlichkeit der Auslieferung der von ihnen bearbeiteten Bestellungen.

Neben Auswertungen für Führungskräfte können personenbezogene Daten aus Ereignisprotokollen oder aus anderen betrieblichen Datenbeständen auch in einer Weise genutzt werden, die direkt in den Arbeitsprozess zurückwirkt – zum Beispiel in Form von Vorgaben oder Handlungsempfehlungen. Celonis bietet etwa neben Analysen auch Funktionen, die Beschäftigten in Echtzeit Arbeitsaufgaben empfehlen, zuweisen oder priorisieren.

5.8.2 Cloud und SaaS, Plattformen und Apps, APIs und Schnittstellen

Die Art, wie Software entwickelt, betrieben und gewartet wird, hat sich in den letzten zwanzig Jahren rapide verändert – ebenso die Rolle, die die Hardware dabei spielt. Während ab den 1980er Jahren der PC dominant wurde, auf dem Programme installiert und dann isoliert auf dem Gerät ausgeführt wurde, erfolgt mit der Cloud quasi eine Rückkehr zum Mainframe – also in eine Zeit, in der alle Funktionen auf Großcomputern ausgeführt wurden und sich die Geräte der NutzerInnen weitgehend auf die Ein- und Ausgabe beschränkten (für den ganzen Abschnitt vgl. Gürses und Van Hoboken 2017; Wedde 2017).

Die **Cloud** – das sind einerseits die großen Rechenzentren von Amazon, Microsoft, Google, IBM oder Oracle[192] mit hunderttausenden untereinander vernetzten Servern, in denen Speicher- und Rechenkapazitäten nach Bedarf gemietet werden können. Andererseits wird unter der Bezeichnung **Software-as-a-Service (SaaS)** cloudbasierte Software in Form von digitalen Diensten angeboten, die vom Anbieter dieser Dienste betrieben und gewartet wird. Während viele Unternehmen weiterhin eigene Rechenzentren betreiben – oder sogenannte „private" Clouds nutzen, bei denen die Cloud-Infrastruktur von derjenigen anderer Unternehmen strikt abgeschottet ist – laufen immer mehr datenverarbeitende Systeme im Betrieb als reine SaaS-Dienste in der Cloud.

Führende Anbieter betrieblicher Software wie Microsoft oder SAP bieten ihre Software inzwischen auch als reine SaaS-Dienste an, bei anderen wie Salesforce oder Workday war dies von Anfang an der Fall. Diese Dienste können technisch unkompliziert mit den Diensten anderer Anbieter verbunden werden. Die Anbieter stellen dafür verschiedene Mechanismen zur Verfügung – von fix eingebauten Integrationen zwischen Diensten verschiedener Anbieter bis zu Programmierschnittstellen, die einen flexiblen automatisierten Zugriff auf Daten und Funktionen eines Diensts ermöglichen – die sogenannten **Application Programming Interfaces (APIs)**. So kann sich ein Betrieb modular ein System aus unterschiedlichen SaaS-Diensten unterschiedlicher Anbieter zusammenstellen, die nahtlos miteinander integriert sind, in Echtzeit Daten miteinander austauschen und schnell durch weitere Dienste erweitert werden können.

Viele Anbieter von SaaS-Diensten ermöglichen anderen Herstellern, die angebotenen Dienste durch zusätzliche Funktionen zu erweitern und werden damit zur **Plattform**, auf der ein Betrieb schnell zusätzliche „**Apps**" aktivieren kann. Sowohl große Anbieter wie Microsoft[193], SAP[194] oder Salesforce[195] als auch viele kleinere Anbieter[196] von SaaS-Diensten bieten heute „App Stores" an, mit denen Betriebe die angebotenen Systeme funktional erweitern können.

Auswirkungen auf Beschäftigte. Alle diese Entwicklungen führen dazu, dass die Unternehmen, die diese cloudbasierten Dienste einsetzen, keine direkte Kontrolle mehr darüber haben – weder über Hardware und Software noch über laufende Updates oder die Verarbeitung personenbezogener Daten. Oft hat nicht einmal die betriebliche IT-Abteilung mehr einen Überblick über das, was in der Cloud genau passiert. Funktionen und damit auch Datenverarbeitungspraktiken sind hochstandardisiert. Das, was früher als aufwändige Anpassung von Standardsoftware an betriebliche Bedürfnisse an der Tagesordnung war, tritt in den Hintergrund. Würden die Anbieter cloudbasierter Systeme die zur Verfügung gestellten Funktionen verantwortungsvoll und rechtskonform gestalten, könnte das aus Beschäftigtensicht theoretisch sogar Vorteile haben. Meist ist aber das Gegenteil der Fall. Wie mehrere Beispiele in der vorliegenden Studie zeigen, orientiert sich das, was an Funktionen zur Verfügung gestellt wird, oft am technisch machbaren, und ermöglicht zum Teil tiefe Eingriffe in die Rechte von ArbeitnehmerInnen. Manchmal passiert sogar genau das, was wir auch als VerbraucherInnen kennen – problematische Funktionen sind standardmäßig aktiviert und müssen vom Betrieb erst deaktiviert werden, damit das System rechtskonform betrieben werden kann.[197]

[192] Siehe z.B. https://cloudwars.co/cloud-wars-top-10-vendors-world/
[193] https://appsource.microsoft.com/
[194] https://store.sap.com/
[195] https://appexchange.salesforce.com/
[196] Siehe z.B. Abschnitt 6.1.5: Mehrere der beschriebenen Callcenter-Systeme stellen „App Stores" zur Verfügung.
[197] Siehe z.B. https://twitter.com/WolfieChristl/status/1331226122990866433

Laufende Updates und die schnelle und einfache Erweiterung der Systeme um mächtige Zusatzfunktionen oder durch komplette Dienste anderer Hersteller führen dazu, dass Beschäftigte und Betriebsrat kaum mehr nachvollziehen oder überprüfen können, welche personenbezogenen Daten zu welchen Zwecken verarbeitet werden – und welcher Anbieter sie überhaupt verarbeitet. Am Ende besteht die Gefahr, dass sich niemand mehr verantwortlich fühlt. Die Anbieter der cloudbasierten Systeme waschen ihre Hände in Unschuld und schieben dem Betrieb die Verantwortung dafür zu, wie die zur Verfügung gestellten Funktionen konkret eingesetzt werden. Die Betriebe verweisen auf den Anbieter und behaupten, selbst nicht genau zu wissen, welche Daten an welcher Stelle verarbeitet werden. Darüber hinaus wird etwa behauptet, bestimmte vom Betriebsrat geforderte Änderungen seien schlicht nicht machbar, weil der Dienst des Anbieters dies gar nicht zulasse.

Datenverarbeitung über Betriebe hinweg. Manche cloudbasierten Dienste ermöglichen nicht nur einzelnen Betrieben, Beschäftigtendaten aus unterschiedlichen Systemen und Unternehmensbereichen zusammenzuführen und auszuwerten, sondern nutzen die Daten über Betriebe hinweg für eigene geschäftliche Zwecke. So bewirbt etwa Peakon, eine Tochterfirma von Workday, ein Produkt für Mitarbeiterumfragen als „weltweit größte[n] standardisierte[n] Datensatz aus Mitarbeiterfeedback“, der auf fast 180 Millionen beantworteten Umfragen in unterschiedlichen Betrieben basiere (siehe Abschnitt 5.4.10). Humanyze, eine Firma, die mit tragbaren Geräten Sprache, Interaktionen und Bewegungen im Büro analysiert, gibt an, dass deren Software auf dem „global größten Datenset für Verhaltensweisen am Arbeitsplatz“ basieren würde (siehe Abschnitt 6.6.1). Auch Microsoft wertet Daten über Betriebe hinweg aus, um etwa Kennzahlen über die Nutzung von Microsoft 365 durch die Belegschaften verschiedener Betriebe zu vergleichen (siehe Abschnitt 5.7.3). Damit werden Beschäftigtendaten zum Produkt.

5.8.3 Branchen-, tätigkeits- und zweckspezifische Systeme

Wie mehrere Beispiele in der vorliegenden Studie zeigen, führen verschiedene Arten branchen-, tätigkeits- oder zweckspezifischer Systeme umfassende Beschäftigtendaten zusammen und ermöglichen invasive Auswertungen.

Einerseits beziehen manche Systeme für Zwecke der IT-Sicherheit oder zur Verhinderung von Betrug, Diebstahl und anderen unerwünschten Verhaltensweisen von ArbeitnehmerInnen personenbezogene Daten aus vielen betrieblichen Systemen in permanente Risikobewertungen mit ein – was einer Totalüberwachung des Arbeitsalltags gleichkommen kann (siehe Abschnitt 5.6). Andererseits spielen etwa die Produkte von Microsoft eine derart wichtige Rolle in vielen Betrieben, dass die innerhalb der cloudbasierten Dienste von Microsoft 365 gesammelten und ausgewerteten Daten über Arbeitstätigkeiten für sich alleine bereits eine sehr weitreichende Zusammenführung von Daten im Betrieb darstellen können. Microsoft 365 stellt Betrieben mit der „Graph API“ umfassende Aktivitätsdaten zur Verfügung und bietet eine Vielzahl an Auswertungsmöglichkeiten (siehe Abschnitte 5.3.4 und 5.7.3).

Ähnliches trifft auf mächtige Systeme wie SAP oder Workday zu – und auf viele branchenspezifische Systeme wie etwa Callcenter-Systeme (siehe Abschnitt 6.1), die ebenfalls für sich alleine bereits umfassende Daten über die Arbeitstätigkeiten von Beschäftigten verarbeiten, zusammenführen und auswerten.

6. Fallstudien über am Markt verfügbare Systeme

Welche Funktionen bieten die Produkte konkreter Hersteller und wie können sie eingesetzt werden? Im Rahmen der vorliegenden Studie wurde eine Auswahl von am Markt verfügbaren datenverarbeitenden Systemen in unterschiedlichen Branchen und für unterschiedliche Aufgabenbereiche näher untersucht – auf Grundlage einer Analyse öffentlich verfügbarer Informationen, technischer Dokumentationen und anderer Literatur (siehe auch Abschnitt 0).

Umfang und Reichweite der Fallbeispiele sind unterschiedlich. Der Abschnitt über algorithmische Kontrolle im Callcenter dokumentiert etwa sehr umfassend die Funktionen von Systemen, die in einem bestimmten Tätigkeitsbereich in einer bestimmten Branche eingesetzt werden. Andere Abschnitte beschreiben Produkte, die bestimmte Aufgabenbereiche abdecken (z.B. Verhaltensdaten für IT-Sicherheit) oder bestimmte Arten personenbezogener Daten für bestimmte Zwecke verarbeiten (z.B. Körper und Verhaltensdaten für Arbeitssicherheit und –gesundheit).

6.1 Überwachung und algorithmische Kontrolle im Callcenter

Das Callcenter gilt schon lange als Prototyp einer Arbeitsumgebung, in der Beschäftigte einer sehr weitgehenden Rundum-Überwachung ausgesetzt sind. Daten über Telefonate und andere Arbeitstätigkeiten werden nicht nur akribisch erfasst und ausgewertet, sondern oft auch in unterschiedlicher Weise zur Leistungskontrolle eingesetzt. Die Notwendigkeit dieser Kontrollmaßnahmen wird meist mit betrieblichen Zwecken argumentiert – von der Sicherstellung eines reibungslosen und effizienten Betriebs bis zur Qualitätssicherung (vgl. Kiesche und Wilke 2012).

Vom Callcenter zum Contact Center. Es ist eine Reihe von cloudbasierten Software-Systemen verfügbar, die den täglichen Betrieb eines Callcenters teilweise bis beinahe vollständig organisieren, steuern und kontrollieren. Zu bekannten Systemen bzw. Anbietern zählen Genesys, Five9, Talkdesk, NICE inContact, Lifesize, Aspect – aber auch große Konzerne wie Cisco und Amazon. Neben eingehenden („Inbound“) und ausgehenden („Outbound“) Telefonaten werden oft auch andere digitale Kanäle wie E-Mail, Chat oder gar Social Media unterstützt.[198] Das Callcenter wird damit zum „Contact Center“.

Der Einsatz erfolgt für unterschiedliche betriebliche Zwecke von Kundenservice bis Verkauf. Der Übergang zwischen Systemen für den Betrieb eines Contact Centers und Software für Customer Relationship Management (CRM), betriebsinterne Dienstleistungen („Helpdesk“) oder ganz allgemein für Kommunikation ist ein fließender.[199] Daneben existieren große Outsourcing-Anbieter wie Saham (früher Bertelsmann Arvato), Majorel, Teleperformance, Sitel, Webhelp oder Bosch, an die Firmen ihre Callcenter oder gleich die komplette Kundenbetreuung auslagern[200] – und die wohl meist ihre eigene Software einsetzen. Was alle diese Systeme vereint, ist ein Fokus auf

[198] Vgl. z.B. Blood, Steve; Kraus, Drew; Rathnayake, Pri (2020): Magic Quadrant for Contact Center as a Service. Gartner, 9.11.2020. Online: https://www.gartner.com/en/documents/3992865/magic-quadrant-for-contact-center-as-a-service, Schoeller, Art; Hong, Daniel; Sjoblom, Sara; Harrison, Peter (2020): The Forrester Wave™: Contact-Center-As-A-Service (CCaaS) Providers, Q3 2020. Forrester, 26.8.2020. Online: https://www.forrester.com/report/The+Forrester+Wave+ContactCenterAsAService+CCaaS+Providers+Q3+2020/-/E-RES157463

[199] Vgl. z.B. Schoeller, Art (2016): Increase Customer Service Agility With Cloud Contact Centers. Forrester, 15.7.2016. Online: https://www.forrester.com/report/Increase+Customer+Service+Agility+With+Cloud+Contact+Centers/-/E-RES121402

[200] Vgl. z.B. Hung, Shirley; Sharma, Sharang; Biswas, Chhandak (2020): Customer Experience Management (CXM) – Service Provider Landscape in EMEA with Services PEAK Matrix® Assessment 2020. Everest Group, 29.9.2020. Online: https://www2.everestgrp.com/reportaction/EGR-2020-21-R-3965/Marketing, PwC (2020): Die Zukunft des deutschen Contact-Center- und CRM-Markts. PwC Studie, 2020. Online: https://www.pwc.de/de/im-fokus/customercentrictransformation/die-zukunft-des-deutschen-contact-center-und-crm-marktes.pdf

Effizienzsteigerung und Kostensenkung durch Funktionen, die eine engmaschige Kontrolle der Tätigkeiten von ArbeitnehmerInnen ermöglichen.

6.1.1 Steuerung und Leistungskontrolle mit der Software von „Genesys“

Das US-Unternehmen Genesys ist mit über 5.000 MitarbeiterInnen[201] und mehreren europäischen Niederlassungen[202] einer der größeren Anbieter von Software zum Betrieb von Contact Centern. Zu den Kunden zählen laut Eigenangabe unter anderem PayPal, BMW, Bosch, Philips, Vodafone, Swisscom, A1 Telekom Austria und Conrad Electronic.[203] Das System bietet eine Vielzahl von Funktionen von der automatisierten Zuweisung von Anrufen an Beschäftigte – die sogenannten „Agents“ – bis zur Vorhersage der Auslastung, der Planung des benötigten Personals und der umfassenden Leistungskontrolle.[204] Daten über Arbeitstätigkeiten werden sekundengenau aufgezeichnet und können sowohl in Echtzeit als auch über längere Zeiträume hinweg ausgewertet werden.

Folgende Abbildung (links oben) zeigt einen Ausschnitt aus der Benutzeroberfläche von Genesys. In diesem Beispiel können Führungskräfte in Echtzeit Listen mit personenbezogenen Informationen über Callcenter-Agents einsehen – etwa nach der aktiven Zeit, der Zahl der bearbeiteten Anrufe und der Sprechdauer. Auch eine Rangliste der Beschäftigten, die ihre Leistung in Form eines Prozentwerts darstellt, steht zur Verfügung:[205]

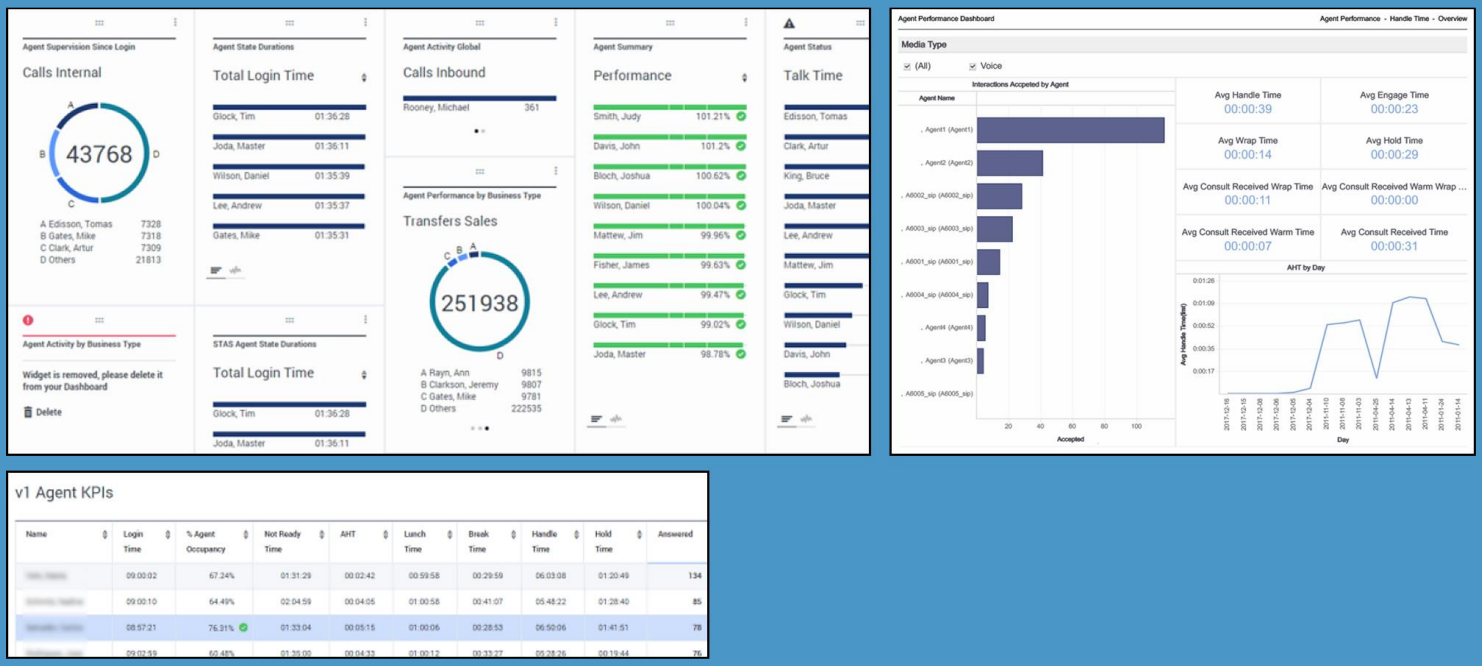


Abbildung 2: Einblicke in Verhaltensdaten von Beschäftigten beim Callcenter-System Genesys. Quelle: Hersteller

[201] https://www.genesys.com/company [22.5.2021]
[202] https://www.genesys.com/global-offices [22.5.2021]
[203] https://www.genesys.com/customer-stories [22.5.2021]
[204] https://www.genesys.com/capabilities [22.5.2021]
[205] Alle Abbildungen (c) Genesys. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quellen: Genesys Pulse 8.5.01, 13.3.2020, S. 6: https://docs.genesys.com/Documentation/EZP/8.5.01/User/Welcome?action=pdfbook [22.5.2021], Genesys Engage, Customer Experience Insights, Agent Performance Dashboard: https://docs.genesys.com/Documentation/GCXI/9.0.0/User/HRCXIAgntPerfDshbrd [22.5.2021], Genesys Pulse 9.0.0, 9.3.2021, S. 30: https://docs.genesys.com/Documentation/EZP/latest/User/Welcome?action=pdfbook&title=Documentation:EZP:User:Welcome:9.0.0 [22.5.2021]

Eine Vielzahl an Leistungskennzahlen. Abbildung 2 (links unten) zeigt auch eine Auswertung in Tabellenform, die für einzelne Beschäftigte folgende Kennzahlen anzeigt – sekundengenau und sortierbar:

- Gesamte Zeit, in der die Person in der Schicht im System eingeloggt war („Login Time“)
- Zeit, in der die Person das System auf „Pause“ oder „Mittagspause“ gestellt hatte
- Zeit, in der die Person nicht telefoniert hat und nicht bereit war, Anrufe anzunehmen („Not Ready Time“)
- Durchschnittliche Dauer der Gespräche („Average Handle Time“, AHT)
- Gesamte Zeitdauer der Gespräche („Handle Time“)
- Zeit, in der die Person ein Telefonat auf „Halten“ gestellt hat („Hold Time“)
- Anzahl der bearbeiteten eingehenden Gespräche

Was in den Auswertungen angezeigt wird, lässt sich anpassen. Es sind viele weitere Kennzahlen verfügbar, etwa:[206]

- Anteil Gesprächszeit im Verhältnis zur gesamten eingeloggten Zeit („Occupancy“)
- Zahl der Gespräche, die der Person angeboten wurden
- Zahl der Gespräche, die die Person angenommen hat
- Zeit, die die Person mit der Nachbearbeitung von Gesprächen verbracht hat
- Summe der Zeit, die die Person mit dem Wählen der Zielnummer verbracht hat
- Summe der Zeit, die die Person einen eingehenden Anruf hat warten lassen
- Zahl der AnruferInnen, die aufgelegt haben, während die Person den Anruf hat warten lassen
- Zahl der Gespräche, die an andere Beschäftigten weitergegeben wurden
- Zahl und Zeit der internen beratenden Telefonate für Rückfragen
- Zahl der Gespräche, die weniger als zehn Sekunden gedauert haben

Abbildung 2 (rechts oben) zeigt eine weitere Rangliste der Callcenter-Agents – sortiert nach der Zahl der angenommenen Gespräche bzw. Interaktionen – und diverse Durchschnitts-Kennzahlen für das gesamte Team. Genesys bezeichnet solche beschäftigtenspezifischen Auswertungen offenherzig als „Dossiers“.[207] Auch für die Auswertung von längerfristigen Verhaltensdaten steht eine große Zahl unterschiedlicher Berichte zur Verfügung[208] – etwa über Verhalten[209] und Produktivität[210] der Agents. Mit diesen Auswertungen wird eine umfassende Leistungskontrolle möglich, die jeden Arbeitsschritt bewertet und die Beschäftigten miteinander vergleicht. Gleichzeitig geht das System über die reine Überwachung von Arbeitstätigkeiten hinaus.

Algorithmische Kontrolle. Gespräche und andere Interaktionen – und damit der Großteil der Arbeitstätigkeiten – werden automatisiert zugewiesen und gesteuert. Genesys gleicht dazu bei der Zuweisung von Gesprächen die im System hinterlegten „Skills“ der Agents wie etwa Sprachkenntnisse oder Erfahrungen mit bestimmten Produkten

[206] Genesys Pulse 9.0.0 Documentation, 9.3.2021, S. 41ff: https://docs.genesys.com/Documentation/EZP/latest/User/Welcome?action=pdfbook&title=Documentation:EZP:User:Welcome:9.0.0 [22.5.2021]
[207] https://docs.genesys.com/Documentation/GCXI/9.0.0/User/HRCXIAgntPerfDshbrd [22.5.2021]
[208] https://help.genesys.com/pureconnect/mergedprojects/wh_rh/desktop/interaction_reporter_reports.htm [22.5.2021]
[209] https://help.genesys.com/pureconnect/mergedprojects/wh_rh/desktop/schedule_adherence_and_conformance_detail_report.htm [22.5.2021]
[210] https://help.genesys.com/pureconnect/mergedprojects/wh_rh/desktop/user_productivity_summary_and_detail.htm [22.5.2021]

mit vorhandenen Kundendaten ab.[211] Das Unternehmen verspricht auch, mit Hilfe umfassender Verhaltensdaten und Methoden der künstlichen Intelligenz dafür zu sorgen, dass jedes Gespräch genau dem Agent zugewiesen wird, der es laut Vorhersage am effektivsten und am schnellsten abwickelt.[212] Über die einzelnen Arbeitsschritte hinaus stellt Genesys komplexe Funktionen zur teilautomatisierten Steuerung von Tätigkeiten innerhalb einzelner Schichten sowie zur Verwaltung von kurz- und längerfristigen Schichtplänen zur Verfügung.[213] Historische Daten können zur Vorhersage und Simulation von Auslastung sowie für die langfristige Personalplanung genutzt werden. Darüber hinaus wird „smartes" und effizientes „just-in-time hiring" auf Basis von „week-over-week data" angeregt – also das kurzfristige Anstellen von Personal nach wöchentlichem Bedarf.[214] Mit dem „Interaction Scripter" können die Gespräche der Agents digital strukturiert werden – von einfachen Gesprächsleitfäden mit Textbausteinen bis zu komplexen Abläufen inklusive Dateneingabe.[215]

6.1.2 Aufzeichnung von Gesprächen und Bildschirmaktivitäten

Neben der bereits sehr weitgehenden Auswertung von Daten über Gespräche und Arbeitstätigkeiten bietet Genesys an, alle Gespräche aufzuzeichnen und mittels automatisierter Transkription in auswertbare Gesprächsprotokolle zu übersetzen – im Namen von Qualitätssicherung, Kundenzufriedenheit, Schulung der Belegschaft und „Compliance".[216] Sogar die Bildschirmaktivitäten der Beschäftigten können aufgezeichnet werden. Die Formulierungen auf der Website von Genesys sind dabei verräterisch. Denn sie schlagen vor, die Funktionen auch für die Leistungskontrolle einzusetzen: „Bewahren Sie jede aufgezeichnete Interaktion für Compliance-Zwecke und mögliche rechtliche Probleme auf. Dies macht es einfach, die Produktivität der Agents zu überwachen".[217] Firmen sollen für die Qualitätssicherung „alle Interaktionen aufzeichnen und speichern", daraus „Schlüsselerkenntnisse" gewinnen und diese für „Handlungen" nutzen – zum Beispiel zur Schulung von Beschäftigten.[218] Genesys betont, dass das Mithören oder Einsehen der Protokolle durch Vorgesetzte auch ohne Wissen der Agents möglich sei.[219]

6.1.3 Schlüsselwörter, Stimmung und Scoring von Gesprächen

Die Protokolle der transkribierten Gespräche und anderer Interaktionen wie E-Mails oder Chats können nach Stichwörtern durchsucht werden – über den letzten Tag, einen Monat oder über die gesamte Datenbank hinweg.[220] Darüber hinaus können Schlüsselwörter und Phrasen definiert werden, die dann automatisiert in Gesprächen erkannt werden sollen – das sogenannte „**Keyword Spotting**". So kann etwa überprüft werden, ob ein zu verkaufendes Produkt, ein Mitbewerber oder Begriffe wie „kaufen", „kündigen" oder „verklagen" erwähnt wurden. Dabei werden sowohl die Sprechanteile der KundInnen als auch die der Beschäftigten analysiert. Es kann überprüft werden, ob die Agents die vorgesehenen Phrasen für Begrüßung und Verabschiedung benutzt haben oder ob sie als unangemessen betrachtete Formulierungen wie „beruhigen sie sich", „sie hören nicht zu" oder „ich bin neu hier" verwendet

[211] https://help.genesys.com/pureconnect/mergedprojects/wh_dlr/mergedprojects/dialer_manager_help2/desktop/skills_based_dialing_and_routing.htm [22.5.2021]
[212] https://www.genesys.com/capabilities/automated-routing [22.5.2021]
[213] https://all.docs.genesys.com/PEC-WFM/Current/Administrator/Scheduling [22.5.2021]
[214] https://www.genesys.com/capabilities/long-term-workforce-planning [22.5.2021]
[215] https://help.genesys.com/pureconnect/mergedprojects/wh_dlr/mergedProjects/scripter_dg/desktop/what_is_interaction_scripter.htm [22.5.2021]
[216] https://www.genesys.com/capabilities/quality-assurance-and-monitoring [22.5.2021]
[217] Ebd. Übersetzung durch den Verfasser, im englischen Original: "Keep every recorded interaction on hand for compliance and legal efforts. This makes it easy to monitor agent productivity"
[218] Ebd. Übersetzung durch den Verfasser, im englischen Original: „Record and store every interaction and study them for key insights. Turn these insights into action items. Use your data for coaching, assigned learning and more"
[219] https://docs.genesys.com/Documentation/IW/8.5.1/User/MonitorCoachAndBarge-inInteractions [22.5.2021]
[220] https://docs.genesys.com/Documentation/IW/latest/Help/Interaction_Search [22.5.2021]

haben.[221] Die definierten Phrasen werden Gruppen zugeordnet und mit positiven oder negativen Punktewerten versehen, damit später berechnet werden kann, **wie positiv oder negativ die Stimmung** im Gespräch war.[222] Begriffe wie „perfekt“, „großartig“ oder „danke“ können etwa positiv bewertet werden, andere Begriffe wie „inakzeptabel“, „lächerlich“ oder „unfair“ negativ.[223] Genesys unterstützt viele Sprachen, auch Deutsch.[224] Die Dokumentation geht darauf ein, wie sich die Qualität der Worterkennung verbessern lässt.[225] Während manche Dialekte eventuell nicht sehr zuverlässig erkannt werden dürften, können die Agents natürlich dazu angehalten werden, sauber zu sprechen.

Die in den Gesprächsprotokollen erkannten Wörter und Phrasen samt deren positiver oder negativer Bewertung stehen in Folge für Auswertungen zur Verfügung. Abbildung 3 (rechts) zeigt eine Auswertung, in der einzelne Gespräche einzelner Agents in Hinblick auf Schlüsselwörter, die mit positiver oder negativer Kundenzufriedenheit verbunden sind, bewertet werden. Für die Sprechanteile der Agents und KundInnen werden separate Scores berechnet. In Summe ergibt sich ein Gesamt-Score für jedes Gespräch. So hat etwa ein Agent ein Gespräch in der Länge von 3 Minuten und 24 Sekunden geführt. Beim Gegenüber wurde ein Kundenzufriedenheits-Score von -30 berechnet. Der Agent konnte die Situation zwar etwas entschärfen – eventuell mit als positiv und beruhigend eingeschätzten Worten – wurde aber mit einem Score von nur 27 bewertet, womit sich für das Gespräch ein negativer Score von -3 ergibt. Folgende Abbildung (links) zeigt zudem, wie bei einem aufgezeichneten Gespräch sekundengenau die Momente markiert werden, in denen als positiv oder negativ bewertete Schlüsselwörter oder Phrasen erkannt wurden. Vorgesetzte können das Gespräch nachhören und Anmerkungen zu Gesprächsteilen hinzufügen:[226]

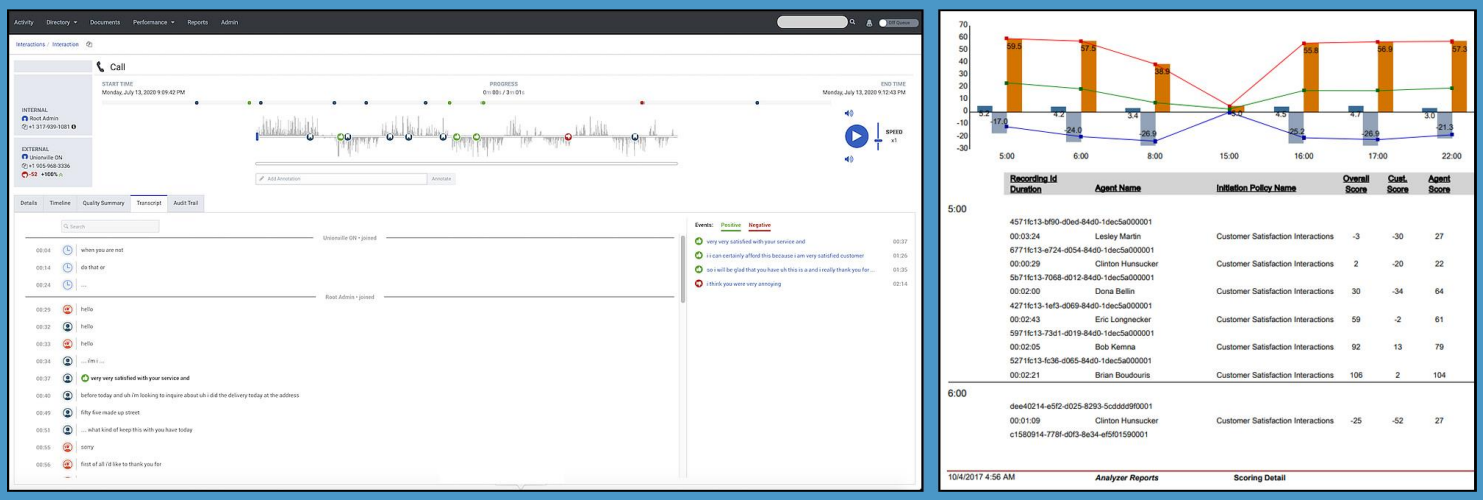


Abbildung 3: Überwachung von Callcenter-Gesprächen, Schlüsselwörtern und Stimmung bei Genesys. Quelle: Hersteller

[221] https://help.genesys.com/pureconnect/mergedprojects/wh_tr/mergedprojects/wh_tr_analyzer/desktop/appendix_a_interaction_analyzer_keyword_examples.htm [22.5.2021]

[222] https://help.genesys.com/pureconnect/mergedprojects/wh_tr/mergedprojects/wh_tr_analyzer/desktop/set_the_score_for_a_keyword.htm [22.5.2021]

[223] https://help.genesys.com/pureconnect/mergedprojects/wh_tr/mergedprojects/wh_tr_analyzer/desktop/appendix_a_interaction_analyzer_keyword_examples.htm [22.5.2021]

[224] https://help.genesys.com/pureconnect/mergedprojects/wh_tr/mergedprojects/wh_tr_analyzer/desktop/language_support_for_interaction_analyzer_keyword_spotting.htm [22.5.2021]

[225] https://help.genesys.com/pureconnect/mergedprojects/wh_tr/mergedprojects/wh_tr_analyzer/desktop/interaction_analyzer_keyword_entry.htm [22.5.2021]

[226] Alle Abbildungen (c) Genesys. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quellen: https://www.genesys.com/blog/post/genesys-cloud-feature-releases-whats-new-in-september-2020 [22.5.2021], S. 10: https://help.genesys.com/pureconnect/mergedprojects/wh_rh/desktop/scoringdetailgenesys.pdf [22.5.2021]

Auch Momente der Stille oder Gesprächsphasen, in denen eine Person einer anderen ins Wort gefallen ist, können automatisiert erkannt werden.[227]

Wie Kiesche und Wilke (2012) schon vor beinahe einem Jahrzehnt geschrieben haben, greift eine derart intensive Überwachung von Gesprächen samt automatisierter Erkennung von Schlüsselwörtern und Stimmung tief in die Persönlichkeitsrechte der Beschäftigten ein. Stellen die in den vorangehenden Abschnitten beschriebenen Funktionen zur Leistungsbewertung auf Basis der Zahl und Dauer abgearbeiteter Telefonate schon eine sehr weitgehende Form digitaler Kontrolle von Arbeitstätigkeiten dar, geht eine Verhaltens- und Leistungskontrolle auf Basis jedes einzelnen gesprochenen Worts noch einmal darüber hinaus.

Die Technologie kann potenziell natürlich auch für Zwecke abseits der Leistungskontrolle eingesetzt werden – zum Beispiel zur gezielten Überwachung einzelner Beschäftigter oder der gesamten Belegschaft.

6.1.4 Laufende „Evaluierung" und Anreize zur Leistungssteigerung

Unter Schlagworten wie „Workforce Optimization" (WFO) und „Workforce Engagement Management" (WEM) bietet Genesys weitere Funktionen, die der Steuerung und der Erhöhung der Leistung der Belegschaft dienen. „Positive Verhaltensweisen" sollen „erkannt und belohnt" werden – und zwar auf Basis der aufgezeichneten Verhaltensdaten. Durch kontinuierliches „Feedback" soll die Arbeitsleistung verbessert werden[228] – etwa in Form von regelmäßigen „Evaluierungen" von Gesprächen und anderen Interaktionen.[229] Auch ein eigenes Softwaremodul für laufende Schulungen wird angeboten.[230]

Anreiz- und Belohnungsmechanismen zur Leistungssteigerung. Dazu steht unter dem Schlagwort „Gamification" eine ganze Reihe von Anreiz- und Belohnungsmechanismen zur Verfügung, die die Beschäftigten motivieren sollen, Vorgaben für Kennzahlen zu erreichen. Ihr „natürliches Bedürfnis" nach Konkurrenz solle genutzt werden und sie sollen „ermächtigt" werden, „sich selbst zu managen" – etwa durch tägliche Ziele und Wettbewerbe. Dafür stellt Genesys ein Punktesystem samt Spielmechanismen wie Abzeichen („Badges") und Ranglisten („Leaderboards") zur Verfügung.[231]

Folgende Abbildung zeigt, wie den Beschäftigten Kennzahlen, Punkte und Leistungsvergleiche angezeigt werden. Eine gute Punktebewertung ergibt sich in diesem Beispiel durch eine Minimierung der Nachbearbeitungszeit von Gesprächen („After Call Work Time Ratio"), eine Minimierung der Dauer von gehaltenen Gesprächen („Average Hold Time") und eine Minimierung von Weiterleitungen von Gesprächen an KollegInnen („Calls Transferred Ratio"). Dazu werden im Verlauf des Arbeitstages nach bestimmten Kriterien Punkte vergeben oder eben nicht. Die Punktebewertung wird im Vergleich zu persönlichen Bestwerten und den Bestwerten von KollegInnen dargestellt – pro Tag, pro Woche und pro Monat – und durch eine Rangliste ergänzt:[232]

[227] https://all.docs.genesys.com/PEC-REC/Current/User/interactions [22.5.2021]
[228] https://www.genesys.com/capabilities/wem-workforce-engagement-management [22.5.2021]
[229] https://all.docs.genesys.com/PEC-REC/Current/User/evaluationsession [22.5.2021]
[230] https://docs.genesys.com/Documentation/GTM [22.5.2021]
[231] https://www.genesys.com/capabilities/gamification-call-center-employees [22.5.2021]
[232] Alle Abbildungen (c) Genesys. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle: https://www.genesys.com/capabilities/employee-performance-management-tools [22.5.2021]

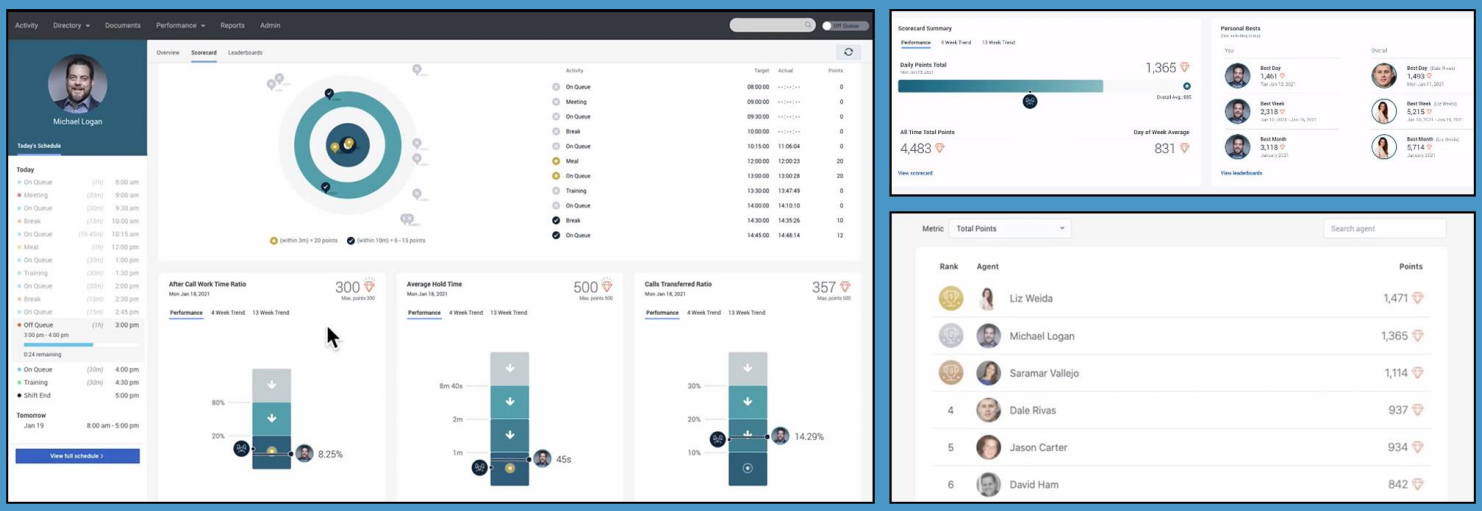


Abbildung 4: Darstellung von Ranglisten und Leistungskennzahlen für Callcenter-Agents bei Genesys. Quelle: Hersteller

Ergänzend können Kennzahlen auch auf für alle einsehbaren Bildschirmen im Großraumbüro angezeigt werden.[233]

6.1.5 Weitere Systeme und Funktionen, Überlappung mit militärischer Technologie

Andere Callcenter-Systeme bieten ähnliche Funktionen. **Five9**, das laut Eigenangabe etwa von Siemens[234] genutzt wird, bietet ebenfalls umfassende Funktionen zur Echtzeitüberwachung[235], Leistungsbewertung[236] und zur Aufzeichnung von Gesprächen und Bildschirminhalten.[237] Jedes Gespräch und jede Interaktion, die die Beschäftigten bearbeiteten, wird mit einem Score bewertet.[238] Bei den Lösungen für Schicht- und Personalplanung wird betont, man helfe dabei, „overstaffing" – also ein Zuviel an Personal – zu verhindern.[239]

Der Hersteller **NICE** betont ebenfalls, man helfe „overstaffing" zu verhindern und „labor waste" – also die Verschwendung von Arbeitskraft – zu reduzieren.[240] Auch bei NICE können Gespräche und Bildschirminhalte aufgezeichnet[241], Stimmungslagen analysiert[242] und Arbeitsleistung ausgewertet werden.[243] Teile des Systems von NICE werden laut Eigenangabe von Teleperformance eingesetzt, einem großen französischen Outsourcing-Anbieter, der 150.000 Agents in 400 Callcentern in 80 Ländern beschäftigt.[244] NICE hat ursprünglich Überwachungstechnologie

[233] https://all.docs.genesys.com/PEC-REP/Current/RT/RTRUserAccess
[234] https://www.five9.com/customers [23.5.2021]
[235] https://www.five9.com/products/capabilities/supervisor-desktop [23.5.2021]
[236] https://www.five9.com/products/capabilities/performance-management-dashboard [23.5.2021]
[237] https://www.five9.com/products/capabilities/quality-management [23.5.2021]
[238] Ebd.
[239] https://www.five9.com/resources/easset_upload_file20578_88851_e.pdf [23.5.2021]
[240] https://www.niceincontact.com/call-center-software/workforce-engagement/workforce-management [23.5.2021]
[241] https://www.niceincontact.com/call-center-software/workforce-engagement/call-recording [23.5.2021]
[242] https://www.niceincontact.com/call-center-software/analytics/interaction-analytics [23.5.2021]
[243] https://www.niceincontact.com/call-center-software/workforce-engagement/performance-management [23.5.2021]
[244] https://www.nice.com/optimizing-customer-engagements/Lists/CustomerSuccesses/Attachments/263/teleperformance_bumi-com_case_study_us.pdf [23.5.2021]

für Geheimdienste und Militär hergestellt[245] und verkauft heute neben Angeboten zur Durchleuchtung und Profilierung von VerbraucherInnen[246] immer noch Produkte für öffentliche Sicherheit, Polizei und Strafverfolgung.[247]

Staatliche, betriebliche und kommerzielle Überwachung. Noch deutlicher sind die Querverbindungen zwischen staatlicher Massenüberwachung und digitaler Kontrolle von ArbeitnehmerInnen bei Verint, einem börsenotierten US-Konzern, der einerseits ein wichtiger Anbieter in den Bereichen Qualitätssicherung[248], Aufzeichnung und Analyse von Gesprächen[249], Leistungskontrolle und Personalverwaltung für Callcenter ist.[250] Andererseits hat Verint Telefonüberwachungstechnologie an den US-Geheimdienst NSA geliefert, wie 2013 berichtet wurde,[251] für Interpol die wahrscheinlich global größte biometrische Stimmerkennungsdatenbank entwickelt[252] und laut Berichten von NGOs immer wieder Überwachungstechnologie an autoritäre Staaten in aller Welt geliefert.[253] Zudem befasst sich Verint wie die meisten Hersteller von Systemen für den Betrieb von Contact Centern, Verkauf und Kundensupport nicht nur mit der Überwachung von ArbeitnehmerInnen, sondern auch mit der Durchleuchtung und Profilierung von VerbraucherInnen.[254]

Von der Callcenter-Software zur „Plattform". Wie viele cloudbasierte Systeme bieten Hersteller von Software zum Betrieb von Contact Centern heute oft einfache Möglichkeiten der Ein- und Anbindung von Drittsoftware – etwa mit Hilfe von API-Schnittstellen oder in Form von „Apps". Genesys[255], Five9[256] oder Talkdesk[257] betreiben etwa umfangreiche „App Stores", mit denen Unternehmen die Funktionen dieser Callcenter-Plattformen schnell erweitern können – von Aufzeichnung und Datenanalyse über Reporting bis Personaloptimierung. Diese Drittsoftware bietet manchmal noch weit invasivere Funktionen als die Plattformen selbst.

Umgekehrt bieten große Tech-Konzerne ihre intern entwickelten und genutzten Systeme an andere Unternehmen an. So stellt **Amazon** etwa ein cloudbasiertes Contact Center zur Verfügung, das ebenfalls Funktionen wie die Aufzeichnung von Gesprächen, Sprach- und Stimmungsanalyse, Volltextsuche in Gesprächsprotokollen und Kennzahlen für Verhalten und Verkäufe bietet und damit „datengestützte Entscheidungen zum Erhöhen der Mitarbeiterproduktivität" ermöglicht.[258]

---

[245] https://web.archive.org/web/20071022204124/http://www.nice.com/news/newsletter/6_03s/anniversary.php
[246] https://www.nice.com/optimizing-customer-engagements/Documents/nx_CJO_brief_footprints.pdf [23.5.2021]
[247] https://www.nice.com/protecting/public-safety/ [23.5.2021]
[248] https://www.verint.com/engagement/our-offerings/solutions/workforce-optimization/automated-quality-management/ [23.5.2021]
[249] https://www.verint.com/engagement/our-offerings/solutions/workforce-optimization/intelligent-recording/ [23.5.2021]
[250] https://www.verint.com/engagement/our-offerings/solutions/workforce-optimization/ [23.5.2021]
[251] Brewster, Thomas (2020): Israeli Surveillance Companies Are Siphoning Masses Of Location Data From Smartphone Apps. Forbes, 11.12.2020. Online: https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps
[252] Kofman, Ava (2018): Interpol rolls out international voice identification database using samples from 192 law enforcement agencies. The Intercept, 25.6.2018. Online: https://theintercept.com/2018/06/25/interpol-voice-identification-database/
[253] Siehe z.B. Privacy International (2014): Privacy International uncovers widespread surveillance throughout Central Asia, exposes role of Israeli companies. Press release, 20.11.2014. Online: https://privacyinternational.org/press-release/1186/privacy-international-uncovers-widespread-surveillance-throughout-central-asia, Privacy International (2015): How Colombia built a shadow state, a new Privacy International investigation reveals. 31.8.2015. Online: https://privacyinternational.org/blog/1362/how-colombia-built-shadow-state-new-privacy-international-investigation-reveals, Amnesty International (2021): South Sudan: Rampant abusive surveillance by NSS instils climate of fear. 2.2.2021. Online: https://www.amnesty.org/en/latest/news/2021/02/south-sudan-abusive-surveillance-by-national-security-service-climate-of-fear/
[254] https://www.verint.com/engagement/our-offerings/solutions/experience-management/ [23.5.2021]
[255] https://appfoundry.genesys.com/filter/genesyscloud [23.5.2021]
[256] https://www.five9.com/partners/app-marketplace [23.5.2021]
[257] https://appconnect.talkdesk.com/ [23.5.2021]
[258] https://aws.amazon.com/de/connect/features/ [23.5.2021]

6.1.6 Vermessung und „Anregung" von Stimmung und Emotionen

Manche Anbieter von Systemen zur Gesprächsüberwachung gehen noch einen Schritt weiter als die zuvor bei Genesys beschriebene automatisierte Erkennung von positiv oder negativ besetzten Schlüsselwörter und Phrasen.

Die Technologie von **observe.ai**, die als App in Genesys[259] oder Five9[260] integriert werden kann, verspricht etwa, Stimmung und Emotionen in Gesprächsteilen mittels Analyse von Tonfall, Sprechgeschwindigkeit und Lautstärke einzuschätzen. Nach eigenen Angaben erfolgt dies mit Hilfe einer KI, die mit „10 Millionen Stunden" von Kundenservice-Gesprächen „trainiert" wurde.[261] Damit könne etwa analysiert und optimiert werden, wie „empathische" Formulierungen der Callcenter-Agents gegenüber „unglücklichen und frustrierten" KundInnen Kennzahlen über Kundenzufriedenheit oder Verkäufe verbessern.[262] Auch die Sprachanalyse-Firma **Voci** gibt an, negative und positive Emotionen[263] mittels KI zu erkennen – unter anderem auf Basis der Tonalität. Eine betroffene Agentin berichtet von kafkaesken Erfahrungen. Das System hätte ihr trotz guter Leistungskennzahlen und Rückmeldungen von Vorgesetzten über ihre „empathische" Gesprächsführung permanent „negative Emotionen" unterstellt (Dzieza 2020).

Cogito, ein aus dem US-Eliteforschungsinstitut MIT heraus gegründetes Startup[264], das sich seit Jahren öffentlichkeitswirksam selbst vermarket[265], behauptet gar, mehr als „200 Indikatoren über den emotionalen Zustand" zu „erkennen und zu vermessen"[266], zeigt diese den Callcenter-Agents in Echtzeit an und gibt ihnen Anweisungen, wie sie ihre Sprechweise und Tonalität verändern sollen.[267] Wie in Abbildung 5 (links) ersichtlich, werden in den Auswertungen bestimmte Merkmale von Gesprächsteilen mittels prozentueller Angaben dargestellt – es geht dabei etwa um langsame Antworten, zu lange Stille, einander ins Wort fallen, schnelles Sprechen, langandauernde Redeflüsse sowie um den Einsatz von „Empathie" und „Energie". Abbildung 5 (Mitte) zeigt, wie dem Agent eine potenziell negative Stimmung im Gespräch angezeigt wird. Der Beschäftigte solle darum laut Botschaft am Display die „Gelegenheit nützen" und mehr „Empathie" zu zeigen, um eine „Verbindung" mit dem Gegenüber aufbauen.

Cogito weist die Agents bei Bedarf auch darauf hin, in einer Situation etwas langsamer oder „energetischer" zu sprechen. Eine Beschäftigte in einem Callcenter einer Versicherung berichtet von absurden Erlebnissen. So habe Cogito lautstarke Freude über die Geburt eines Kindes seitens eines Anrufers als emotionalen Stress interpretiert und sie – und damit auch potenziell ihre Vorgesetzten – darüber alarmiert, dass nun mehr „Empathie" gezeigt werden müsse. Da sie aber schon gewusst habe, dass Cogito insbesondere die Formulierung „es tut mir leid" als „empathisch" einstufen würde, habe sie genau das gesagt. Sie würde während 10stündiger Schichten den ganzen Tag Anrufe von Menschen entgegennehmen, die von unheilbaren Krankheiten, Todesfällen, Fehlgeburten und anderen traumatischen Ereignissen berichten. Pro Anruf stünden 12 Minuten zur Verfügung, maximal eine Minute für das Ausfüllen der Versicherungsformulare und nur 30 Minuten pro Monat für Toilettenbesuche und kleine Pausen (Dzieza 2020). Anstatt diese katastrophalen Arbeitsbedingungen zu verbessern, wird also ein System wie Cogito eingesetzt. Cogito hält in einer Broschüre fest, es wäre für Callcenter-Agents nicht einfach, auf Knopfdruck eine

[259] https://appfoundry.genesys.com/filter/genesyscloud/listing/affe88f8-7759-4304-a683-9a33b8890aa9 [23.5.2021]
[260] https://www.five9.com/partners/app-marketplace/isv-partner/observeai [23.5.2021]
[261] https://www.observe.ai/blog/ai-sentiment-analysis-contact-centers-customer-experience [23.5.2021]
[262] https://www.observe.ai/blog/what-are-empathy-statements-and-how-do-you-coach-agents-on-them [23.5.2021]
[263] https://docs.vocitec.com/en/emotion,-sentiment,-and-gender.html [23.5.2021]
[264] https://cogitocorp.com/about/ [23.5.2021]
[265] https://cogitocorp.com/news/ [23.5.2021]
[266] https://cogitocorp.com/reduce-talk-time-and-increase-first-call-resolution/ [23.5.2021]
[267] https://cogitocorp.com/product/ [23.5.2021]

emotionale Verbindung herzustellen. Man könne aber dabei helfen, Empathie automatisiert zu vermessen und zu verbessern – und damit „empathy at scale“ zu implementieren.[268]

Callminer. Auch Callminer verspricht, automatisiert Informationen über Stimmungen, Emotionen und andere Verhaltensweisen aus Gesprächen zu extrahieren und berechnet daraus Kennzahlen über die Kundenzufriedenheit („Customer Satisfaction“, kurz CSAT).[269] Wie folgende Abbildung (rechts oben) zeigt, wird auch die „Qualität“ des Beschäftigten mit einer Zahl bewertet. In diesem Beispiel wird ein Callcenter-Agent mit der Zahl 87,5 bewertet und zudem festgehalten, dass die Person zu wenig Höflichkeit zeige und zu wenig Komplimente mache. Die Sprachverständlichkeit wird hingegen als gut bewertet:[270]

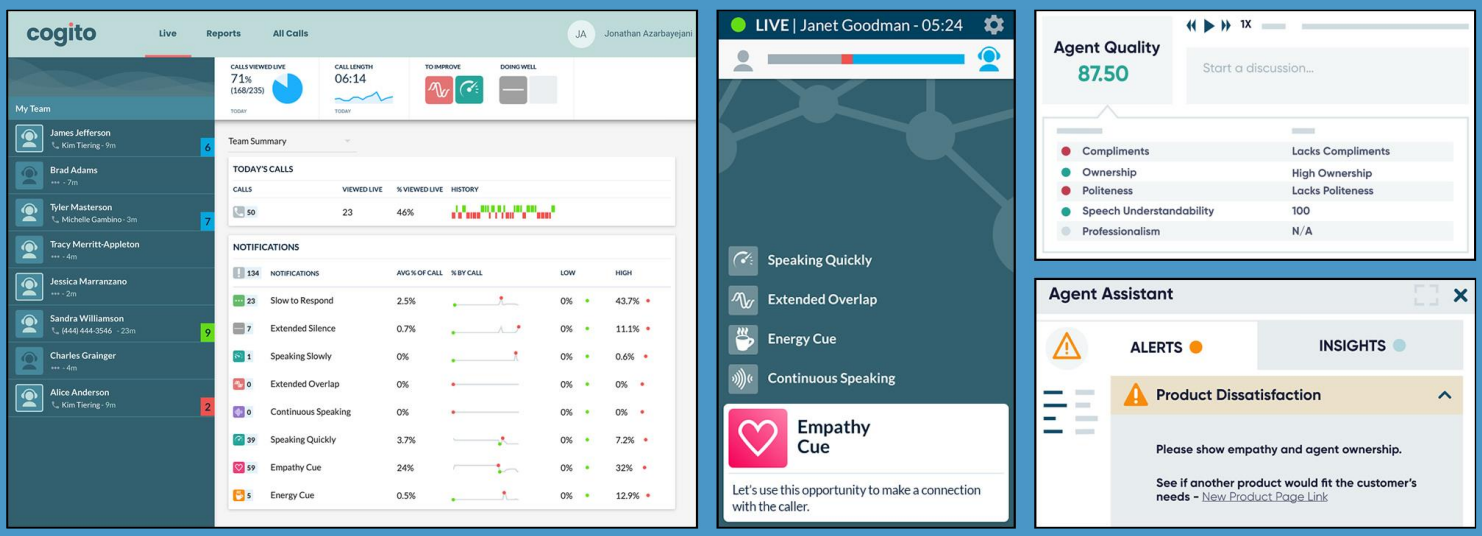


Abbildung 5: Analyse und Anregung von Emotionen bei Cogito (links, Mitte) und bei Callminer (rechts). Quelle: Hersteller

Auch Callminer alarmiert die Beschäftigten in Echtzeit über schlechte Stimmungen im Gespräch und gibt Anweisungen, wie das Problem zu lösen sei. Abbildung 5 (rechts unten) zeigt den digitalen „Assistenten“ von Callminer. In diesem Beispiel hat das System festgestellt, dass der Kunde „Unzufriedenheit mit dem Produkt“ zeigen würde. Der Agent solle darum nun mehr „Empathie“ zeigen. Laut einem Bericht sendet Callminer in einem typischen Gespräch drei bis fünf Benachrichtigungen pro Minute an die die Agents (vgl. Cannon 2019).

Wie Camilla Cannon (2019) in ihrem Artikel „Aufgezeichnet zum Zwecke der Qualitätssicherung. Die Datafizierung von Affekt in der Callcenter-Industrie“ ausführt, sind Validität, Aussagekraft und Zweckmäßigkeit derartiger automatisierter Bewertungen von Stimmungen und Emotionen mit Hilfe von KI höchst zweifelhaft. Behauptungen von „Objektivität“ wären leere Versprechungen. Vielleicht sei dies für die Unternehmen, die solche Systeme einsetzen, aber auch irrelevant – solange damit bestimmte geschäftliche Ziele erreicht werden könnten.

[268] https://cogitocorp.com/wp-content/uploads/2020/12/cogito_annual_report_2020_Update.pdf [23.5.2021]
[269] https://pages.callminer.com/rs/347-XFV-966/images/CX_CallMiner_AUS_web.pdf [23.5.2021]
[270] Alle Abbildungen (c) Cogito bzw. Callminer. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quellen: https://cogitocorp.com/product/ [23.5.2021], https://callminer.com/products/coach [23.5.2021], https://callminer.com/products/alert [23.5.2021]

Kiesche und Wilke (2012) vermuten, dass Methoden der Stimmungsanalyse und -beeinflussung in Deutschland gegen das Grundgesetz und die Menschenwürde der Beschäftigten verstoßen würden, da hier ein unantastbarer „Kernbereich der Individualität, Identität und Integrität“ betroffen wäre.

6.1.7 Situation in österreichischen und deutschen Callcentern

Auch wenn Callcenter schon seit vielen Jahren als Vorreiter bei der engmaschigen digitalen Kontrolle von Bildschirmarbeit gelten, ist unklar, wie weitgehend die in den vorangehenden Abschnitten beschriebenen Funktionen von Callcenter-Systemen in Österreich oder Deutschland eingesetzt werden.

Sandra Stern et al (2010) haben vor über einem Jahrzehnt eine Untersuchung über die Arbeit in **österreichischen Callcentern** auf Basis von Erfahrungsberichten veröffentlicht. Auch wenn die eingesetzte Software nicht im Vordergrund steht, so wird doch immer wieder die zentrale Rolle der akribischen zeitlichen Auswertung von Tätigkeiten und Kennzahlen im Arbeitsalltag beschrieben. In einem Callcenter habe die Vorgabe gelautet, pro Stunde hundert Anrufe zu tätigen, zehn Gespräche zu führen und einen Verkauf zu erzielen. Wer die Quote nicht geschafft habe, wäre zum Vorgesetzten geschickt worden. In Bezug auf eingehende Anrufe habe eine für alle sichtbare farbige Ampel in Form eines farbigen Balkens Druck ausgeübt. Bei „grün“ war alles in Ordnung. „Gelb“ habe angezeigt, dass die Anrufenden zu lange warten würden. Die Farbe „rot“ habe „Alarmstufe“ bedeutet – in diesem Fall hätten alle gewusst, dass dem Callcenter-Betreiber eine Vertragsstrafe droht (ebd., S. 19).

Auch einem anderen Callcenter sei oft auf die Notwendigkeit der Einhaltung des sogenannten „Service Level“ hingewiesen worden – also auf zwischen dem Betreiber und dem Auftraggeber vereinbarte Kennzahlen wie die Wartezeit für Anrufende oder die „Kundenzufriedenheit“. Dies habe die „permanente Überwachung“ ins Bewusstsein gerückt. Bei Bedarf hätten Vorgesetzte via E-Mail darauf hingewiesen, Gesprächsdauer und Bearbeitungszeit wegen des Service Levels kurz zu halten. Bei überzogenen Pausen wäre eine sofortige Erklärung an den Vorgesetzten via E-Mail erwartet worden, ansonsten wäre eine „Rüge“ die Folge gewesen. Neben sichtbaren wurden „unsichtbare Kontrollorgane“ vermutet, über die es „unterschiedliche Spekulationen“ gegeben habe (ebd., S. 14).

In einem weiteren Callcenter lautete die Vorgabe, pro Stunde im Schnitt 30 Gespräche samt Nachbearbeitung durchzuführen – damit hätten zwei Minuten pro Gespräch zur Verfügung gestanden. In dieser Zeit sei es unmöglich gewesen, auf die Anliegen der GesprächspartnerInnen angemessen einzugehen. Der Verfasser des Erfahrungsberichts habe nur einen Schnitt von vier Minuten pro Gespräch geschafft. Während der Arbeit habe er sich einloggen müssen und auf „Bereitschaft“ schalten, nach Beendigung eines Gesprächs auf „Nachbearbeitung“. Auf diese Weise wären die Wartezeiten auf Anrufe, die Dauer von Gesprächen und Nachbearbeitung sowie die Zeit zwischen Nachbearbeitung und erneuter „Bereitschaft“ detailliert erfasst worden. Für Toilettenbesuche, den kleinen Imbiss zwischendurch, um einen Kaffee zu holen oder für sonstige kleine Verschnaufpausen habe er auf „Pause“ schalten müssen. In einer Achtstunden-Schicht habe in Summe 45 Minuten Pausenzeit zur Verfügung gestanden. Da das Mittagessen im Nebengebäude kaum unter einer halben Stunde zu schaffen war, habe sich die Zeit für sonstige kleine Pausen auf 15 Minuten oder weniger reduziert. Diese Art der technischen Überwachung von Arbeitstätigkeiten sei eines der Hauptprobleme im Job gewesen – neben der Beschäftigung über eine Personalleasingfirma mit der Aussicht, jederzeit gekündigt werden zu können (ebd., S. 21f). Die Notwendigkeit, permanent den aktuellen Arbeitsstatus einzustellen – etwa „Toilette“, „Pause“ oder „Schulung“ – wird in den Berichten mehrfach beschrieben (ebd., S. 50).

Ein anderer Bericht beschreibt, dass die Funktionsweise der technischen Zeiterfassung zu unbezahlten Vor- und Nachbereitungszeiten geführt habe. Der Login musste vor Dienstbeginn erfolgen – das Öffnen von Programmen oder die Abfertigung von Anrufen bei Dienstende wäre nicht als bezahlte Arbeitszeit erfasst worden (ebd., S. 57). In einem weiteren Callcenter habe man bei Arbeitsbeginn eine unbezahlte Viertelstunde vor der vollen Stunde vor dem Rechner sitzen müssen. Habe man sich eine Minute zu spät eingeloggt, wäre die bezahlte Anwesenheit erst ab einer halben Stunde später gerechnet worden (ebd., S. 41f). Hier zeigt sich, dass digitale Kontrolle sehr exakt funktionieren kann, aber auch sehr ungenau oder gar grob fehlerhaft – je nach betrieblichen Interesse. Zusammenfassend halten Stern et al (2010) fest, dass Callcenter-Systeme in Österreich umfassende Daten über Tätigkeiten sekundengenau aufzeichnen – etwa die Dauer von Gesprächen, deren Annahme, Nachbearbeitungen oder kleine Pausen. Diese Daten würden von Vorgesetzten zur Leistungsbewertung herangezogen – etwa in Form durchschnittlicher Bearbeitungszeiten oder Verkaufszahlen (ebd., S. 101ff).

Laut Wolfgang Däubler (2017, S. 238ff) sind Beschäftigte in **deutschen Callcentern** einem „umfassenden Kontrollsystem“ unterworfen. In einem Betrieb wären an fünf von sieben Wochentagen sämtliche Gespräche aufgezeichnet worden. Für alle Beschäftigten würden wöchentlich jeweils fünf Gespräche durch einen Vorgesetzten angehört und bewertet. Davon hänge ab, ob in diesem Monat eine Prämie bezahlt werde oder ArbeitnehmerInnen dazu aufgefordert wurden, mehr auf die „Gesprächsqualität“ zu achten. Eine automatische Auswertung von Gesprächen samt Analyse von Schlüsselwörtern laufe laut Däubler auf eine „Totalüberwachung“ hinaus. Gegen eine Aufzeichnung und Auswertung der geführten Gespräche bestünden datenschutzrechtliche Bedenken. Eine Kontrolle „auf Verdacht“ oder zur „Aufrechterhaltung der Qualität“ sei in Deutschland rechtlich nicht möglich. Die meisten Probleme sieht Däubler bei Callcenter-Firmen, die das ausgelagerte „Massengeschäft“ vieler anderer Unternehmen abwickeln. Dies sei heute jedoch der „Regelfall“.

Für Österreich schreibt Thomas Riesenecker-Caba, dass Gespräche in „vielen Fällen“ aufgezeichnet würden (Haslinger et al 2020, S. 56). Das Vorhandensein eines Betriebsrats sei entscheidend für den Schutz der Belegschaft vor übermäßiger digitaler Kontrolle. Dies ist aber nicht immer der Fall (Stern et al 2010, S. 103). Kiesche und Wilke (2012) vermuten, dass diverse „Maßnahmen der Qualitätssicherung“ nach mehreren Datenschutzskandalen in Deutschland nicht mehr offen eingesetzt bzw. thematisiert werden würden und hoffen auf mehr Transparenz – als Voraussetzung für eine Eindämmung unverhältnismäßiger Methoden.

6.2 Leistungskontrolle, Betrugserkennung und Videoanalyse im Handel

Daten über Bezahlvorgänge an einer Kasse, über die an der Supermarktkasse mit dem Barcode-Lesegerät erfassten Produkte oder über Bestellungen und Zahlungen in einem Restaurant ermöglichen weitreichende Rückschlüsse über die Arbeitstätigkeiten von Beschäftigten in Handel, Dienstleistung und Gastronomie. Kassendaten bilden oft beinahe den gesamten Arbeitsalltag ab. Folgender Abschnitt zeigt Beispiele für Systeme, die diese Daten für verschiedene Zwecke nutzen. Die laufende Auswertung von Kassendaten zur Verhinderung von Betrug und Diebstahl durch ArbeitnehmerInnen ist seit langem üblich (vgl. Leopold 2008). Während diese Art der Profilierung im Ausnahmefall und unter strikten Rahmenbedingungen gerechtfertigt sein mag, ist die Auswertung für die Leistungskontrolle fragwürdig. Gängige Kassensoftware bietet jedoch vielfältige Funktionen für den Zweck der Leistungskontrolle – auch in Österreich und Deutschland. Derartige Auswertungen üben Druck auf die Belegschaft aus, selbst wenn sie nicht für die Sanktionierung eingesetzt werden, sondern „nur" für die Belohnung leistungsstarker ArbeitnehmerInnen oder zur Erkennung von „Schulungsbedarf". Abschnitt 6.2.3 beschreibt ein System, dass darüber hinaus mit automatisierter Videoanalyse die Bewegungen der Belegschaft auswertet.

6.2.1 Oracle Retail – Betrugserkennung und Leistungsbewertung in einem System

Der IT-Gigant Oracle bietet im Rahmen der Produktlinie „Oracle Retail"[271] vielfältige Funktionen zur Überwachung und Bewertung der Arbeitstätigkeiten von Verkaufspersonal im Einzelhandel. Das cloudbasierte **Betrugserkennungssystem** „XBRi Loss Prevention"[272] verspricht etwa, auf Basis von Kassendaten verdächtige Verhaltensweisen wie etwa ungewöhnliche Rückerstattungen, Rabatte oder Stornos zu erkennen.[273] Oracle bezeichnet die Software als global meistgenutztes System für Diebstahl- und Betrugsprävention sowie für Datenanalyse im Einzelhandel.[274] Folgende Abbildung zeigt, wie verdächtige Kassa-MitarbeiterInnen namentlich in einer Rangliste dargestellt werden – einige davon sind zusätzlich mit den Kategorisierungen „Hochrisiko" oder „Beobachtung" markiert:[275]

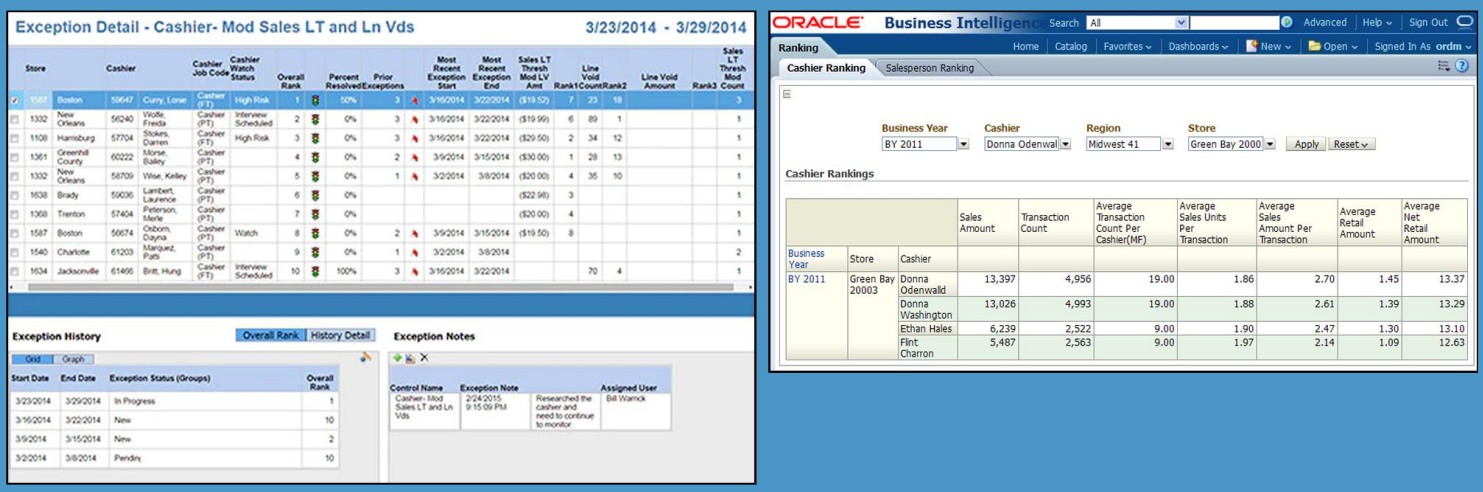


Abbildung 6: Betrugserkennung (links) und Leistungsauswertung (rechts) bei Oracle Retail. Quelle: Hersteller

[271] https://www.oracle.com/industries/retail/ [9.7.2021]
[272] https://www.oracle.com/a/ocom/docs/industries/retail/oracle-xbri-cloud-service-ds.pdf [9.7.2021]
[273] https://blogs.oracle.com/retail/post/four-new-applications-for-loss-prevention-data-and-exception-based-reporting [9.7.2021]
[274] https://www.oracle.com/a/ocom/docs/industries/retail/oracle-xbri-cloud-service-ds.pdf [9.7.2021]
[275] Abbildungen © Oracle. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quellen: https://www.oracle.com/industries/retail/products/xbri-cloud-service/, https://docs.oracle.com/cd/E16338_01/doc.112/e20361/sample_report2_rdm.htm [9.7.2021]

Neben der Aussonderung von als verdächtig oder riskant eingeschätzten Beschäftigten auf Basis einer kontinuierlichen Profilierung steht eine Funktion zur Verfügung, die Vorgesetzten für bestimmte Kassentransaktionen den zeitlich passenden Ausschnitt eines Überwachungsvideos zugänglich macht.[276] Zudem bietet das gleiche System neben der Diebstahl- und Betrugsprävention unter der Bezeichnung „XBRi Sales and Productivity" ein Zusatzmodul für die **Leistungsbewertung** von Verkaufspersonal.[277] Damit können Vorgesetzte beschäftigtenspezifische Auswertungen[278] über Leistungskennzahlen wie Verkaufsumsätze oder Verkäufe pro Stunde einsehen – und eine Rangliste der täglichen „Top 5 Performer".[279] Der Einsatz dieses Moduls ist optional. Dennoch ist es bemerkenswert, dass Oracle in ein System für die Diebstahl- und Betrugsprävention Funktionen zur Leistungsbewertung integriert.

Als Teil der Angebote für **Business Intelligence** im Handel stellt Oracle auch unabhängig davon umfassende Funktionen zur beschäftigtenspezifischen Leistungsbewertung zur Verfügung. Wie Abbildung 6 (rechts) zeigt, kann etwa eine Rangliste eingesehen werden, die für alle Kassa-MitarbeiterInnen anhand der bewältigten Zahlungsvorgänge darstellt, wie viele KundInnen sie in einem bestimmten Zeitraum abgefertigt haben. Dazu werden pro ArbeitnehmerIn und Zahlungsvorgang die durchschnittliche Anzahl von Produkten und deren durchschnittlicher Wert eingeblendet. Es steht eine Vielzahl an weiteren Leistungsauswertungen und Ranglisten zur Verfügung – sowohl für Kassa-MitarbeiterInnen als auch für anderes Verkaufspersonal.[280]

6.2.2 Systeme für Handel und Gastronomie in Österreich, Deutschland und Schweden

PosBill, ein deutsche Anbieter für Kassensysteme und -software in Gastronomie und Einzelhandel, der angibt, KundInnen in über 30 Ländern zu betreuen, darunter „mehrere tausend Kassensysteme" in Österreich[281], bewirbt sehr offenherzig Funktionen zur Leistungskontrolle. In einem Werbetext aus dem Jahr 2010 mit dem Titel „Kontrolle der Mitarbeiter an der Kasse" wird die Funktion „Kellneraktivitäten" beschrieben – laut Website ein „wun-

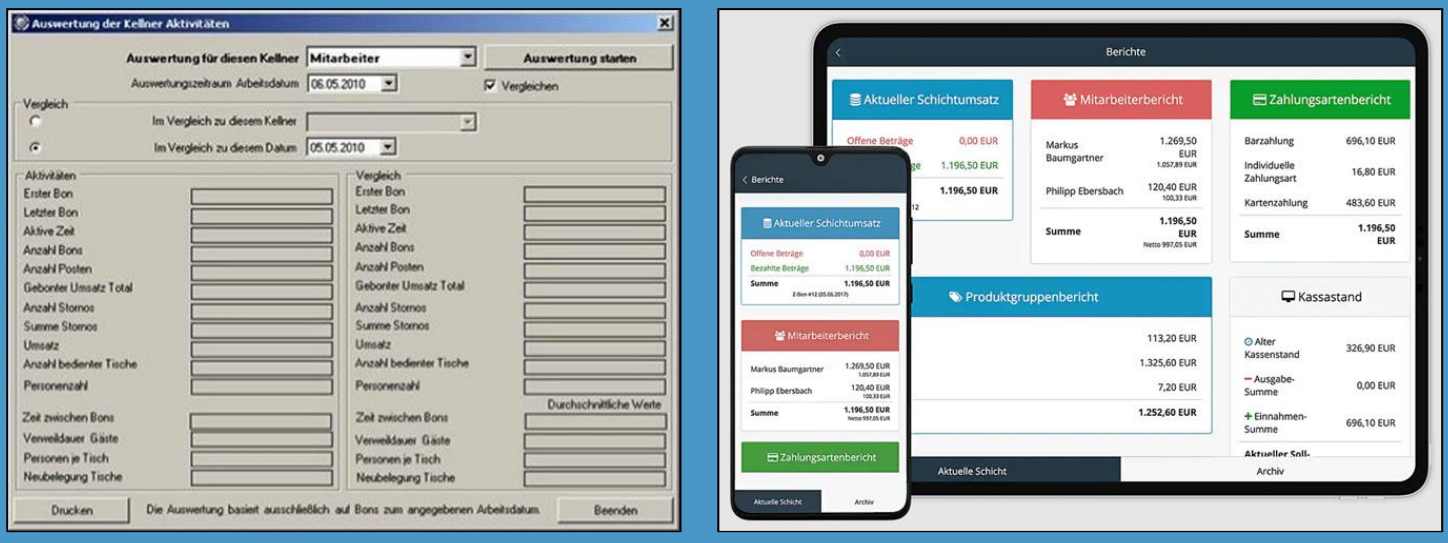


Abbildung 7: Auswertungen von Kassendaten bei PosBill (links) und ready2order (rechts). Quelle: Hersteller

[276] https://docs.oracle.com/cd/E71330_01/xbri/pdf/181/xbrics-181-ag.pdf, p. 41 [9.7.2021]
[277] https://www.oracle.com/industries/retail/products/xbri-cloud-service/ [9.7.2021]
[278] https://docs.oracle.com/cd/E71330_01/xbri/pdf/181/xbrics-181-ag.pdf, p. 58 [9.7.2021]
[279] https://docs.oracle.com/cd/E62106_01/xpos/pdf/180/html/managers_guide/mis_functions.htm [9.7.2021]
[280] https://docs.oracle.com/cd/E16338_01/doc.112/e20361/sample_report2_rdm.htm [9.7.2021]
[281] https://www.posbill.com/presseinformationen [11.6.2020]

derbares Tool um zum Beispiel einen einzelnen Mitarbeiter an der Kasse, aber an unterschiedlichen Tagen zu vergleichen. Oder zwei Mitarbeiter miteinander".[282] Wie der Ausschnitt aus der Bedienoberfläche in obiger Abbildung 7[283] (links) zeigt, können pro ArbeitnehmerIn nicht nur Umsatz, Bonierungsaktivitäten, Stornos, bediente Tische und Daten zur Zeit zwischen den Bons sowie zur Verweildauer von Gästen angezeigt, sondern auch Vergleiche zwischen ArbeitnehmerInnen sowie zu Durchschnittswerten der Beschäftigten durchgeführt werden.

Viele Datenverarbeitungszwecke. Das Unternehmen legt einerseits nahe, es solle damit verhindert werden, dass „Servicemitarbeiter in der Hektik" nicht „mit ihrer Kasse durcheinander kommen". Für die „Ein- und Ausgänge" müsse es doch „eine Kontrolle" geben. Hier wird ein Einsatz zur Verhinderung von Fehlern oder Betrug suggeriert. Schlussendlich wird aber festgehalten, es sei das „Ziel", zu sehen, wie „sich der einzelne Servicemitarbeiter im Vergleich verhält". Die Auswertung könne anschließend „als Hilfe zur Kellnerabrechnung benutzt" werden.[284]

Die Funktion war in einem – noch 2020 online abrufbaren – Benutzerhandbuch aus dem Jahr 2012 beschrieben.[285] Seither ist eine neuere Version der Benutzerhandbuchs online, in dem die Funktion nicht mehr angeführt ist.[286] Aber auch in der neueren Version werden Funktionen beschrieben, mit denen sich Umsatzstatistiken „nach Zeitraum und Kellner" anzeigen lassen. Damit wäre ersichtlich, welche KellnerIn „die meisten Getränke verkauft" habe.[287] Außerdem können vollständige Listen aller Bons, bonierter Einzelposten und Stornos nach Zeitraum und beschäftigter Person eingesehen werden.[288] Dazu können für einzelne KellnerInnen sogenannte „ABC-Analysen" der verkauften Artikel erstellt werden.[289] Neben der Kassensoftware für die Gastronomie wird auch eine allgemeine Version für den Einsatz in Einzelhandel und Dienstleistung angeboten – vom **Textil- und Schuhhandel bis zum Friseurladen**.[290] Diese bietet laut Benutzerhandbuch ähnliche Funktionen inklusive Umsatzstatistiken[291], ABC-Analysen[292] sowie Listen aller Bons, bonierter Einzelposten und Stornos[293] nach Zeitraum und beschäftigter Person.

Auch das **Wiener Unternehmen ready2order**, das eine cloudbasiertes Kassensoftware für Handel, Dienstleistung und Gastronomie anbietet[294], verspricht neben der Verwaltung von Personal und Dienstplänen eine „Analyse der Leistung" von ArbeitnehmerInnen.[295] Wie Abbildung 7 (rechts) zeigt, wird für jede einzelne MitarbeiterIn der Umsatz prominent angezeigt, was einen unmittelbaren Vergleich ermöglicht. Diese Einblicke in die „Umsatzdaten [der] Mitarbeiter" sollen laut ready2go dabei helfen, „zu sehen, wer am besten abschneidet und wer weitere Trainings braucht". Mit der Formulierung „verfolgen Sie die Leistung Ihrer Mitarbeiter" wird die Software explizit als Mittel

[282] https://blog.posbill.com/kontrolle-der-mitarbeiter-in-der-kasse-kellneraktivitaten/ [11.6.2020]
[283] Abbildung links © PosBill, Abbildung rechts © ready2order. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quellen: https://blog.posbill.com/kontrolle-der-mitarbeiter-in-der-kasse-kellneraktivitaten/ [11.6.2020], https://ready2order.com/de/funktionen/mitarbeitermanagement/ [21.2.2021]
[284] https://blog.posbill.com/kontrolle-der-mitarbeiter-in-der-kasse-kellneraktivitaten/ [11.6.2020]
[285] s. 72: https://www.posbill.com/uploads/media/PosBill14_Handbuch_Gastro.pdf [11.6.2020]
[286] https://www.posbill.com/uploads/downloads/PosBill_DE_V18_Gastro.pdf [21.2.2021]
[287] Ebd., s. 95
[288] Ebd., s. 307ff
[289] Ebd., s. 301ff
[290] https://www.posbill.com/PosBill [21.2.2021]
[291] s. 82 https://www.posbill.com/uploads/downloads/PosBill_DE_V18_Handel.pdf [21.2.2021]
[292] Ebd., s. 266ff
[293] Ebd., s. 272ff
[294] https://ready2order.com/de/ [21.2.2021]
[295] https://ready2order.com/de/funktionen/mitarbeitermanagement/ [21.2.2021]

der Leistungskontrolle beworben. Gleichzeitig soll „mithilfe umfassender Sicherheitskontrollen“ Diebstahl durch ArbeitnehmerInnen verhindert werden.[296]

In einem Überblick über die in der Benutzeroberfläche verfügbaren Reports wird unter der Überschrift „Mitarbeiter-Performance“ beschrieben, dass Betriebe einsehen könnten, „wie viel Umsatz jeder Mitarbeiter macht, wie viele Bons erstellt wurden und wer in Folge die meisten Rechnungen erstellt hat“, um die „Leistung [der] Angestellten“ im Blick zu behalten – natürlich nur, um sie „weiter auszubilden und sie zu motivieren“.[297]

Zettle, ein schwedischer Anbieter von Bezahlsystemen für Handel und Dienstleistung, der 2018 für 2,2 Milliarden Dollar von PayPal übernommen wurde[298], bietet ebenfalls weitreichende Funktionen, um „Verkäufe und Mitarbeiterleistung […] mit täglichen Umsatzberichten“ zu „analysieren“ und die „Produktivität von Mitarbeitern in täglichen Berichten“ zu „prüfen“.[299] Auch dieses System zeigt Umsatz und Anzahl der Verkäufe durch einzelne Beschäftigte an – um die „Verkaufsleistung“ des Personals „schnell analysieren zu können“. Außerdem können Berichte über die Art und Anzahl der verkauften Produkte, Erstattungen und Rabatte für einzelne ArbeitnehmerInnen erstellt werden.[300]

6.2.3 RetailNext – Datenintegration, Profiling und automatisierte Videoanalyse

Das US-Unternehmen RetailNext konzentriert sich auf „In-Store Analytics“, also auf die Analyse von Verhaltensweisen und Bewegungen von KundInnen und Beschäftigten in den Räumlichkeiten von Geschäften und Einkaufszentren[301], um den laufenden Betrieb und den Verkauf zu optimieren, Auslastung und Personalbedarf vorherzusagen, Diebstahl und Betrug zu verhindern und die Leistung der Beschäftigten zu vermessen.

Profiling von VerbraucherInnen. Wie Abbildung 8 (rechts) zeigt, werden umfassende Datenquellen zusammengeführt. Neben der Auswertung von Daten aus Videokameras und Kassensystemen werden vor allem WLAN- und Bluetooth-Kennungen von mobilen Geräten wie Smartphones einbezogen, um die Bewegungen von Personen in Geschäften zu analysieren.[302] Dazu werden vernetzte Geräte angeboten, die Kameras und WLAN/Bluetooth-Sensoren eingebaut haben.[303] Auch Videodaten werden zur automatisierten Analyse von Bewegungsmustern herangezogen.[304] Außerdem werden mit Videodaten Alter und Geschlecht der einkaufenden Personen eingeschätzt.[305] Laut eigenen Angaben ist die Technologie von RetailNext in 85 Ländern im Einsatz[306] und erfasst dabei mit „zehntausenden“ Sensoren in Geschäften jährlich Daten über eine Milliarde Einkaufende. RetailNext hat eine Niederlassung in Madrid, stellt die Website auch in deutscher Sprache zur Verfügung[307] und suchte im Juli 2021 einen Betreuer für Firmenkunden in Berlin.[308]

---

[296] Ebd.
[297] https://ready2order.com/at/post/kennzahlen-fuer-kmus-warum-du-auch-als-kleines-unternehmen-daten-auswerten-sollte/ [21.2.2021]
[298] Irrera, Anna und Olof Swahnberg (2018): PayPal expands retail payments with $2.2 billion Zettle buy. Reuters, 17.5.2018. Online: https://www.reuters.com/article/us-izettle-m-a-paypal-hldg/paypal-expands-retail-payments-with-2-2-billion-zettle-buy-idUKKCN1II2MT
[299] https://www.zettle.com/de/kassensystem/funktionen [21.2.2021]
[300] https://www.zettle.com/de/help/articles/1084803-informationen-zu-berichten [21.2.2021]
[301] https://retailnext.net/en/about-us/ [10.2.2021]
[302] https://retailnext.net/en/how-it-works/ [10.2.2021]
[303] https://www.qualcomm.com/media/documents/files/retailnext-aurora-sensor-case-study.pdf [10.2.2021]
[304] https://retailnext.net/en/products/shopper-activity-maps/ [10.2.2021]
[305] https://retailnext.atlassian.net/wiki/spaces/PUBLICDOCS/pages/1851195558/RetailNext+Privacy+Resources+Product+Capabilities [10.2.2021]
[306] https://retailnext.net/en/about-us/ [10.2.2021]
[307] https://retailnext.net/de/contact-us-de/ [10.2.2021]
[308] https://retailnext.net/open-position/5293799002 [23.7.2021]

Beschäftigtendaten. Das System versucht einerseits, Einkaufende von ArbeitnehmerInnen zu unterscheiden, um letztere von bestimmten Analysen auszunehmen.[309] Dazu müssen die Beschäftigten aber erst identifiziert werden. Laut einem Patent erfolgt die Identifikation von ArbeitnehmerInnen auf Basis von Video- sowie WLAN/Bluetooth/RFID-Daten.[310] Andererseits werden auch über Beschäftigte weitreichende Auswertungen durchgeführt.

Riskante ArbeitnehmerInnen. Neben Analysen für Verkauf und Marketing bietet RetailNext ein System für „Loss Prevention", das Betrug und Diebstahl durch MitarbeiterInnen an der Kassa erkennen und verhindern soll. Wie der Ausschnitt aus der Benutzeroberfläche in folgender Abbildung (links) zeigt, werden dabei sowohl Kassendaten als auch Videobilder ausgewertet. Neben einer Liste verdächtiger Kassentransaktionen wird eine nach Risiko gereihte Liste von namentlich zugeordneten „Hochrisiko"-KassamitarbeiterInnen eingeblendet und damit eine Art von laufendem Profiling von ArbeitnehmerInnen durchgeführt:[311]

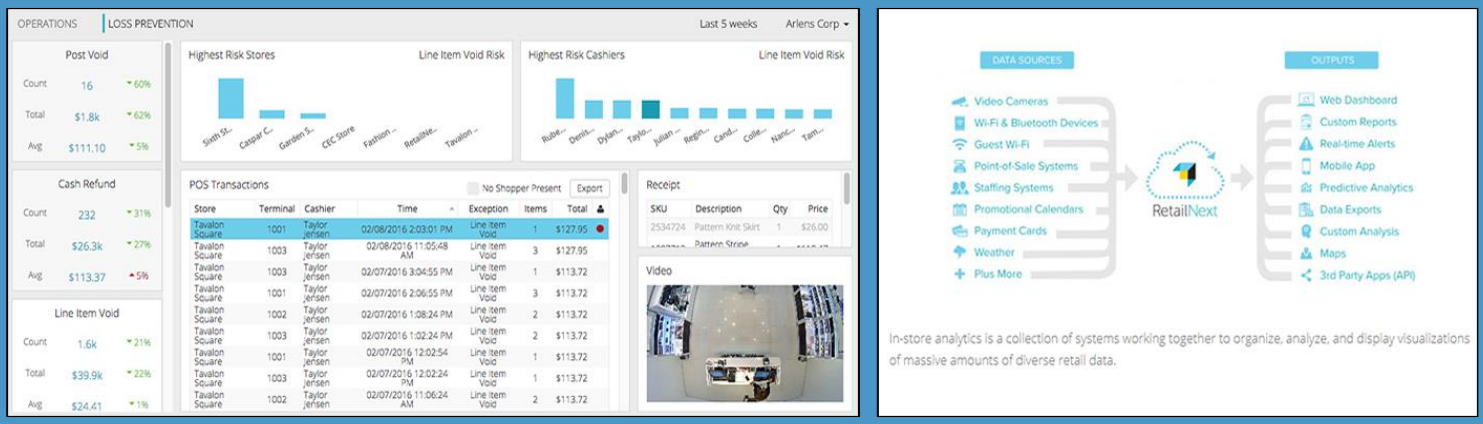


Abbildung 8: Betrugserkennung (links) und Datenintegration (rechts) bei RetailNext. Quelle: Hersteller

In einer anderen Ansicht der Benutzeroberfläche sind numerische Risiko-Scores für einzelne Beschäftigte einsehbar, dazu Unter-Scores für bestimmte als verdächtig eingestufte Transaktionen wie „Storno" oder „Erstattung von Bargeld". Auch ganze Filialen werden nach Betrugsrisiko sortiert dargestellt.[312] Zu jeder Einzeltransaktion ist ein archiviertes Kameravideo des Kassenbereichs rund um den Zeitpunkt der Transaktion verfügbar. Die Videokamerabilder können aber auch in Echtzeit eingesehen werden. Stellt das System verdächtige Verhaltensweisen fest, kann es „Alarm" schlagen.[313] Alle Daten können auch durchsucht werden.[314]

[309] https://retailnext.net/en/blog/when-it-comes-to-shopper-traffic-accuracy-is-everything/ [10.2.2021]
[310] https://patents.google.com/patent/US9569786B2/en [10.2.2021]
[311] Abbildungen © RetailNext. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quellen: https://retailnext.net/en/blog/lp-made-easy-ier-pos-exception-reporting-with-integrated-video/, https://retailnext.net/en/how-it-works/ [10.2.2021]
[312] https://retailnext.net/en/blog/lp-made-easy-ier-pos-exception-reporting-with-integrated-video/ [10.2.2021]
[313] http://retailnext.net/wp-content/uploads/2014/01/RetailNext_Data-Sheet_Real-Time-In-Store-Analytics.pdf [10.2.2021]
[314] https://retailnext.net/en/products/pos-exception-reporting/ [10.2.2021]

Analyse von Beschäftigtendaten. Wie folgende Tabelle zeigt, bietet das System auch abseits der Diebstahl- und Betrugsprävention eine Vielfalt an Auswertungsmöglichkeiten auf Basis unterschiedlicher Datenquellen:[315]

Art der Auswertung	Datenquellen
Anzahl der Beschäftigten, die an einem Tag das Geschäft betreten haben	Video, Bluetooth-Tags
Anzahl der Beschäftigten, die an einem Tag das Geschäft verlassen haben	Video, Bluetooth-Tags
Anzahl der Beschäftigten, die an einem Tag in ausgewählten Bereichen des Geschäftslokals stehen	Video, Bluetooth-Tags
Durchschnittliche Zeit, die Beschäftigte an einem Tag in ausgewählten Bereichen des Geschäftslokals stehen	Video, Bluetooth-Tags
Anteil der Beschäftigten, die in ausgewählte Bereiche gehen und dort auch stehenbleiben („Engagement-Rate“)	Video, Bewegungsdaten
Anzahl der Interaktionen zwischen Beschäftigten und KundInnen in ausgewählten Bereichen im Geschäftslokal	Video, Bewegungsdaten
Anteil der KundInnen in ausgewählten Bereichen im Geschäftslokal, mit denen Beschäftigte interagiert haben	Video, Bewegungsdaten
Anwesendes Personal in einem Zeitraum	Personaldaten
KundInnen pro Beschäftigtenstunde	Video, Personaldaten
Nettoverkäufe pro Beschäftigtenstunde („Produktivität“), auch für individuelle ArbeitnehmerInnen	Kassendaten, Personaldaten

Tabelle 1: Auswahl von Auswertungen über Beschäftigte bei RetailNext. Quelle: Hersteller

Dabei werden Daten aus Personalverwaltung und Kassasoftware mit Daten über Bewegungen sowie aus der Videoüberwachung verknüpft und zur Berechnung von unterschiedlichen Kennzahlen über Verhalten und Leistung der Beschäftigten genutzt. Darüber hinaus bietet RetailNext Funktionen zur „Personaloptimierung“ an, die „detaillierte individuelle Statistiken zur Leistung von Beschäftigten“ versprechen.[316] Generell ist eine Vielfalt an Daten zu Verkäufen und Zahlungen auf individueller Ebene einsehbar.[317]

Das Beispiel RetailNext zeigt, wie personenbezogene Daten über ArbeitnehmerInnen im Einzelhandel zusammengeführt und für viele unterschiedliche Zwecke von der laufenden Risikobewertung bis zur Leistungsbewertung eingesetzt werden – unter Einbeziehung von Kassendaten und Informationen über Bewegungen von Beschäftigten in Innenräumen, die unter anderem mit automatisierter Videoanalyse erfasst werden. Gleichzeitig werden die KundInnen überwacht. Es bleibt jedoch unklar, ob diese Angebote auch im deutschen Sprachraum eingesetzt werden.

[315] https://retailnext.atlassian.net/wiki/spaces/PUBLICDOCS/pages/144867353/Metrics+Glossary#Staff [10.2.2021]
[316] https://retailnext.net/en/products/staffing-optimization/ [10.2.2021]
[317] https://retailnext.atlassian.net/wiki/spaces/PUBLICDOCS/pages/144867353/Metrics+Glossary [10.2.2021]

6.3 Datenintensive Prozessanalyse und -automatisierung mit „Celonis“

Celonis, ein 2011 gegründetes und zum Teil durch kalifornische Risikokapitalgesellschaften finanziertes Münchner Unternehmen mit rund 1000 MitarbeiterInnen, betreibt eine cloudbasierte Plattform, mit der betriebliche Aktivitäten auf Basis von Ereignisdaten aus bestehenden Systemen analysiert, optimiert und automatisiert werden sollen.[318] Die akribische Durchleuchtung betrieblicher Abläufe und Arbeitsschritte in Bereichen wie Ein- und Verkauf, Kundenservice, Materialwirtschaft oder Produktion wird unter dem Begriff „Process Mining“ vermarket.[319] Laut Celonis wurde oder wird deren Plattform von Firmen wie Deutscher Telekom[320], Siemens, Lufthansa, Vodafone, Edeka und Airbus eingesetzt – in Österreich von A1 Telekom Austria und Wien Energie.[321] Die Uniqa-Versicherung setzt Celonis im Bereich Schadenabwicklung ein.[322] Standardisierte und digital überwachte betriebliche Abläufe können besser ausgelagert werden. Folgerichtig bewirbt Celonis insbesondere den Einsatz im Rahmen des sogenannten „Business Process Outsourcing“, dem Auslagern ganzer Tätigkeitsbereiche eines Unternehmens an Dritte.[323]

6.3.1 Analyse und Optimierung von betrieblichen Abläufen und Arbeitsschritten

Zusammenführung von Daten. Grundlage für alle anderen Funktionen ist die Einspeisung von detaillierten Ereignisprotokollen[324] aus bestehenden Anwendungen – etwa aus den ERP-, HRM- oder CRM-Systemen von SAP, Oracle, Microsoft und Salesforce. Sowohl Cloud-Dienste als auch Systeme, die vor Ort betrieben werden, können mit 80 vorgefertigten Modulen in Echtzeit angebunden werden. Celonis extrahiert daraus Daten über Aktivitäten mit Zeitstempeln und transformiert sie anwendungsspezifisch in Informationen über betriebliche Prozesse – also über Abläufe, Arbeitsschritte und Tätigkeiten.[325]

Standardisierung, Optimierung und Automatisierung. In weiterer Folge werden die identifizierten Prozesse samt aller vorkommenden Varianten visuell dargestellt und in Bezug zu geschäftlichen Kennzahlen wie Zeit, Kosten oder Kundenzufriedenheit gesetzt. Celonis verspricht, Unternehmen dabei zu helfen, unerwünschte, ineffiziente oder kostenintensive Abläufe und Arbeitsschritte zu entdecken und zu eliminieren. Auch der Grad der Automatisierung und die Automatisierbarkeit werden für jeden Prozess bewertet. Prozesse sollen hinsichtlich strategischer Ziele standardisiert, rationalisiert, optimiert und automatisiert werden.

Im Anschluss können Abläufe und Arbeitsschritte auf Basis fortgesetzter Einspeisung von Echtzeit-Daten weiter beobachtet und vermessen werden, resultierend in laufenden Handlungsempfehlungen für Führungskräfte. Darüber hinaus kann die sogenannte „Action Engine“ von Celonis unmittelbar in den Arbeitsalltag der Beschäftigten eingreifen und als „intelligenter Assistent“ Anweisungen für zu verrichtende Tätigkeiten zuweisen und priorisieren.[326]

---

[318] https://www.celonis.com/de/careers, https://www.celonis.com/de/company/ [28.2.2021]
[319] https://www.celonis.com/process-mining/what-is-process-mining [28.2.2021]
[320] Kroker, Michael (2021): Wird Celonis das zweite SAP, nach dem Deutschland so lange suchte? Wirtschaftswoche, 2.6.2021. Online: https://www.wiwo.de/erfolg/gruender/software-start-up-wird-celonis-das-zweite-sap-nach-dem-deutschland-so-lange-suchte/27209228.html
[321] https://www.celonis.com/de/customers/ [28.2.2021]
[322] https://www.celonis.com/de/blog/well-insured-uniqa-harmonizes-their-claims-handling-with-celonis/ [28.2.2021]
[323] https://www.celonis.com/solutions/bpo/ [28.1.2021]
[324] Siehe auch Abschnitt 5.8.1
[325] https://www.celonis.com/intelligent-business-cloud/event-collection, https://www.celonis.com/blog/self-driving-enterprise-start-with-the-ems [28.2.2021]
[326] https://assets.ctfassets.net/zmrtlfup12q3/4CUYlOAz0xC07vcbPtznOK/e4a7872feac4d4c713d7ce35cb3604a0/Ultimate_Guide_to_Process_Mining.pdf [28.2.2021]

Seit kurzem bezeichnet Celonis die Plattform als „Execution Management System“ (EMS) und legt den Fokus damit noch mehr auf die Veränderung – und nicht nur die Analyse – von betrieblichen Prozessen.[327]

Beispiel Schadenabwicklung bei einer Versicherung. In einer von Celonis bereitgestellten Produktdemonstration in Form eines Videos wird der Einsatz der Plattform bei einer Fahrzeugversicherung beschrieben.[328] Dabei werden Daten über die Abläufe bei etwa 140.000 Schadenmeldungen mit einem Auszahlungsbetrag von rund 300 Millionen Dollar und einer durchschnittlichen Bearbeitungszeit von 32 Tagen analysiert. Folgende Abbildung (links) zeigt die Visualisierung einiger Arbeitsschritte, von der Überprüfung des Versicherungsvertrags über die Genehmigung der Reparatur bis zum Einscannen und Buchen der Rechnung der Autowerkstatt:[329]

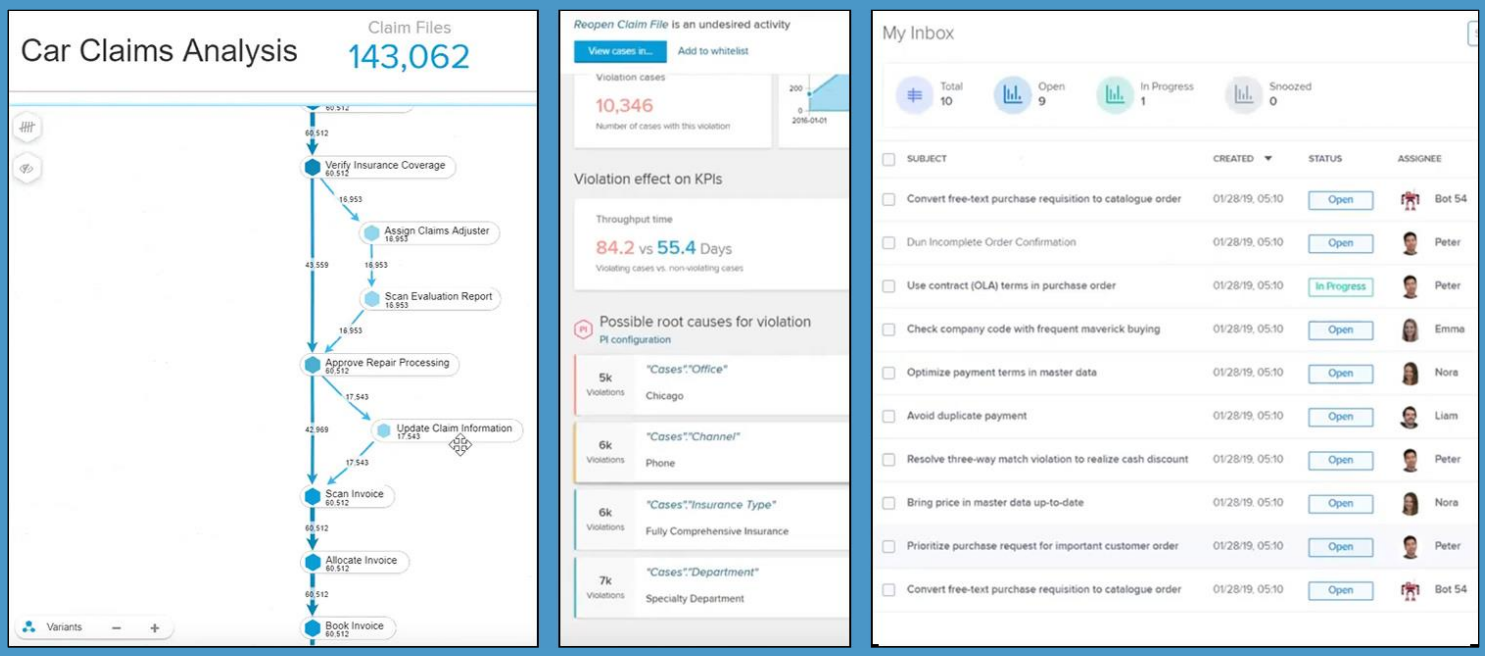


Abbildung 9: Prozessanalyse, unerwünschte Aktivitäten und Zuweisung von Aufgaben bei Celonis. Quelle: Hersteller

Für jeden Übergang von einem Arbeitsschritt zum anderen stehen detaillierte Zahlen zur Verfügung, etwa zu Dauer und Anzahl der betroffenen Fälle. Ein Arbeitsschritt kann sich dabei sowohl auf Tätigkeiten von ArbeitnehmerInnen als auch auf automatisierte Vorgänge beziehen. Insgesamt werden in diesem Beispiel 64 Varianten des Ablaufs von der Schadensmeldung bis zur Erledigung identifiziert. Diese können nach Zeiträumen, Auszahlungsbeträgen, Unternehmensstandorten und anderen Kriterien gefiltert werden – etwa auch danach, ob die Schadensmeldung via Telefon, E-Mail oder Brief eingegangen ist. Unternehmensstandorte können miteinander verglichen werden, etwa in Hinblick auf die Automatisierungsrate oder den Grad der „Prozess-Konformität“, die angibt, wie viele Fälle über als effizient eingeschätzte Abläufe abgewickelt werden und wie viele davon abweichen.[330]

[327] https://www.celonis.com/ems [28.2.2021]
[328] https://www.youtube.com/watch?v=p0tKTzesc4g [28.2.2021]
[329] Alle Abbildungen Standbilder aus Video (c) Celonis. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle Video bei Minute 3:15, 10:35 und 13:18: https://www.youtube.com/watch?v=p0tKTzesc4g [28.2.2021]
[330] https://www.youtube.com/watch?v=p0tKTzesc4g [28.2.2021]

Unerwünschte Aktivitäten. Sogenannte „Verletzungen" des optimalen Ablaufs sowie „unerwünschte Aktivitäten" können näher untersucht werden. Wie in Abbildung 9 (Mitte) ersichtlich, wurde in der vorliegenden Produktdemonstration eine erneute Bearbeitung eines Schadensfalls als „unerwünschte Aktivität" identifiziert. Zur Untersuchung der möglichen Ursachen für die unerwünschte Aktivität wird dargestellt, in wie vielen Fällen sie aufgetreten ist – aufgeschlüsselt nach Unternehmensstandort, Abteilung und anderen Kriterien. An dieser Stelle warnt Celonis, dass die Auswertungen personenbezogene Anteile enthalten könnten.[331] Auch wenn die meisten Auswertungen aggregiert erfolgen, verarbeitet das System in jedem Fall umfassende personenbezogene Daten über Beschäftigte.

6.3.2 Automatisierte Zuweisung und Priorisierung von Arbeitsaufgaben

Die Verarbeitung personenbezogener Daten durch das System wirkt sehr unmittelbar auf ArbeitnehmerInnen zurück, wenn die „Action Engine" von Celonis in einem weiteren Schritt ähnlich einem Ticketsystem konkrete Arbeitsaufgaben zuweist, priorisiert oder gar mit automatisierten Arbeitsanweisungen durch „Bots" ergänzt.

Celonis spricht von einem „KI-basierte[n] Prozessassistent, der ständig Daten analysiert, Verbesserungspotenziale in Echtzeit erkennt und dann Signale an alle Beteiligten sendet, um konkrete Maßnahmen vorzuschlagen, welche erforderlich sind, um einen Prozess wieder auf Kurs zu bringen". Die Software „lernt ständig dazu, beobachtet das Ergebnis jeder empfohlenen Handlung und aktualisiert zukünftige Empfehlungen".[332]

Die Grenze zwischen Handlungsempfehlung und Arbeitsanweisung ist hier wohl fließend. Diese Funktionen können als eine Form des **algorithmischen Managements** gefasst werden.

Wie in Abbildung 9 (rechts) ersichtlich, können Führungskräfte außerdem in Echtzeit die den Beschäftigten zugewiesenen Arbeitsaufgaben und Statusinformationen wie etwa „in Bearbeitung" einsehen.

6.3.3 „Task Mining" mit Auswertung von Bildschirminhalten, Maus- und Tastaturnutzung

Die zuvor beschriebenen Funktionen beschränken sich auf die Analyse von Ereignisdaten über betriebliche Abläufe – also zum Beispiel die Zeitpunkte, zu denen eine Rechnung erstellt, bestätigt, bezahlt oder abgelehnt wurde. Ergänzend kann ein von Celonis als „Task Mining" bezeichnetes System dazu genutzt werden, beinahe jegliche Aktivitäten auf den Rechnern von Beschäftigten aufzuzeichnen und auszuwerten. Dabei wird eine Spionagesoftware auf den Rechnern installiert, die bei der Nutzung von E-Mail, Excel, Websites oder anderen Anwendungen laufend Nutzerinteraktionen samt Zeitstempel erfasst – vom Öffnen oder Wechseln der genutzten Anwendung über Mausklicks und Scrollvorgänge bis zu Eingaben über die Tastatur. Dabei können Bildschirminhalte und sogar der Inhalt der Zwischenablage gespeichert werden.[333]

Verknüpfung von Daten über Nutzerinteraktionen, Arbeitstätigkeiten und betriebliche Abläufe. Im Anschluss versucht das System, einzelne Interaktionen in zusammenhängende Arbeitstätigkeiten zu gruppieren, etwa das „Ausfüllen der Bestellung, Überprüfen der Bestellmenge", das „Abgleichen von Aufträgen mit Rechnungen"

---

[331] Ebd.

[332] https://www.celonis.com/de/intelligent-business-cloud/action-engine [28.2.2021]

[333] https://www.celonis.com/de/process-mining/what-is-task-mining, https://www.celonis.com/de/intelligent-business-cloud/desktop-data-collection, https://assets.ctfassets.net/zmrtlfup12q3/1IXZl8eoB4QPhUd2arGZaG/9b342f2fdd86a8149f7f17c8afd4ecc4/IDC.Celonis_Task_Mining.lcUS45581919.pdf, https://assets.ctfassets.net/zmrtlfup12q3/4FvTct1rFVTE3TOgSKkplY/0a9d18ae5afdad71cb295d5e686ee2bc/20210121-Task_Mining_Data_Privacy_by_Design_-_Whitepaper.pdf [28.2.2021]

oder eine „zehnminütige[n] Recherche auf LinkedIn“. Durch den Abgleich von Benutzernamen, Bestell- und Kundennummern, Beschriftungen von Formularfeldern und anderen Schlüsselwörtern werde die Nutzerinteraktionsdaten mit Daten über betriebliche Abläufe verknüpft. Auch aus den gespeicherten Bildschirminhalten werden dazu mittels Texterkennung Wörter, Zahlen und Schlüsselwörter extrahiert.[334]

6.3.4 Vermessung und Steigerung von Produktivität, Leistung und Automatisierung

Mit dem von Celonis als „Task Mining“ bezeichneten System könnten Unternehmen „datengestützt verstehen, wie Mitarbeiter ihre Aufgaben erfüllen“, „Ineffizienzen in manuellen Arbeitsmustern […] aufdecken“ und nicht zuletzt „die Produktivität Ihrer Mitarbeiter messen und optimieren“. Es könnten „Kennzahlen über ArbeitnehmerInnen und Top-Performer bei bestimmten Aufgaben“ etwa in Bezug auf die benötigte Zeit oder deren „Produktivität“ gewonnen werden. Es ließen sich „Verhaltensweisen, welche zu positiven Ergebnissen führen, ermutigen und diejenigen vermeiden, welche zu negativen Ergebnissen führen“.

Unternehmen könnten einerseits Aufgaben „with the potential for replacing workers with automation“ finden, also mit dem Potenzial, ArbeitnehmerInnen durch Automatisierung zu ersetzen. Andererseits könnten auch „Aufgaben mit hoher Produktivität“ identifiziert werden, die „nicht automatisiert werden können“, um in diese zu investieren. Celonis hebt hervor, dass Systeme, die sich auf Daten zur PC-Nutzung beschränken und diese nicht mit Daten über betriebliche Abläufe verknüpfen, Beschäftigte als ineffizient einschätzen könnten, die zwar im Durchschnitt mehr Zeit mit bestimmten Aufgaben verbringen, damit aber bessere geschäftliche Resultate erzielen.[335]

Folgende Abbildung (links) zeigt, wie im System von Celonis Nutzerinteraktionen erfasst und eingesehen werden können. In diesem Fall hat eine Nutzerin innerhalb von wenigen Sekunden fünf Aktivitäten durchgeführt, von der Nutzung einer Anwendung von Salesforce im Browser und dem mehrfachen Wechseln des Browserfensters bis zu einer Tastatureingabe, die offenbar zu einer Änderung des Inhalts der Zwischenablage geführt hat:[336]

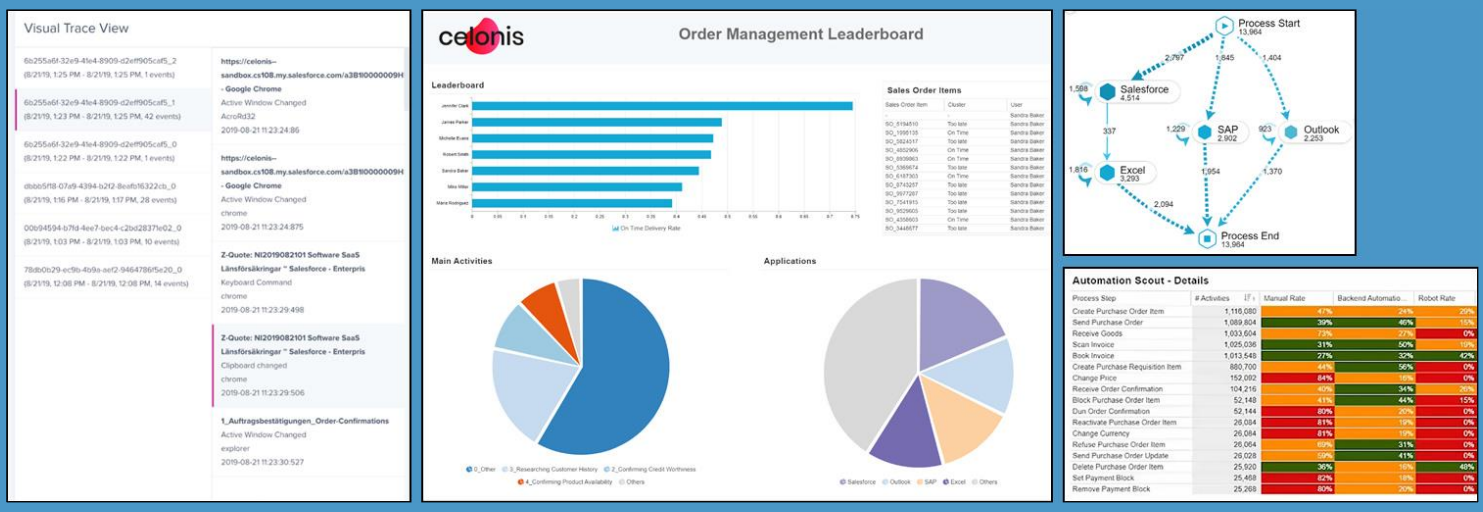


Abbildung 10: Auswertung von PC-Nutzung und Arbeitsabläufen sowie Leistungsvergleich bei Celonis. Quelle: Hersteller

[334] Ebd.
[335] Ebd.
[336] Alle Abbildungen (c) Celonis. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle Abbildungen links, Mitte, und recht oben (Ausschnitte Benutzeroberfläche): https://www.celonis.com/de/intelligent-business-cloud/desktop-data-collection [28.2.2021], Quelle Abbildung rechts unten (Standbild aus Video, bei Minute 1:46): https://www.youtube.com/watch?v=mP_yfoXjbnE [28.2.2021]

Ein weiterer Ausschnitt aus der Benutzeroberfläche in Abbildung 10 (Mitte) zeigt Auswertungen über den Ablauf der Abwicklung von Bestellungen bei einem Unternehmen. Dabei ist ersichtlich, welche Aktivitäten hauptsächlich durchgeführt werden und welchen Zeitaufwand diese anteilig verursachen, von der Einsichtnahme in die Kundendatenbank über die Überprüfung der Kreditwürdigkeit bis zur Bestätigung der Produktverfügbarkeit. In einer weiteren Tortengrafik wird dargestellt, zu welchen zeitlichen Anteilen die Beschäftigten auf ihren Rechnern Excel, Outlook sowie Anwendungen von Salesforce und SAP nutzen. In einem Ablaufdiagramm über die erfassten Nutzerinteraktionen (siehe Abbildung 10 rechts oben) wird dargestellt, in welcher Reihenfolge die Anwendungen genutzt werden. Besonders sticht heraus, dass auch eine **Rangliste** namentlich genannter Beschäftigter angezeigt wird, gereiht nach dem Grad der Pünktlichkeit der Auslieferung der bearbeiteten Bestellungen, sowie eine Liste der von einer einzelnen Mitarbeiterin bearbeiteten Bestellungen samt Pünktlichkeitsgrad der Auslieferung.[337]

Automatisierung vermessen und steigern. Eine andere Produktdemonstration in Form eines Videos (siehe Abbildung 10 rechts) zeigt, welche große Zahlen an Nutzeraktivitäten in Verbindung mit betrieblichen Abläufen gesetzt und analysiert werden. Das Erstellen einer Bestellung wurde hier über 1,1 Millionen mal durchgeführt, das Scannen und Buchen der Rechnung jeweils ungefähr eine Million mal. Andere Arbeitsschritte wie die Änderung der abzurechnenden Währung führten nur zu etwa 26.000 Nutzeraktivitäten. Darüber hinaus wird für jeden Arbeitsschritt aufgeschlüsselt, welcher prozentuelle Anteil der Aktivitäten manuell bzw. automatisiert erfolgt.[338]

Um Abläufe im Anschluss an die Analyse tatsächlich zu automatisieren, kann einerseits auf andere Anbieter wie „Automation Anywhere“ zurückgegriffen werden, die sogenannte „Robotic Process Automation“ (RPA)[339] anbieten. Celonis bewirbt aber die eigenen Angebote zur Prozessautomatisierung mit direkter Anbindung an Systeme von SAP bis Oracle als überlegen.[340]

Datenschutz? Celonis beschreibt in einem Dokument, wie das System zum “Task Mining” datenschutzkonform einsetzt werden könnte.[341] Die überwachten Anwendungen und erfassten Metadaten können etwa eingeschränkt werden. Benutzernamen, eingegebene Texte und andere Informationen können ausgeblendet werden. Die Daten können pseudonymisiert werden, womit sie aber immer noch personenbezogene Daten im Sinne der DSGVO bleiben. Betriebe können wahlweise eine Maske einblenden, die die Beschäftigten um ihre freiwillige „Einwilligung“ für die Datenverarbeitung durch Celonis bittet. Die „Einwilligung“ ist aufgrund des Machtungleichgewichts zwischen Betrieb und Beschäftigten aber eine sehr fragwürdige Rechtsgrundlage (vgl. Däubler 2017, S. 121ff).

Ob die vorgeschlagenen Maßnahmen den Anforderungen von DSGVO und Arbeitsrecht in Österreich und Deutschland genügen können, hängt auch vom konkreten Einsatz ab und kann hier nicht abschließend beurteilt werden. In jedem Fall verarbeitet das System sehr exzessive personenbezogene Daten über Arbeitstätigkeiten von Beschäftigten und kann für eine Vielfalt an Zwecken eingesetzt werden.

---

[337] https://www.celonis.com/de/intelligent-business-cloud/desktop-data-collection [28.2.2021]
[338] https://www.youtube.com/watch?v=mP_yfoXjbnE [28.2.2021]
[339] https://www.gartner.com/en/information-technology/glossary/robotic-process-automation-rpa
[340] https://www.celonis.com/solutions/initiatives/rpa-automation [28.2.2021]
[341] https://assets.ctfassets.net/zmrtlfup12q3/4FvTct1rFVTE3TOgSKkplY/0a9d18ae5afdad71cb295d5e686ee2bc/20210121-Task_Mining_Data_Privacy_by_Design_-_Whitepaper.pdf [28.2.2021]

6.4 Beschäftigte als Risiko: Verhaltensdaten für IT-Sicherheit

Die IT-Infrastruktur von Unternehmen ist vielfältigen Bedrohungen ausgesetzt. Zur Gewährleistung von Informationssicherheit wird eine große Vielfalt an unterschiedlichen technischen Systemen eingesetzt (siehe Abschnitt 5.6.3). Einige IT-Sicherheitslösungen verarbeiten in sehr exzessiver Weise personenbezogene Daten über ArbeitnehmerInnen und ihr Verhalten, direkt oder indirekt. Systeme zur Erkennung, Verhinderung und Analyse von Cyberangriffen werten heute in Echtzeit umfassende Daten aus allen möglichen Datenquellen im Unternehmen aus. Neben Bedrohungen von außen stehen auch die Beschäftigten als mögliche „Insider" unter Pauschalverdacht.

Unzufriedene Beschäftigte und interner Aktivismus. Wie Abbildung 11 (links) zeigt, empfiehlt der Chiphersteller und IT-Konzern Intel in einem „Weißbuch" zur IT-Sicherheit, ArbeitnehmerInnen in vielfacher Hinsicht als potenzielle Bedrohung zu betrachten. So könnten Beschäftigte etwa im Interesse „feindlich" gesonnener Konkurrenzunternehmen, Zulieferer, Partner, dem organisierten Verbrechen oder gar dem Terrorismus arbeiten. Sie könnten schlicht leichtsinnig, abgelenkt oder schlecht ausgebildet sein, das Unternehmen durch Diebstahl oder aus Unzufriedenheit schädigen – oder auch weil sie als „Aktivisten" bestimmte Anliegen unterstützen. Ähnlich der IT-Sicherheitskonzern Forcepoint, der „Menschen" als „Risikofaktor Nummer Eins" für Organisationen bezeichnet. Wie folgende Abbildung (rechts) aus einer Präsentation von Forcepoint zeigt, zählen zu den vermuteten Bedrohungen etwa Beschäftigte mit gehackten Zugangsdaten, aber auch Fahrlässigkeit sowie der Diebstahl von Daten oder Geschäftsgeheimnissen. Auch unzufriedene ArbeitnehmerInnen, die einen „großen Streit mit dem Chef" hatten und zu „Saboteuren" werden, und „interne Aktivisten", die Informationen an Medien geben könnten, werden genannt:[342]

THREAT AGENT TYPE	DEFINITION
Reckless Insider	Person who knowingly and deliberately circumvents safeguards for expediency but does not intend harm or serious consequences
Untrained/Distracted Insider	Person with harmless intent who inadvertently misuses systems or safeguards
Outward Sympathizer	Person who knowingly misuses the enterprise's systems to attack others in support of a cause external to the enterprise, but with harmless intent to the enterprise itself
Supplier	Business partner who seeks inside information for business advantage over its own competitors (that is, other suppliers)
Partner	Business partner with whom the enterprise has voluntarily shared sensitive data for collaborative efforts and who may either accidentally or deliberately expose that information
Irrational Individual	Person acting with illogical purpose and behavior
Thief	Opportunistic person with profit motive
Disgruntled Insider	Unhappy current or former insider with intent to harm the enterprise, industry, or fellow insider
Activist	Highly motivated supporter of a cause who does not engage in physical violence
Terrorist	Person who relies on physical violence or extreme acts to support a socio-political agenda
Organized Crime	Crime syndicate with significant resources and attack skills
Competitor	Business adversary who competes for customers, revenues, public exposure, or resources
Nation State	State-sponsored attacker with significant resources, and able to affect a major disruption to even national scale

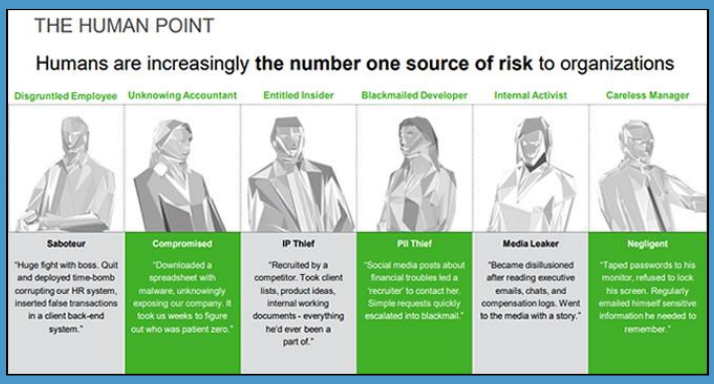


Abbildung 11: Beschäftigte als „Insider"-Bedrohung für den Betrieb bei Intel (links) und Forcepoint (rechts)

Wie die Beispiele in den folgenden Abschnitten zeigen, verschwimmen die Grenzen zwischen IT-Sicherheit, Betrugs- und Diebstahlsprävention, dem Schutz von Kundendaten und Geschäftsgeheimnissen („Data Loss Prevention", abgekürzt „DLP") oder etwa der Sicherstellung der Einhaltung von Gesetzen, Richtlinien und sonstiger Verhaltensregeln im Unternehmen („Compliance") zunehmend. Systeme für die Abwehr von Cyberangriffen, die Verwaltung von Zugriffsberechtigungen oder für die Fernwartung von Geräten greifen ineinander und werden auch

[342] Abbildung links © Intel, Abbildung rechts © Forcepoint. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quellen: Casey, Tim (2015): A Field Guide to Insider Threat. IT@Intel White Paper, October 2015. Online: https://www.researchgate.net/publication/324068663_A_Field_Guide_to_Insider_Threat_Understanding_Insider_Threat_Vectors_to_Further_Improve_Enterprise_Security_Strategies [18.3.2021], Forcepoint (2017): Forcepoint UEBA User & Entity Behavior Analytics. Online: https://www.forcepoint.com/sites/default/files/resources/files/presentation_ueba_webinar_slides_en.pdf [18.3.2021]

genutzt, um Fehlverhalten zu verhindern – ob fahrlässig, absichtlich, unabsichtlich oder in anderer Weise unerwünscht. Die gleiche Software, die das Abrufen auf virenverseuchte Websites verhindern soll, wird auch zur Sperrung des Zugriffs auf betrieblich unerwünschte Internet-Dienste eingesetzt und liefert Daten über Verhaltensmuster.

6.4.1 SIEM und UEBA – Analyse von Verhaltensdaten

Im weiten Feld der IT-Sicherheit wird eine Vielzahl von Bezeichnungen und Abkürzungen für unterschiedliche Arten von Systemen verwendet. So führen etwa integrierte Plattformen für „Security Information and Event Management" (SIEM) Log- und Ereignisdaten aus bestehenden IT-Systemen im Unternehmen zusammen. Software für „User and Entity Behavior Analytics" (UEBA) analysiert explizit Nutzerverhalten, um als Risiko oder als Bedrohung eingeschätzte Verhaltensweisen zu erkennen – auf Basis von Regeln sowie von KI-Analysetechnologien. Diese Systeme „lernen" laufend, wie sich Beschäftigte „normalerweise" verhalten und versuchen dann, außergewöhnliches bzw. „anormales" Verhalten zu erkennen und das damit verbundene Risiko zu bewerten. Dabei werden vielfältige Datenquellen in Echtzeit überwacht – vom Netzwerkdatenverkehr und der Nutzung von Geräten und Programmen über die Ablage und Bearbeitung von Dateien und jeglicher Kommunikation bis hin zur Einbeziehung von Personal- oder gar Leistungsdaten. Mehrere Produkte werten sogar Tastatureingaben aus und zeichnen auf, was am Bildschirm zu sehen ist – für den Einsatz in „forensischen" Untersuchungen vergangener Aktivitäten von ArbeitnehmerInnen. Zu den bekannten Anbietern in den Bereichen SIEM und UEBA zählen unter anderem IBM, Microsoft, Forcepoint, Splunk, Exabeam, Securonix, LogRhythm, Rapid7 oder Micro Focus.[343]

Nähe zu Militär und Geheimdiensten, Diskreditierung von Gewerkschaften. Einige Anbieter haben enge Verbindungen zum militärischen Bereich und zu Geheimdiensten. Die CIA-Risikokapitalgesellschaft In-Q-Tel[344] war und ist an einer ganzen Reihe von IT-Sicherheitsfirmen beteiligt[345] – so etwa am 2019 von Micro Focus übernommenen UEBA-Anbieter Interset[346] oder am 2017 von Forcepoint übernommenen UEBA-Anbieter RedOwl.[347] Forcepoint selbst gehörte bis vor kurzem zum US-Rüstungsgiganten Raytheon, bevor das Unternehmen 2020 von einer privaten Beteiligungsgesellschaft übernommen wurde.[348] Der Gründer von RedOwl, dessen Software nun die UEBA-Funktionen von Forcepoint abdeckt, ist ehemaliger NSA-Offizier und hatte zuvor das Unternehmen Berico Technologies gegründet, das an einem 2011 aufgedeckten Plan zur großangelegten Diskreditierung gewerkschaftlicher Gruppen in den USA beteiligt war[349] – etwa mittels Auswertung von Socialmedia-Daten.[350] [351]

---

[343] Marktüberblicke siehe z.B. Gartner (2018): Market Guide for User and Entity Behavior Analytics, 23.4.2018; Gartner (2020): Magic Quadrant for Security Information and Event Management, 18.2.2020; Forrester (2020): The Forrester Wave: Security Analytics Platforms, Q4 2020, 1.12.2020

[344] https://www.dhs.gov/science-and-technology/iqt [18.3.2021]

[345] https://www.iqt.org/portfolio?&taxonomy=tech_areas&tax_id=147, https://www.iqt.org/portfolio?&taxonomy=tech_areas&tax_id=156 [18.3.2021]

[346] https://www.microfocus.com/en-us/products/interset/overview [18.3.2021]

[347] Biesecker, Calvin (2017): Raytheon's Forcepoint Cyber Company Acquires Behavior Analytics Firm RedOwl. Defense Daily, 29.8.2017. Online: https://www.defensedaily.com/raytheons-forcepoint-cyber-company-acquires-behavior-analytics-firm-redowl/business-financial/

[348] Harris, David (2020): Raytheon Unloads Security Subsidiary Forcepoint To Private Equity. CRN, 27.10.2020. Online: https://www.crn.com/news/security/raytheon-unloads-security-subsidiary-forcepoint-to-private-equity

[349] Harkinson, Josh (2011): ChamberLeaks: What Did The Chamber Know? Mother Jones, 12.2.2011. Online: https://www.motherjones.com/politics/2011/02/chamberleaks-strategies-defame-foes-us-chamber-revealed/

[350] Johnson, Brad (2011): ChamberLeaks: Military Contractors Palantir And Berico Under Scrutiny. Think Progress, 19.3.2011. Online: https://archive.thinkprogress.org/chamberleaks-military-contractors-palantir-and-berico-under-scrutiny-480cae35e353/

[351] Danke an Michelle Miller, die die Verbindungen zwischen RedOwl, Berico Technologies und dem „ChamberLeaks" Skandal recherchiert hat

6.4.2 Umfassendes Profiling von Beschäftigten mit „Forcepoint“

Forcepoint ist ein führender IT-Sicherheitsanbieter für Unternehmen. Neben Produkten für Cloud- und Netzwerksicherheit und für das Filtern und Sperren von Zugriffen auf unerwünschte Websites verkauft Forcepoint Software zur Analyse von Nutzerverhalten (UEBA), zum Schutz betrieblicher Daten (DLP) und zur Verhinderung von Bedrohungen durch „Insider“.[352]

Das UEBA-System von Forcepoint wertet kontinuierlich eine Vielzahl an Log- und Ereignisdaten über Aktivitäten von Beschäftigten aus und berechnet daraus Risikobewertungen. Dazu zählen Login-Vorgänge, auf dem Rechner genutzte Programme, das Öffnen, Ändern oder Kopieren von Dateien, Zugriffe auf Websites, Suchvorgänge mit Google, Kommunikation via E-Mail, Chat und Telefon inklusive Kommunikationsinhalte – bei Anrufen mittels automatisierter Transkription von Sprache in Text – und sogar Daten über den physischen Zutritt zu Räumlichkeiten.[353] Der Ausschnitt aus der Benutzeroberfläche in folgender Abbildung (links) zeigt, wie „auffällige“ Beschäftigte mit hohen Risiko-Scores in einer Liste dargestellt werden, die Abbildung (rechts) zeigt eine Auswertung über die Aktivitäten einer Einzelperson:[354]

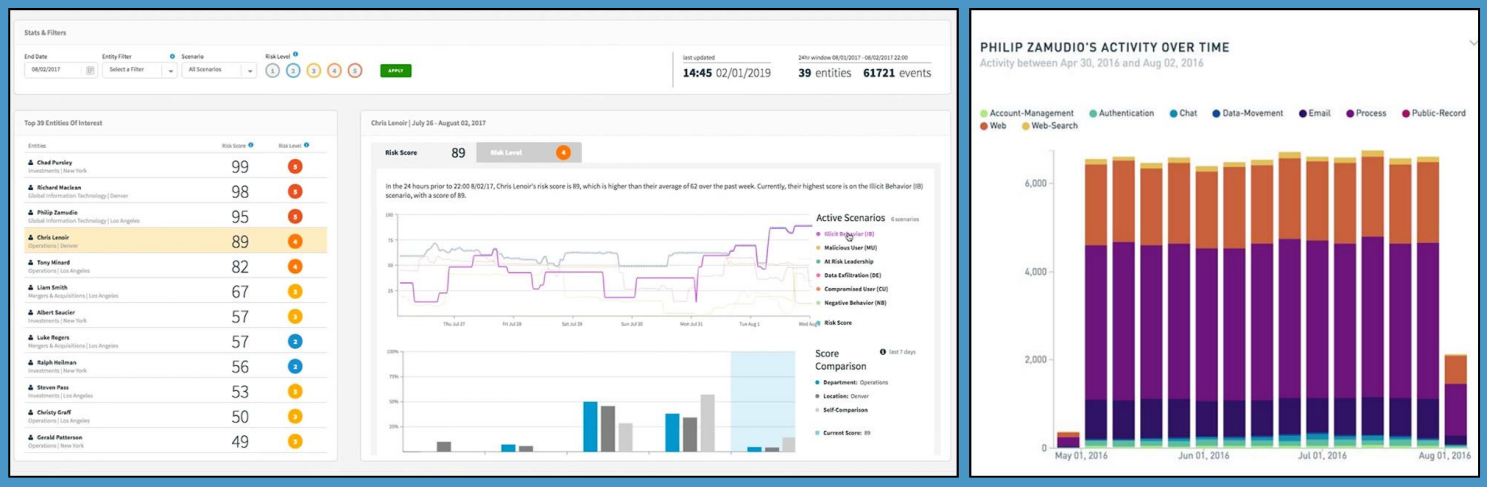


Abbildung 12: „Riskante“ Beschäftigte (links) und Auswertung Einzelperson (rechts) bei Forcepoint. Quelle: Hersteller

Umfassendes Profiling von ArbeitnehmerInnen. Die Gesamtrisikobewertung für eine Einzelperson ergibt sich dabei aus der Summe der Risikobewertungen hinsichtlich unterschiedlicher vorab definierter Bedrohungs-Szenarien. In Abbildung 12 (links) ist ersichtlich, wie sich bei einem bestimmten Beschäftigten der Risiko-Score für das Szenario „rechtswidriges Verhalten“ im Lauf einer Woche verändert bzw. erhöht hat. Der Score für das Szenario „Kompromittierter Nutzeraccount“, also das Risiko eines gehackten Accounts, ist hingegen niedrig. Die Risiko-Scores werden außerdem ins Verhältnis zu Durchschnittswerten für Abteilung, Standort und des früheren Verhaltens des Beschäftigten gesetzt. Die individuellen Risikobewertungen pro Szenario setzen sich wiederrum aus Risiko-Scores für bestimmte Verhaltensweisen zusammen, die Forcepoint „Verhaltensmodelle“ nennt und die jeweils

[352] https://www.forcepoint.com/products [18.3.2021]
[353] https://www.websense.com/content/support/library/ueba/v33/user_manual/user_manual.pdf [18.3.2021]
[354] Beide Abbildungen (c) Forcepoint. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle links Standbild Video bei Minute 1:01: https://www.youtube.com/watch?v=Y3mum4tSmXI [18.3.2021], Quelle rechts S. 32 https://www.websense.com/content/support/library/ueba/v33/user_manual/user_manual.pdf [18.3.2021]

die Wahrscheinlichkeit dafür angeben, ob eine außergewöhnliche Verhaltensweise einer Person vorliegt.[355] Folgende Tabelle zeigt eine Auswahl voreingebauter Szenarien und Verhaltensmodelle, deren Nutzung Forcepoint bei der Einrichtung eines IT-Sicherheitssystems „empfiehlt“:[356]

Szenario	Risiko-Verhaltensmodell	Beschreibung
Datenverlust	Interne Datenbewegungen	Anormale Bewegungen von Daten innerhalb des Unternehmens
	Externe Datenbewegungen	Anormale Bewegungen von Daten außerhalb des Unternehmens-Netzwerks
	Dateioperationen	Anormale Interaktionen mit Dateien wie z.B. Dateizugriff, um den Inhalt zu prüfen
	Dateifreigabe-Volumen	Zugriff auf eine anormale Zahl unterschiedlicher Dateifreigaben
	Erkundung	Aktivitäten, die auf das breite Durchsuchen von Datenbeständen hindeuten
	Datenabfluss	Verhaltensweisen, die auf die Weitergabe sensibler Informationen hindeuten
Verdächtiger Nutzer	Erkundung des Netzwerks	Durchsuchen des Unternehmensnetzwerks nach Ressourcen
	Verdächtiger Login	Anormale Login-Aktivitäten
	Anforderung von Berechtigungen	Anforderung von Nutzerberechtigungen zur Durchführung verdächtiger Aktivitäten
	Verwaltung von Berechtigungen	Berechtigungsverwaltung durch Beschäftigte, die dies normalerweise nicht tun
	Prozess-Aktivitäten	Verdächtige laufende Programme mit privilegierten Berechtigungen
	Systemadministration	Aktivitäten, die Systemkonfigurationen beschädigen könnten
	Systemkomponenten	Interaktionen mit System-Dateien
	Verdächtige Informationssammlung	Sammlung von Informationen über die Durchführung verdächtiger Aktivitäten
	Physischer Zutritt	Anormaler Zutritt zu sensiblen Räumlichkeiten
Kompromittierter Nutzeraccount	Phishing	Risiko, dass Beschäftigte Opfer von Phishing geworden sind, etwa durch bösartige Anhänge oder Links in gefälschten E-Mails
	Schadsoftware	Risiko, dass Beschäftigte unabsichtlich Schadsoftware installiert haben
Negatives Verhalten	Obszöne Inhalte	Aufruf von „obszönen“ Websites oder Eingabe entsprechender Web-Suchbegriffe
	Negatives Sentiment	Negative Stimmung oder unangemessene Diskussionen in Kommunikationsdaten
	Kündigungsrisiko	Kommunikationsdaten oder aufgerufene Websites zeigen Kündigungsabsichten (z.B. Lebenslauf in E-Mail, Aufruf von Job-Portalen)
	Finanzielle Schwierigkeiten	Kommunikationsdaten oder aufgerufene Websites zeigen, dass Beschäftigte in finanziellen Schwierigkeiten sind und nach Wegen suchen, das zu ändern
	Entzug von Aufsicht/Kontrolle	Kommunikationsdaten zeigen Anzeichen dafür, dass sich Beschäftigte Kontrollmaßnahmen und Aufsicht entziehen möchten
	Verringerte Produktivität	Beschäftigte verbringen viel Zeit mit nicht-arbeitsbezogenen Aktivitäten
	Disengagement, Rückzug	Beschäftigte interagieren nicht mit wichtigen Unternehmensressourcen
	Kommunikationsvolumen	Beschäftigte kommunizieren weniger mit anderen Beschäftigten als zuvor
	Gewalt am Arbeitsplatz	Kommunikationsdaten zeigen Anzeichen für Vorfälle von Gewalt am Arbeitsplatz
	Sexuelle Belästigung am Arbeitsplatz	Kommunikationsdaten zeigen Anzeichen für sexuelle Belästigung am Arbeitsplatz
Rechtswidriges Verhalten	Industriespionage	Kommunikation mit Konkurrenzunternehmen, die Geschäftsgeheimnisse enthält oder auf Jobwechsel-Absichten hindeutet
	Whistleblowing	Kommunikation mit Medien, die auf die Bereitschaft zur Weitergabe interner Informationen hindeutet
	Clearance Evasion	Suche nach Informationen zur Umgehung von Sicherheitsüberprüfungen oder Lügendetektortests

Tabelle 2: Auswahl von Auswertungen über Beschäftigte bei Forcepoint. Quelle: Hersteller

[355] https://www.websense.com/content/support/library/ueba/v33/user_manual/user_manual.pdf [18.3.2021]

[356] Ebd., S. 85ff. Übersetzung durch den Verfasser (ohne Gewähr). Quelle für „Komprimittierter Nutzeraccount“: https://www.forcepoint.com/sites/default/files/resources/files/presentation_ueba_webinar_slides_en.pdf [18.3.3021]

Während die Erkennung von Phishing, Schadsoftware, verdächtigen Login-Aktivitäten oder ungewöhnlichen Änderungen bei Systemdateien noch dem engeren Feld der IT-Sicherheit zuordenbar sind, stellen die meisten anderen Modelle die Beschäftigten unter Pauschalverdacht und greifen durch eine fast vollständige Überwachung des Arbeitsalltags unverhältnismäßig in ihre Rechte und Freiheiten ein.

Weitreichende Auswertungen. Die dem Szenario „Negatives Verhalten" zugeordneten Verhaltensmodelle versuchen durch Auswertung von Web- und Kommunikationsaktivitäten zu erkennen, ob ArbeitnehmerInnen in finanziellen Schwierigkeiten stecken, ob sie Kündigungsabsichten haben, wieviel sie mit KollegInnen kommunizieren, ob sie „obszöne" Inhalte aufrufen oder ob eine „negative" Stimmung herrscht. Sogar Leistungsdaten über „verringerte Produktivität" werden einbezogen. Bei der Erkennung von Gewalt oder sexueller Belästigung am Arbeitsplatz stellt sich die Frage, ob dazu derart tiefgreifende Überwachungsmaßnahmen angemessen sind – oder ob es hier vielleicht gar nicht vorrangig um den Schutz der Betroffenen geht, sondern nur um einen weiteren fragwürdigen Indikator zur Erkennung von mutmaßlich unzuverlässigen Beschäftigten. Die Erkennung einer etwaigen Ansammlung betrieblicher Daten erfordert eine vollständige Überwachung von Dateizugriffen und Suchvorgängen. Während derartige Maßnahmen zur Verhinderung von Industriespionage noch gerechtfertigt erscheinen mögen, hinterlässt der Zweck einer Verhinderung der Weitergabe von Informationen an Medien einen sehr schalen Nachgeschmack.[357]

Untersuchung von Beschäftigtenaktivitäten im Detail. Während die beschriebenen Modelle darauf abzielen, als riskant bewertete Verhaltensweisen zu entdecken, können in Folge einzelne Beschäftigte unter besondere Beobachtung gestellt und deren Aktivitäten näher untersucht werden. Eine Produktdemonstration zeigt, wie das System zur Analyse des Verhaltens eines Flughafen-Mitarbeiters genutzt wird, der des Drogenhandels verdächtigt wird:[358]

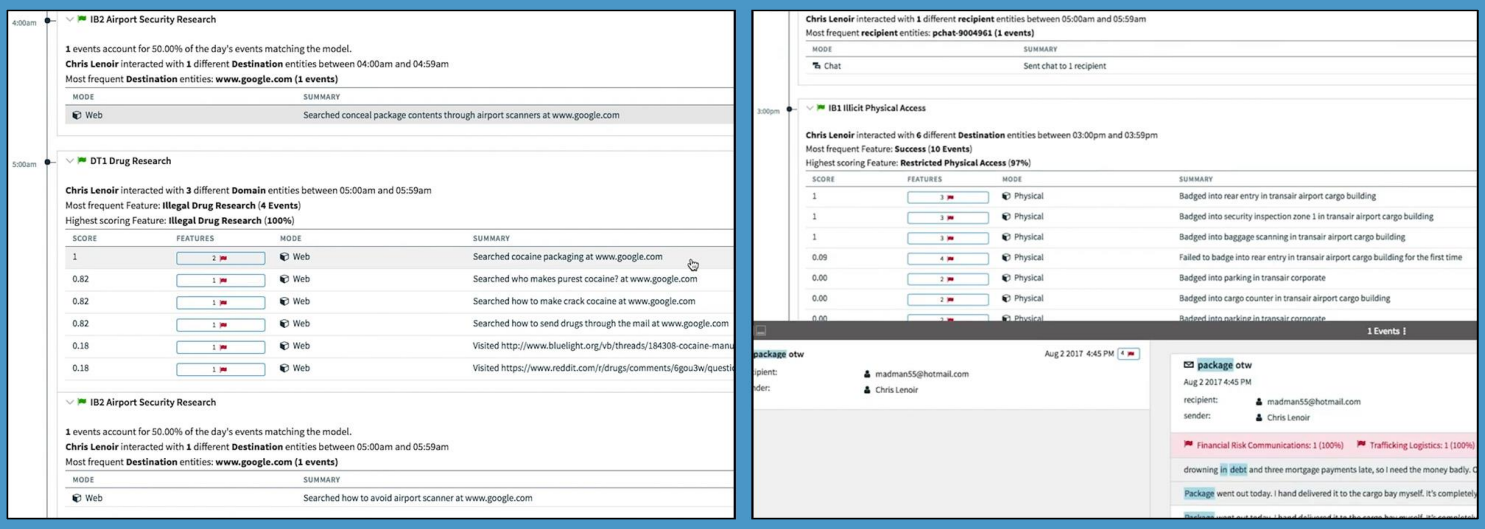


Abbildung 13: Einblick in die Aktivitäten eines verdächtigen Beschäftigten bei Forcepoint. Quelle: Hersteller

Abbildung 13 (links) zeigt, wie das System eine Reihe von verdächtigen Website-Aufrufen und Google-Suchbegriffen darstellt und bewertet. Der betroffene Mitarbeiter hat hier danach gesucht, wie Drogen erworben, veredelt, verpackt und versandt werden und wie sie an Kontrollen vorbei geschleust werden können. In Folge habe er zwei

[357] Ebd.

[358] Beide Abbildungen Standbild aus Video (c) Forcepoint. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quellen bei Minute 1:27 und 2:02: https://www.youtube.com/watch?v=Y3mum4tSmXI [18.3.2021]

Websites zum Thema aufgerufen. Abbildung 13 (rechts) zeigt eine detaillierte Abfolge von Räumlichkeiten, zu denen er sich mittels Karte Zutritt verschafft hat. In einem Gebäude wurde ihm der Zutritt verwehrt. Dazu wird eine E-Mail samt Inhalt dargestellt, die den Arbeitnehmer wegen Wörter wie „Schulden“ und „Paket“ als „in finanziellen Schwierigkeiten“ einstuft und einen Bezug zu Drogenhandel herstellt. Auch eine Chat-Nachricht wird als verdächtig eingestuft. Das Szenario „Rechtswidriges Verhalten“ nutzt hier im Vergleich zu den in Tabelle 2 angeführten Risikoverhaltensmodellen noch weitere ergänzende Modelle, die auf die Umgebung Flughafen zugeschnitten sind.[359]

Als **Datenquellen** für das System werden neben Produkten von Microsoft (Windows, Active Directory, Exchange, Office 365, Skype), Salesforce (CRM, Slack), SAP (Concur) oder Cisco auch Personalverwaltungssysteme wie Workday angeführt. Auch Logdaten von Druckern, GPS-Standortdaten[360] und Mitarbeiterbeurteilungen[361] werden als mögliche Datenkategorien genannt. Aktivitäten am Wochenende bzw. außerhalb der Arbeitszeit werden generell als riskanter bewertet, was impliziert, dass auch Aktivitäten am Wochenende bzw. außerhalb der Arbeitszeit überwacht werden.[362] Dazu können Listen von Schlüsselwörtern verwaltet werden, die zur Erkennung von „negativer Stimmung“ oder anderen als riskant eingeschätzten Verhaltensweisen herangezogen werden. Eine anpassbare Liste der Adressen von Job-Websites fließt in die Bewertung des Kündigungsrisikos ein.[363]

Forensische Untersuchung von Tastatureingaben und PC-Nutzung. Während die Verhinderung von Bedrohungen durch „Insider“ bei den beschriebenen Produkten für UEBA-Nutzerverhaltenanalyse nur einen von mehreren Einsatzzwecken darstellt, bietet Forcepoint auch Software an, bei der es explizit um „Insider“ geht.[364] Dabei werden auf den Rechnern der Beschäftigten[365] noch viel weitgehendere Nutzungsdaten erfasst.

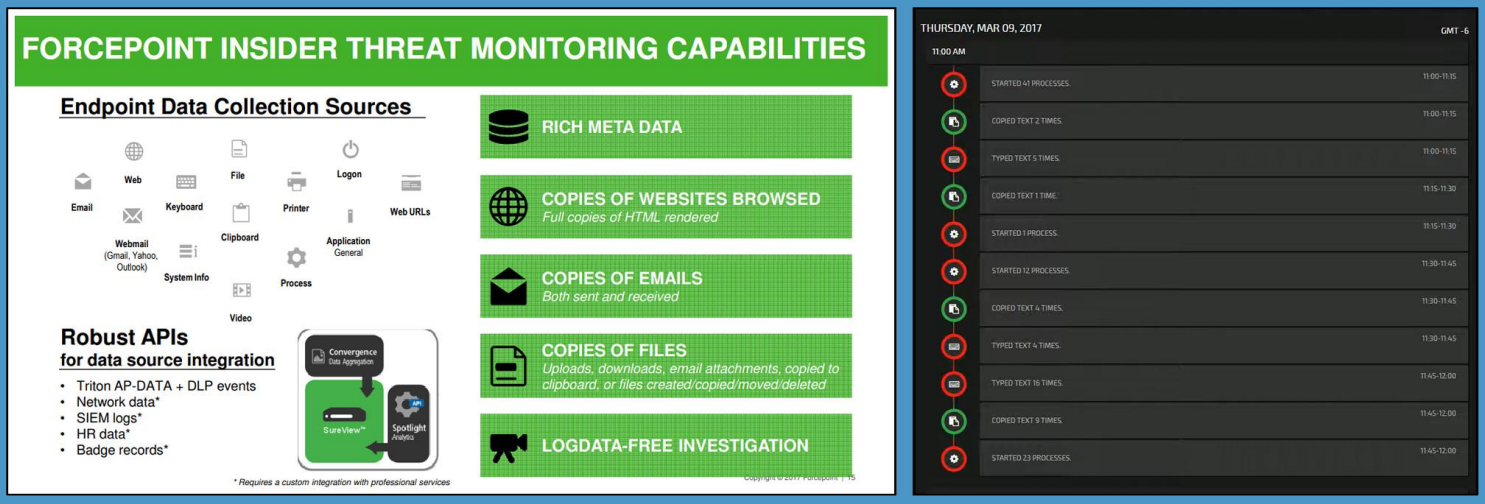


Abbildung 14: Datenquellen (links) und Auswertung (rechts) bei „Forcepoint Insider Threat“. Quelle: Hersteller

[359] Ebd.
[360] https://www.forcepoint.com/sites/default/files/resources/files/ueba-platform-architecture-overview.pdf, https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_brief_behavioral_analytics_en.pdf [18.3.2021]
[361] https://www.forcepoint.com/sites/default/files/resources/datasheets/ueba-discover-and-stop-insider-threat.pdf [28.3.2021]
[362] S. 19 https://www.websense.com/content/support/library/ueba/v33/user_manual/user_manual.pdf [28.3.2021]
[363] Ebd., S. 51
[364] https://www.forcepoint.com/product/fit [18.3.2021]
[365] https://www.forcepoint.com/deployment/endpoint-security-solutions [18.3.2021]

Abbildung 14[366] zeigt mögliche Datenquellen (links) und einen Ausschnitt aus der Benutzeroberfläche (rechts), mit der etwa gestartete Programme, Texteingaben und Kopiervorgänge über die Zwischenablage nachvollzogen werden können. Dieses weiterreichende System zur Verhinderung von Bedrohungen durch „Insider" analysiert und bewertet ebenfalls fortlaufend das Verhalten der Beschäftigten. Darüber hinaus können Untersuchungen durchgeführt werden. Neben Tastatureingaben, Kopiervorgängen über die Zwischenablage und der Anfertigung von Screenshots wird die Tätigkeit am Rechner in einer Form aufgezeichnet, die es ermöglicht, im Nachhinein komplette Nutzungsvorgänge samt sichtbarer Bildschirminhalte als Video einzusehen – für die „forensische" Untersuchung von Vorfällen.[367] Laut einer Broschüre ermöglichen die Videoaufnahmen einen „Über-die-Schulter-Blick" auf den Rechner des Beschäftigten.[368] Insgesamt überwacht „Insider Threat" von Forcepoint laut Eigenangabe über eine Million Geräte.[369] Über alle IT-Sicherheitsprodukte hinweg analysiert Forcepoint Daten von über 900 Millionen Geräten.[370]

Normalisierung invasiver Überwachung? Die in Tabelle 2 angeführten Funktionen zur Erkennung von Versuchen, Sicherheitsüberprüfungen oder gar Lügendetektortests zu umgehen, weisen auf den militärischen und geheimdienstlichen Hintergrund von Forcepoint hin. Andere verfügbare Risiko-Szenarien wie die Erkennung von „Insider Trading" oder „Conduct Risk" überwachen unter anderem „persönlichen Aktienhandel im Web" oder eine mögliche Erpressbarkeit von Beschäftigten und sind wohl hauptsächlich für Banken und Finanzwelt vorgesehen.[371] Der Einsatz von Forcepoint beschränkt sich allerdings bei weitem nicht auf diese Bereiche. Die Produkte für UEBA, Data Loss Prevention und die Erkennung von „Insider Threats" werden laut Eigenangabe von Rüstungskonzernen, Banken und Versicherungen, Energieversorgern, Telekom-Firmen, Fluglinien und Krankenhäusern sowie in allen möglichen Branchen von der Metall- und Automobilindustrie bis zum Getränkehersteller oder einem Kundenservice-Dienstleister eingesetzt[372] – auch in Deutschland.[373] Selbst wenn die exzessiven Funktionen zur Verhaltensüberwachung von Forcepoint nur in Hochsicherheitsbranchen und nur für privilegierte ArbeitnehmerInnen in sensiblen Arbeitsbereichen eingesetzt würden, greifen sie tief in die Autonomie der Beschäftigten ein und bieten ein hohes Potenzial für gezielten Missbrauch durch ArbeitgeberInnen. Darüber hinaus ist zu befürchten, dass derartig invasive Funktionen im Lauf der Zeit in immer mehr Bereichen eingesetzt werden, so sie erst einmal verfügbar sind.

Datenschutz? Im UEBA-System von Forcepoint können die in der Benutzeroberfläche angezeigten Namen der Beschäftigten im Analysealltag optional durch Pseudonyme ersetzt werden, sind bei Bedarf aber trotzdem immer zugänglich.[374] Die Produkte zur Verhinderung von Bedrohung durch „Insider" können in Bezug auf die ausgewerteten Datentypen angepasst werden.[375] In einer deutschsprachigen Präsentation verspricht Forcepoint die „Anonymisierung personenbezogener Daten" und „[v]ollständige Konformität zu DSGVO/GDPR". Es gäbe „kein[en] wahllosen Generalverdacht" gegen Beschäftigte. Ein „Mehr-Augen-Prinzip" sowie die „Einhaltung aller Anforderungen eines [Betriebsrats]" wären möglich.[376] Ob die vorgeschlagenen Maßnahmen den Anforderungen von

[366] Beide Abbildungen (c) Forcepoint. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle links S. 15, Präsentation 2017: https://oldsite.amcham.gr/wp-content/uploads/2017/11/NICK-NICOLESCU.pdf [18.3.2021]. Quelle rechts Standbild Video bei Minute 22:05: https://www.youtube.com/watch?v=qSHexqYW-jE [18.3.2021]
[367] https://www.forcepoint.com/sites/default/files/resources/files/brochure_sureview_insider_threat_en.pdf [18.3.2021]
[368] https://www.exit123c.com/wp-content/uploads/2016/05/Forcepoint_sureview_insider_threat_datasheet.pdf [18.3.2021]
[369] https://www.forcepoint.com/sites/default/files/resources/files/brochure_sureview_insider_threat_en.pdf [18.3.2021]
[370] https://www.forcepoint.com/sites/default/files/resources/brochures/brochure_forcepoint_dlp_endpoint_en.pdf [18.3.2021]
[371] https://www.forcepoint.com/sites/default/files/resources/files/presentation_ueba_webinar_slides_en.pdf [18.03.2021]
[372] https://www.forcepoint.com/de/company/customers?industry=All&products=All&location=All&region=All [18.3.2021]
[373] https://www.forcepoint.com/de/customer-stories/herdecke [18.3.2021]
[374] S. 27 https://www.websense.com/content/support/library/ueba/v33/user_manual/user_manual.pdf [18.3.2021]
[375] https://www.exit123c.com/wp-content/uploads/2016/05/Forcepoint_sureview_insider_threat_datasheet.pdf [18.3.2021]
[376] Forcepoint Präsentation, 2017, https://www.it-sa.de/CDB/download/26538302-2793-4f06-8150-044cd33c7d54

DSGVO und Arbeitsrecht in Österreich und Deutschland genügen können, darf bezweifelt werden, hängt aber auch vom konkreten Einsatz ab und kann hier nicht abschließend beurteilt werden.

6.4.3 Securonix und andere Anbieter wie IBM und Microsoft

Securonix, ein texanischer Anbieter von IT-Sicherheitsprodukten, vermarket seine Angebote im Bereich SIEM und UEBA[377] sehr offenherzig als umfassende Überwachungstechnologien. So wird etwa in einem düsteren Werbevideo dargestellt, wie ein „verärgerter" Beschäftigter dabei ist, betriebliche Informationen weiterzugeben. Schon zuvor landet er durch eine vorangegangene schlechte Leistungsbeurteilung auf der „Watchlist" des Systems von Securonix. Der Zugriff auf eine Job-Website macht ihn zum „Kündigungsrisiko". Außerdem betritt er die Büroräumlichkeiten außerhalb der üblichen Arbeitszeiten und das System beobachtet Dateizugriffe und Kopiervorgänge, die im Vergleich zu Beschäftigten mit ähnlichen Aufgabengebieten als ungewöhnlich bewertet werden.[378] Das System wird unter dem Markennamen „Snypr" verkauft – in Anlehnung an die englische Bezeichnung für Scharfschützen. Einem militärischen Scharfschützen ist üblicherweise ein sogenannter „Spotter" beigestellt, der die Umgebung beobachtet[379] – diese Bezeichnung nutzt Securonix für die eingebaute Suchmaschine.[380]

Die UEBA-Lösung von Securonix verspricht, durch laufend eingespeiste Daten aus unterschiedlichen betrieblichen Systemen zu "lernen", wie sich Netzwerk, Geräte und Beschäftigte „normalerweise" verhalten und davon ausgehend auffälliges, abweichendes, anormales Verhalten zu erkennen – zur Bekämpfung von Cyberangriffen, aber auch von Betrug und betriebsinternen Bedrohungen durch "Insider".[381]

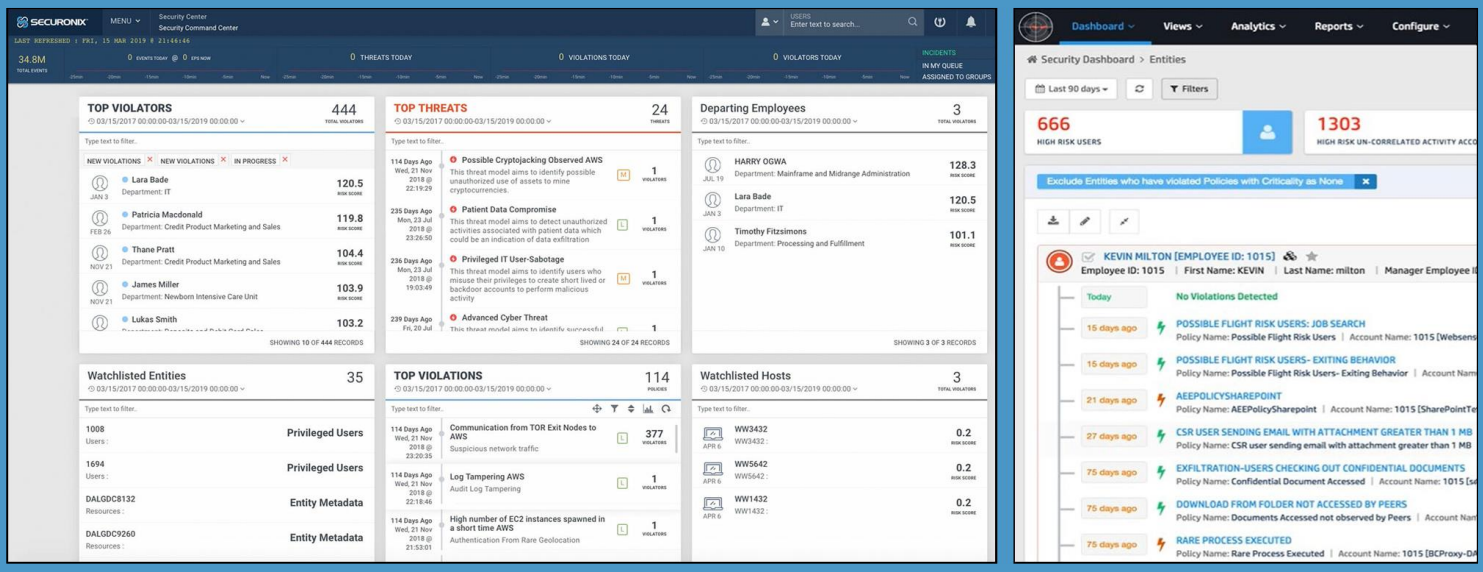


Abbildung 15: „Riskante" Beschäftigte (links) und Auswertung Einzelperson (rechts) bei Securonix. Quelle: Hersteller

[377] https://www.securonix.com/ [25.3.2021]
[378] https://www.youtube.com/watch?v=a9nJuGVmn7w [25.3.2021]
[379] Vgl. https://en.wikipedia.org/wiki/Sniper
[380] https://documentation.securonix.com/onlinedoc/Content/Cloud/Content/Glossary.htm [25.3.2021]
[381] https://www.securonix.com/web/wp-content/uploads/2019/06/Securonix-UEBA-Datasheet.pdf [25.3.2021]

Der Ausschnitt aus der Benutzeroberfläche in Abbildung 15[382] (links) zeigt, wie als auffällig eingestufte Personen samt Risiko-Scores aufgelistet werden. ArbeitnehmerInnen, die bald das Unternehmen verlassen, stehen ebenfalls unter gesonderter Beobachtung. Abbildung 15 (rechts) zeigt einen weiteren Ausschnitt aus der Benutzeroberfläche mit detaillierteren Profildaten zu einem von hunderten „Hochrisiko-Nutzern", die als Bedrohung identifiziert wurden. Der betroffene Beschäftigte hat auf vertrauliche Dokumente sowie auf einen Ordner zugegriffen, auf den ArbeitnehmerInnen mit ähnlichen Tätigkeitsbereichen laut Verhaltensanalyse normalerweise nicht zugreifen, eine E-Mail mit einem Anhang größer als 1 MB verschickt – und die besuchten Websites deuten für Securonix auf eine Job-Suche und auf ein baldiges Verlassen des Unternehmens hin.

Verdächtige Verhaltensweisen. Securonix erwähnt in der Dokumentation viele andere Verhaltensweisen, die als Teil von „Bedrohungsmodellen" dazu führen können, dass Beschäftigte als Risiko bewertet werden – von einer „anormalen Zahl ausgedruckter Seiten" über „Anomalien bei den gearbeiteten Stunden" bis zum physischen Zutritt zu Gebäuden, die Beschäftigte mit ähnlichen Tätigkeitsbereichen laut Verhaltensanalyse normalweise nicht betreten. Neben der Suche nach Jobs im Netz oder dem Ausdrucken von Lebensläufen können sich ArbeitnehmerInnen auch durch E-Mail-Weiterleitungen oder den E-Mail-Versand an die private E-Mail-Adresse verdächtig machen. Ebenso können eine durch die Überwachung von Anmeldevorgängen und E-Mail-Kommunikation festgestellte „Produktivitätsverminderung", schlechte Leistungsbeurteilungen oder nicht erfolgte Beförderungen, Bonuszahlungen oder Gehaltserhöhungen die Beschäftigten zum Risiko machen.[383]

Darüber hinaus erwähnt Securonix weitere „Bedrohungsindikatoren" wie „Überarbeitung", „Unzufriedenheit", „psychosoziale Anomalien" in Bezug auf „Aggressionsbewältigung", „Stress" oder „Missachtung von Autorität" und andere „persönliche" bzw. „nicht-technische" Risikoindikatoren. Es wird nicht angeführt, welche Datenquellen und Verhaltensweisen hier relevant sind. In einem Fall wird erwähnt, dass die Diagnose „Unzufriedenheit" und „Missachtung von Autorität" auf Grundlage der erfassten Suchbegriffe im Web erfolge.[384] Die Namen und Domains von Konkurrenzunternehmen, Job-Websites, „nicht geschäftlichen" Websites und andere „kritische Schlüsselwörtern", die zur Erkennung von riskanten Verhaltensweisen genutzt werden, können angepasst werden.[385]

Als **Datenquellen** können Aktivitätsdaten aus Systemen verschiedener Hersteller dienen – von Microsoft Windows, Active Directory, Outlook und Office 365[386] bis zu Systemen und Cloud-Diensten von Cisco, IBM, Oracle, Symantec, Google, Amazon, Slack und Salesforce.[387] Auch Daten aus Personalverwaltungssystemen wie Workday[388] und Ereignisprotokolle aus dem ERP-System von SAP können eingebunden werden.[389]

---

[382] Beide Abbildungen (c) Securonix. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle rechts: https://www.scmagazine.com/wp-content/uploads/2020/03/Securonix.jpg [25.3.2021], Quelle rechts Standbild Video bei Minute 46:24: https://www.youtube.com/watch?v=UyPBzmJFsEo [25.3.2021]

[383] Übersetzungen durch den Verfasser (ohne Gewähr), Quelle: https://documentation.securonix.com/onlinedoc/Content/6.2%20CU4/Content/Apps%20and%20Add%20ons/Data%20Security%20Analytics.htm [6.9.2021]

[384] Ebd.

[385] https://documentation.securonix.com/onlinedoc/Content/6.4%20Cloud/Content/SNYPR%206.3/Cloud/Data%20Integration%20Guide/6.3%20Lookup%20Tables_Intro.htm [6.9.2021]

[386] https://documentation.securonix.com/onlinedoc/Content/Connectors/Content/Content%20Guides/Supported%20Datasources/Vendors/Microsoft%20Corporation.htm [6.9.2021]

[387] https://documentation.securonix.com/onlinedoc/Content/Connectors/Content/Content%20Guides/Supported%20Datasources/_Supported%20Datasources%20Introduction.htm [6.9.2021]

[388] https://www.securonix.com/solutions/cloud-security/ [6.9.2021]

[389] https://documentation.securonix.com/onlinedoc/Content/Connectors/Content/Datasource%20Deployment%20Guides/PDF%20Deployment%20Guides/Old%20Datasource%20Guides/SNYPR%206.2%20Deployment%20Guide%20SAP_WHE%20ERP.pdf [6.9.2021]

Vorratsdatenspeicherung. Securonix wertet diese Daten in Echtzeit aus, betont aber, dass für den Vergleich mit vergangenen Verhaltensweisen der betroffenen Beschäftigten und ihrer KollegInnen „historische" Daten entscheidend sind. Zur automatisierten Erkennung von verdächtigen Verhaltensmustern müssten bestimmte Verhaltensweisen zuvor mindestens zehn Mal aufgezeichnet worden sein – unabhängig davon ob dies innerhalb von zehn Tagen oder zehn Wochen geschehe.[390] Am anderer Stelle werden alle Befürchtungen von DatenschützerInnen bestätigt. Es wird begeistert darauf hingewiesen, dass die von Securonix genutzten Formate der Speicherung von Daten auch für künftige „Analysetechniken oder Technologien" geeignet seien, denn schließlich wisse „niemand genau, wofür die heute aufgezeichneten Daten in Zukunft genutzt werden" könnten.[391]

Securonix hat ähnlich wie Forcepoint **Verbindungen zum US-Geheimdienstsektor**. Im siebenköpfigen Vorstand des Unternehmens sitzen ein ehemaliger Direktor sowie ein ehemaliger stellvertretender Direktor des US-Geheimdiensts NSA.[392] Ein wichtiger Referenzkunde ist Booz Allen[393], ein führender Dienstleister für Militär und Geheimdienste in den USA und ehemaliger Arbeitgeber von Edward Snowden.[394]

Datenschutz? Im System von Securonix können die in der Benutzeroberfläche angezeigten Namen, IP-Adressen und andere personenbezogene Daten „maskiert" und durch Pseudonyme ersetzt werden. Der Unternehmen bezeichnet dies fälschlicherweise als „Anonymisierung", was nichts daran ändert, dass im Hintergrund weiterhin exzessiv personenbezogene Daten verarbeitet werden. Die Maskierung kann jederzeit durch einen definierten Ablauf, der immerhin protokolliert wird, aufgehoben werden.[395] Welche Datenquellen verwendet werden, welche Verhaltensweisen überwacht werden und wie sich diese auf die Risikobewertungen auswirken, kann angepasst, eingeschränkt oder erweitert werden.[396] Ob diese Vorkehrungen ausreichen, um einen Einsatz von Securonix in Österreich und Deutschland zu rechtfertigen, der den Anforderungen von DSGVO und Arbeitsrecht genügt, kann hier nicht abschließend beurteilt werden.

Einsatz in Deutschland. Securonix bewirbt seine Produkte mindestens seit 2014 für den deutschsprachige Raum[397], auf der Website ist ein Büro in Deutschland angeführt[398] und laut LinkedIn existiert die Rolle eines Verkaufsdirektors für den DACH-Raum.[399] Die einzige Kundin aus dem deutschsprachigen Raum, zu der es öffentlich verfügbare Informationen gibt, ist UniCredit Services Deutschland, die IT-Dienste und Backoffice für UniCredit Deutschland

[390] S. 7: https://documentation.securonix.com/onlinedoc/Content/Cloud/Content/SNYPR%206.3/Cloud/PDF%20Guides/6.3.1%20Cloud_Analytics%20Guide.pdf

[391] „No one knows exactly how the data we are gather today will be used in the future, but by storing data in an OEF (the widely adopted standard), organizations can confidently control and use their data, no matter the analytical technique or technology that may come along" https://documentation.securonix.com/onlinedoc/Content/Cloud/Content/Content%20Guides/Data%20Dictionary/Open%20Event%20Format%20Introduction.htm

[392] https://www.securonix.com/team-members/#board-of-directors [25.3.2021]

[393] https://www.securonix.com/press-release/securonix-powers-booz-allens-new-cloud-based-siem-as-a-service/ [25.3.2021]

[394] Vgl. https://en.wikipedia.org/wiki/Booz_Allen_Hamilton

[395] https://documentation.securonix.com/onlinedoc/Content/On-Prem/Content/SNYPR%206.3/On-Prem/Security%20Analyst%20Guide/6.3%20Privacy%20Settings%20for%20GDPR.htm [6.9.2021]

[396] https://documentation.securonix.com/onlinedoc/Content/Cloud/Content/SNYPR%206.3/Cloud/PDF%20Guides/6.3.1%20Cloud_Analytics%20Guide.pdf [6.9.2021]

[397] https://softprom.com/sites/default/files/materials/IT-ilovepdf-compressed.pdf [25.3.2021]

[398] https://www.securonix.com/contact-us/ [25.3.2021]

[399] https://www.linkedin.com/in/hagen-reiche-57747814/ [6.9.2021]

alias Hypovereinsbank abwickelt.[400] Laut Betriebsrat gibt es seit 2019 eine arbeitsgerichtliche Auseinandersetzung um den Einsatz von Securonix bei UniCredit Services Deutschland.[401]

Bekannte Technologiekonzerne wie IBM und Microsoft bieten Produkte an, die ähnliche Funktionen wie die Systeme von Forcepoint und Securonix zur Verfügung stellen. Die UEBA-Funktionen von QRadar, der SIEM-Lösung von IBM[402], berechnen ebenso auf Basis von umfassenden Verhaltensdaten Risiko-Scores für gesamte Belegschaften. Beschäftigte, die sich ungewöhnlich oder verdächtig verhalten und darum als mögliche Bedrohung für den Betrieb identifiziert werden, können unter spezielle Beobachtung gestellt werden.[403]

Microsoft vermarktet eine Vielfalt an Produkten im Bereich von IT-Sicherheit und Risikoanalyse. Das SIEM-System Azure Sentinel[404] bietet umfassende UEBA-Funktionen[405]. Für die wegen ihrer Aktivitäten und Verhaltensweisen als „riskant" bewerteten ArbeitnehmerInnen schlägt Microsoft vor, näher zu untersuchen, ob es sich dabei etwa um einen „verärgerte[n] Mitarbeiter" handeln könnte, der „bei einer Beförderung gerade übergangen wurde".[406] Microsoft-Produkte zur Gewährleistung von „communication compliance" und gegen Bedrohungen durch „Insider" überwachen Aktivitäten und Kommunikationsvorgänge, um Betrug, Datendiebstahl, Interessenkonflikte, Belästigung und Gewalt am Arbeitsplatz und andere Verletzungen von Unternehmensregeln zu entdecken.[407] Die eDiscovery-Lösung für Microsoft 365 ermöglicht die Durchsuchung von E-Mails, Dokumenten, Chats und anderen Datentypen und wird von Microsoft damit beworben, dass sie zum Beispiel für die Auswertung betrieblicher Daten im Rahmen von Rechtsstreitigkeiten mit Beschäftigten genutzt werden könne.[408]

[400] https://www.unicreditgroup.eu/en/worldwide/our-worldwide-presence/europe/germany/unicredit-services-s-c-p-a---zweigniederlas.html, https://en.wikipedia.org/wiki/HypoVereinsbank
[401] https://muenchen.verdi.de/branchen/finanzdienstleistungen/bg-ubis/++co++2698f7bc-2b0c-11ea-b275-001a4a160100 [23.3.2021]
[402] https://www.ibm.com/at-de/products/qradar-siem [7.9.2021]
[403] https://www.ibm.com/at-de/products/qradar-user-behavior-analytics [7.9.2021]
[404] https://docs.microsoft.com/en-us/azure/sentinel/ [7.9.2021]
[405] https://docs.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics [7.9.2021]
[406] https://docs.microsoft.com/de-de/cloud-app-security/tutorial-ueba [7.9.2021]
[407] https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-solution-overview?view=o365-worldwide [7.9.2021]
[408] https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-legal-investigations?view=o365-worldwide [13.7.2021]

6.5 Ortung von Beschäftigten mit Bewegungsmeldern und WLAN-Daten

Folgende Abschnitte beschreiben zwei Systeme, die Anwesenheit, Standorte und Bewegungen von Beschäftigten in Innenräumen mit invasiven Methoden erfassen – vorrangig zur Analyse und Optimierung der Nutzung von Büroräumlichkeiten im Rahmen der Gebäudeverwaltung (siehe auch Abschnitt 5.5.2).

6.5.1 Bewegungsmelder zur Überwachung von Anwesenheit an Arbeitsplätzen

An einem Montag im Januar 2016 entdeckte die Belegschaft der britischen Zeitung „Daily Telegraph" kleine Boxen unter den Schreibtischen. Es stellte sich heraus, dass es sich dabei um Bewegungsmelder handelte. Nach einem Medienbericht erklärte das Management der Belegschaft, dass die über das Wochenende ohne Ankündigung installierten Sensoren für vier Wochen unter den Tischen verbleiben würden, um zur Verbesserung der „Energieeffizienz" der Büroräumlichkeiten die Nutzung von Arbeitsplätzen durch Beschäftigte zu untersuchen. Nach anhaltender Kritik wurden die Sensoren entfernt.[409] Ähnliches passierte bei der britischen Bank Barkleys.[410]

Das in beiden Fällen eingesetzte System **OccupEye** kann laut Hersteller sowohl für Analyse der Nutzung ganzer Bürogebäude, Stockwerke oder Abteilungen verwendet werden als für die Auswertung der Nutzung individueller Arbeitsplätze – sowohl in Echtzeit als auch über längere Zeiträume hinweg.[411] Die Sensorboxen können unter Tischen, an Wänden, an der Decke oder unter Sesseln montiert werden[412] und enthalten neben einem Infrarot-Bewegungsmelder auch Sensoren zur Messung von Raumtemperatur, Luftqualität, Luftdruck, Geräuschpegel, Lichtintensität und Feuchtigkeit.[413] Über eine Weboberfläche können verschiedene Auswertungen über die Belegung von Schreibtischen bis auf die Ebene von Einzelarbeitsplätzen eingesehen werden, wie folgende Abbildung zeigt:[414]

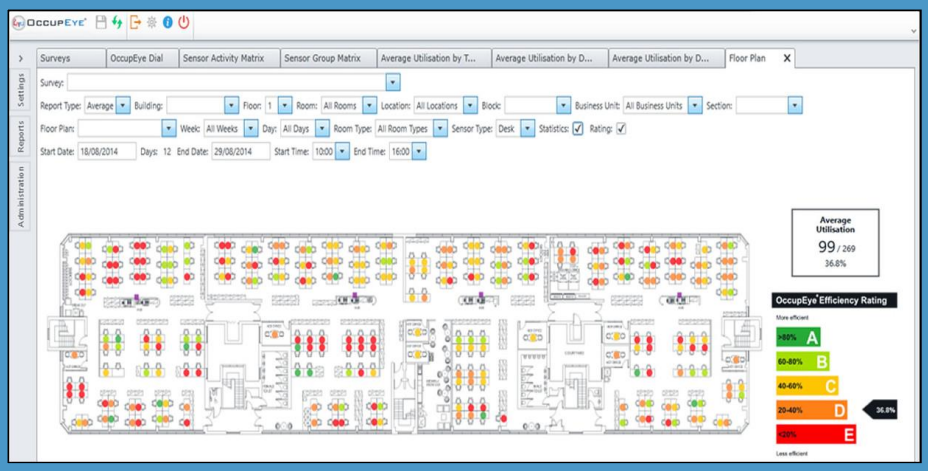


Abbildung 16: Ausschnitt Bedienoberfläche OccupEye. Quelle: Hersteller

[409] Quinn, Ben; Jackson, Jasper (2016): Daily Telegraph to withdraw devices monitoring time at desk after criticism. The Guardian, 11.01.2016. Online: https://www.theguardian.com/media/2016/jan/11/daily-telegraph-to-withdraw-devices-monitoring-time-at-desk-after-criticism

[410] Morris, Stephen; Griffin, Donal; Gower, Patrick (2017): Barclays Puts in Sensors to See Which Bankers Are at Their Desks. Bloomberg, 18.08.2017. Online: https://www.bloomberg.com/news/articles/2017-08-18/barclays-puts-in-sensors-to-see-which-bankers-are-at-their-desks

[411] "With OccupEye, a single unit can be used to monitor individual desk utilisation and defined staff workspace, as well as larger areas such as meeting rooms … True 1:1 continual space utilisation analysis, over any period of time", https://www.occupeye.com/how-it-works/ [21.10.2020]

[412] Ebd.

[413] https://www.occupeye.com/wp-content/uploads/2018/09/SmartView-by-OccupEye_OE-06_18.pdf [21.10.2020]

[414] Abbildung © OccupEye. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle: https://www.occupeye.com/how-it-works/ [21.10.2020]

Als Zweck des Systems werden vom Hersteller neben dem Potenzial zur Senkung der Energiekosten vor allem mögliche Kosteneinsparungen durch effizientere Raumnutzung oder die Reduktion von Büroflächen hervorgehoben.[415] Dies wird als "Workplace Analytics" bezeichnet.[416] Darüber hinaus wird eine Variante angeboten, die die Belegung bzw. Verfügbarkeit von flexiblen Arbeitsplätzen und Besprechungsräumen in Echtzeit anzeigt.[417]

OccupEye wird von einer Tochter der Firma fm:systems betrieben, einem Anbieter von „digitalen Arbeitsplatzlösungen" und von technischen Systemen für die Gebäudeverwaltung. Laut Eigenangabe hat die Firma 250.000 Sensoren für 1.400 Kunden in 80 Ländern installiert, u.a. bei Banken, Universitäten und bei der Hälfte der 50 größten US-Unternehmen. Auch BMW wird als Kundin angeführt.[418] Eine Auswertung über die Rückkehr aus dem Homeoffice an den Arbeitsplatz während der Corona-Krise legt nahe, dass fm:systems Zugriff auf Daten über die Büronutzung in mehreren europäischen Ländern inklusive Deutschland hat.[419]

6.5.2 Ortung von Beschäftigten in Innenräumen mit WLAN-Daten

Auch der global führende Netzwerktechnologie-Konzern Cisco bietet in Partnerschaft mit fm:systems[420] ein Produkt für „Workplace Analytics" zur Vermessung der Belegung und Nutzung von Büroräumlichkeiten an.[421] Das System von Cisco ermöglicht die Ortung von Beschäftigten in Innenräumen durch die Ortung von Laptops, Tablets und Smartphones mit Hilfe von WLAN-Daten. Die WLAN-Router, die die Räumlichkeiten mit einem drahtlosen Internetzugang versorgen, dienen als Ortungsgeräte. Folgende Abbildung zeigt einen Ausschnitt aus der Verwaltungssoftware von Cisco. In den grün eingefärbten Büroflächen können Laptops und Smartphones mit einer Genauigkeit von sieben Metern geortet werden, in den rot eingefärbten Flächen ist die WLAN-Abdeckung zu niedrig:[422]

Abbildung 17: Ortung mit WLAN-Daten durch Cisco. Quelle: Hersteller

[415] https://www.occupeye.com/what-is-occupeye/, https://www.occupeye.com/costs-calculator/ [21.10.2020]
[416] https://www.occupeye.com/wp-content/uploads/2018/09/SmartView-by-OccupEye_OE-06_18.pdf [21.10.2020]
[417] https://www.occupeye.com/live-space-finder/ [21.10.2020]
[418] https://fmsystems.com/ [21.10.2020]
[419] https://fmsystems.com/our-resources/covid-19-coronavirus/space-data-visualization/ [30.9.2021]
[420] Cisco's Angebot ist eine Integration mit „Rifiniti", das wie OccupEye zu fm.systems gehört, siehe: https://fmsystems.com/news/verdantix-fmsystems-is-rebranding-its-product-offerings-as-a-digital-workplace-solutions-suite/ [21.10.2020]
[421] https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_cisco_workplace_analytics_design_and_implementation_guide.html [21.10.2020]
[422] Abbildung © Cisco. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_cisco_workplace_analytics_design_and_implementation_guide.html [21.10.2020]

Die Dokumentation enthält keine Hinweise darüber, ob eine Zuordnung der zu ortenden Laptops, Tablets und Smartphones zu spezifischen ArbeitnehmerInnen mittels Kennungen erfolgt. Das System erkenne jedenfalls mit Hilfe von künstlicher Intelligenz, welche Geräte zu einzelnen Beschäftigten gehören und welches davon ihr „Primärgerät" sei. Damit werden zumindest pseudonymisierte personenbezogene Daten verarbeitet. Darüber hinaus können viele andere Datenquellen einbezogen werden. Dazu zählen neben den im vorigen Abschnitt beschriebenen Bewegungsmeldern von OccupEye etwa Daten aus der Zutrittskontrolle und über Anmeldungen in Besprechungsräumen mittels Chipkarte sowie Kalenderdaten über Einladungen zu Besprechungen aus Microsoft Exchange, Office 365 oder Google Calendar.[423]

Das Angebot basiert auf dem Produkt „Connected Mobile Experiences" (CMX) von Cisco, das nicht nur als System zur Erstellung von Bewegungsprofilen am Arbeitsplatz vermarket wird, sondern auch der Analyse von Bewegungsdaten von VerbraucherInnen in Innenräumen auf Basis von WLAN-Daten dient.[424]

[423] https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_cisco_workplace_analytics_design_and_implementation_guide.html [21.10.2020]
[424] https://developer.cisco.com/site/cmx-mobility-services/, https://blogs.cisco.com/networking/introducing-cisco-cmx-engage [21.10.2021]

6.6 „People Analytics" mit den tragbaren Geräten von „Humanyze"

Humanyze, eine US-Firma mit Niederlassung in Amsterdam, analysiert den Arbeitsalltag von Beschäftigten auf Basis von Verhaltensdaten, die von tragbaren Geräten und anderen betrieblichen Systemen erfasst werden.[425] Über das Unternehmen wird seit Jahren medial berichtet. Trotz des oft kritischen Tons[426] dürften die Berichte die Bekanntheit von Humanyze erheblich gesteigert haben. Man könnte fast meinen, das Spiel mit dem „Grusel" der Totalüberwachung gehöre zur Marketingstrategie – auch wenn der euphemistische Firmenname anderes nahelegt.

Humanyze vermarket seit über zehn Jahren ein kleines Gerät mit Sensoren, das am Körper getragen wird – ähnlich einer intelligenten Zutrittskarte.[427] Es zeichnet **Sprache, soziale Interaktionen und Körperbewegungen** auf – mittels Mikrofon, Infrarot-Sensor, Akzelerometer[428] und Bluetooth-Sensor (vgl. Kayhan 2018). Andererseits bietet das Unternehmen Software an, die Verhaltensweisen und „Interaktionen" – also zwischenmenschliche Kommunikationsvorgänge – am Arbeitsplatz auswertet und daraus Kennzahlen berechnet.[429] Wie aus untenstehenden Darstellungen der Firma ersichtlich gehören zu den möglichen Datenquellen neben den tragbaren Geräten von Humanyze viele Systeme von Drittherstellern wie Microsoft, SAP, Workday oder Salesforce sowie Kommunikations- und Kollaborationssysteme von Slack bis Zoom. Neben einem sogenannten „Organizational Health Score", der laut Humanyze die „Effektivität" einer Organisation misst[430], werden Kennzahlen für „Leistung", „Engagement" und „Anpassungsfähigkeit" der Belegschaft berechnet:[431]

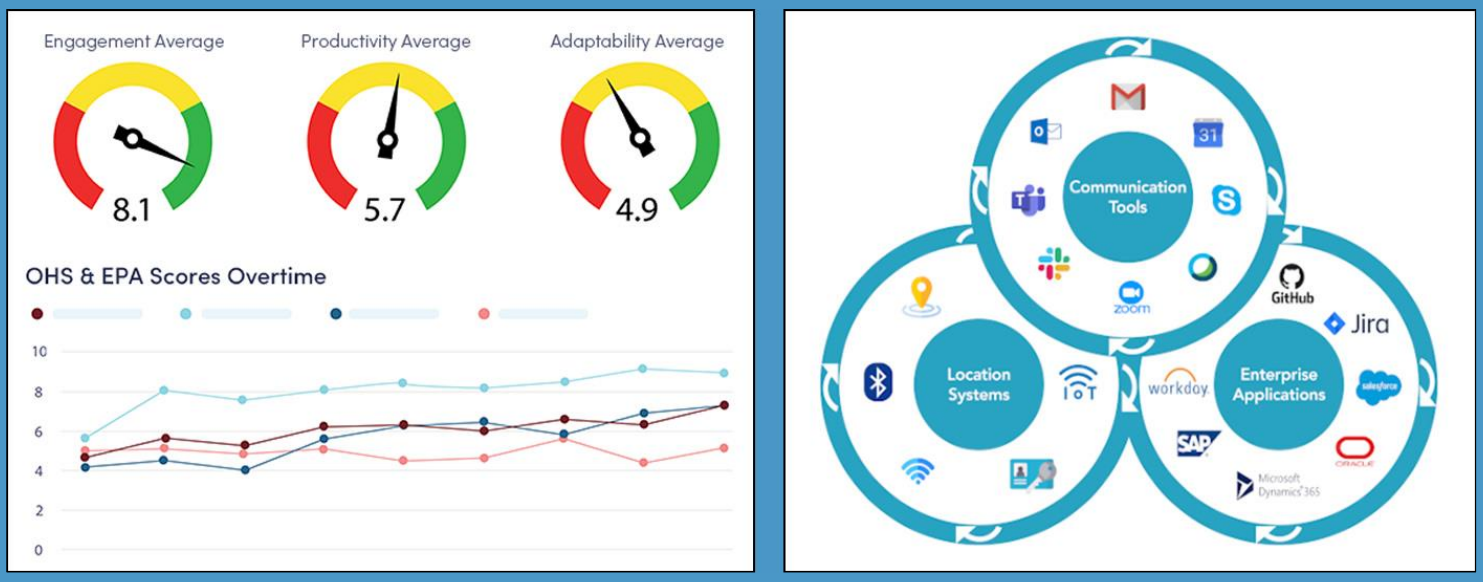


Abbildung 18: Darstellungen von Scores und Datenquellen bei Humanyze. Quelle: Hersteller

[425] https://humanyze.com/europeanheadquartersamsterdam/ 29.1.2021]

[426] Vgl. z.B. The Economist (2018): There will be little privacy in the workplace of the future, 28.3.2018. Online: https://www.economist.com/special-report/2018/03/28/there-will-be-little-privacy-in-the-workplace-of-the-future

[427] Miller, Ron (2015): New Firm Combines Wearables And Data To Improve Decision Making. TechCrunch, 24.2.2015. Online: https://techcrunch.com/2015/02/24/new-firm-combines-wearables-and-data-to-improve-decision-making/

[428] Beschleunigungssensor, der körperliche Bewegungen messen kann, vgl. https://de.wikipedia.org/wiki/Beschleunigungssensor

[429] https://humanyze.com/product-release-organizational-health-score/ [29.1.2021]

[430] Ebd.

[431] Abbildungen © Humanyze. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quellen: https://humanyze.com/wp-content/uploads/2020/12/Web-Banner-Continuously_v2.png [18.2.2021], https://www.humanyze.com/wp-content/uploads/datasourcegraphic-3-e1588371610289-2.png [26.9.2020]

6.6.1 Bewertung von Zufriedenheit, Zusammenarbeit, Charakter, Kreativität und Leistung

Humanyze betont immer wieder die Herkunft des Unternehmens aus dem renommierten MIT Media Lab und verweist auf mehrere wissenschaftliche Studien, die den Nutzen der Technologie belegen sollen. Folgende Tabelle zeigt, welche Sensoren und Datentypen des sogenannten „Sociometric Badge" – also des von Humanyze vermarkteten tragbaren Geräts – in Studien für welche Arten der Auswertung genutzt worden sind. Bis auf eine wurden alle diese Studien unter Beteiligung von Mitgründern des Unternehmens durchgeführt (Tabelle nach Kayhan 2018):

Genutzte Datentypen und Sensoren	Art der Auswertung
Physische Aktivität (Akzelerometer), Sprechen (Mikrofon)	Zusammenarbeit in Teams
Persönliche Interaktionen (Infrarot-Sensor), Nähe zwischen Personen (Bluetooth-Sensor), physische Aktivität (Akzelerometer), Sprechen (Mikrofon)	Zufriedenheit mit Interaktionen und Produktivität
Persönliche Interaktionen (Infrarot-Sensor), Nähe zwischen Personen (Bluetooth-Sensor), Tonlage beim Sprechen (Mikrofon)	Netzwerk-Kohäsion und Produktivität
Persönliche Interaktionen (Infrarot-Sensor), Nähe zwischen Personen (Bluetooth-Sensor), physische Aktivität (Akzelerometer), Sprechen (Mikrofon)	Charaktereigenschaften und Gruppen-Leistung
Persönliche Interaktionen (Infrarot-Sensor), Nähe zwischen Personen (Bluetooth-Sensor), physische Aktivität (Akzelerometer), Sprechen (Mikrofon)	Job-Zufriedenheit und Gruppen-Interaktionen
Physische Aktivität (Akzelerometer), Sprechen (Mikrofon)	Gruppen-Leistung
Persönliche Interaktionen (Infrarot-Sensor), Nähe zwischen Personen (Bluetooth-Sensor)	Einstellung zum Job und Leistung
Persönliche Interaktionen (Infrarot-Sensor), Nähe zwischen Personen (Bluetooth-Sensor)	Kreativität
Persönliche Interaktionen (Infrarot-Sensor), Nähe zwischen Personen (Bluetooth-Sensor)	Arbeitsplatzgestaltung

Tabelle 3: Auswertungen auf Basis von Daten des Geräts von Humanyze. Quelle: Kayhan 2018

Das Gerät zeichnet mit dem eingebauten Mikrofon unter anderem auf, wie ArbeitnehmerInnen miteinander sprechen. Das Unternehmen versichert, man würde dabei nicht auswerten, worüber die Leute sprechen – aber etwa wieviel sie sprechen, wie oft sie andere unterbrechen oder wie laut sie sprechen. Mittels **Stimmanalyse** könne man zum Beispiel bewerten, ob jemand gestresst sei.[432] Große Unterschiede in der Lautstärke der Stimme würden auf soziale Unverträglichkeit schließen lassen (Olguin 2009), bestimmte Tonfälle auf Enthusiasmus und Motivation (Wu 2008). Auch der Grad des Einflusses, den eine Person auf eine andere Person ausübt, soll mit der Analyse von Sprache vermessen werden können.

Mit dem Infrarot-Sensor, der die Nähe zwischen Personen misst, werden direkte **Interaktionen zwischen Personen** analysiert, die sich mit weniger als einem Meter Abstand einander zuwenden. Die Daten des Akzelerometers sollen über die **physische Aktivität** Auskunft geben und etwa erkennen, ob eine Person sitzt oder geht (ebd.). Der Bluetooth-Sensor vermisst allgemeiner, **wer sich wo bewegt** und dabei wem wie oft begegnet. Auf Basis der Daten von Infrarot- und Bluetooth-Sensor wurden beispielsweise die sozialen Netzwerke zwischen ArbeitnehmerInnen analysiert, unter Einbeziehung unterschiedlicher Sensordaten Korrelationen zwischen Verhaltensweisen und allen möglichen Aspekten von Charaktereigenschaften bis Arbeitsleistung (Olguín 2009, Wu 2008).

[432] Kane, Gerald C. (2015): 'People Analytics' Through Super-Charged ID Badges, MIT Sloan Review, 7.4.2015. Online: https://sloanreview.mit.edu/article/people-analytics-through-super-charged-id-badges/

Aussagekraft? Die Studien legen zum Teil offen, dass die entdeckten Korrelationen schwach sind (Olguin 2009). Eine Studie ohne Beteiligung des Unternehmens hat schon bei der Art der Erfassung der Sensordaten signifikante Probleme gefunden. So waren etwa die internen Uhren der Geräte nicht synchron und wichen im Schnitt um rund drei Minuten voneinander ab (Kayhan 2018). Allein das macht eigentlich jede sinnvolle Auswertung von sozialen Interaktionen hinfällig. Auch darüber hinaus darf die Aussagekraft und Sinnhaftigkeit derartiger Auswertungen für Unternehmen bezweifelt werden. Über die Funktionsweise und Zuverlässigkeit der von Humanyze aktuell eingesetzten Software, die neben Daten von tragbaren Geräten auch verschiedene andere Datenquellen nutzt, um Kennzahlen über Unternehmen und deren Beschäftigte zu berechnen, ist jedoch wenig bekannt.

In jedem Fall greift die permanente Erfassung und Auswertung von Verhaltensdaten tief in die Autonomie von ArbeitnehmerInnen ein. Auch wenn, wie Humanyze betont, immer nur aggregierte Auswertungen durchgeführt werden, tragen solche Angebote dazu bei, permanente Überwachung zu normalisieren.

Humanyze legt nahe, hauptsächlich im Bereich höherqualifizierter Wissensarbeit tätig zu sein[433] und gibt an, Daten über 210 Millionen Arbeitstage von ArbeitnehmerInnen verarbeitet zu haben.[434] Es wird hervorgehoben, dass die Software auf dem „global größten Datenset für Verhaltensweisen am Arbeitsplatz“ beruhen würde. Darum ist anzunehmen, dass die erfassten Daten auch über Unternehmen hinweg genutzt werden.[435]

[433] https://humanyze.com/category/case-study/ [29.1.2021]
[434] https://humanyze.com/ [29.1.2021]
[435] https://humanyze.com/product-release-organizational-health-score/ [29.1.2021]

6.7 Körper- und Verhaltensdaten für Arbeitssicherheit und -gesundheit

Folgende Abschnitte beschreiben Systeme, die versprechen, die Sicherheit und Gesundheit von ArbeitnehmerInnen mit Hilfe invasiver Erfassung von Körper- und Verhaltensdaten zu verbessern (siehe auch Abschnitt 5.6.2).

6.7.1 Vermessung körperlicher Arbeit für Gesundheitszwecke

Das Gerät „Reflex" der Firma Kinetic wird am Gürtel getragen und verspricht, durch die Erkennung gesundheitsschädlicher Bewegungen wie zum Beispiel **falschem Bücken oder exzessiver Drehungen** das Verletzungsrisiko von ArbeiterInnen in Logistikzentren oder Fabriken zu senken. Es warnt bei falschen Bewegungen mit Vibrationen und sendet Daten an einen Cloud-Dienst. Wie folgende Abbildung zeigt, können Vorgesetzte Auswertungen über „Hochrisiko-Bewegungen" einsehen – für das gesamte Unternehmen, für Gruppen und für Einzelpersonen:[436]

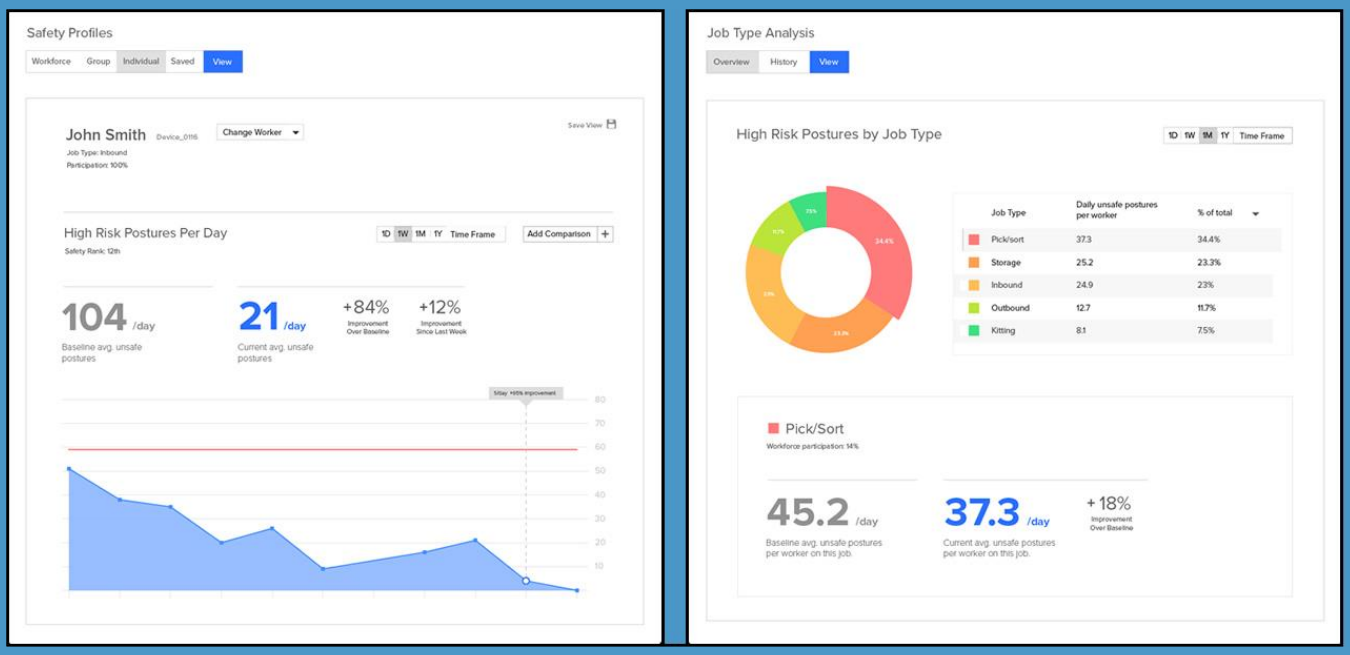


Abbildung 19: Auswertungen „hochriskanter" Bewegungen bei Kinetic. Quelle: Hersteller

Die Auswertungen zeigen unter anderem die tägliche Anzahl der „Hochrisiko-Bewegungen" von Einzelpersonen über lange Zeiträume hinweg und sind laut Kinetic für „personalisiertes Coaching" gedacht.[437] Darüber hinaus bietet das System Spielmechaniken mit persönlichen Zielen, Belohnungen und Ranglisten, um „Gewohnheiten" und „Verhaltensweisen" zu „verändern". Kinetic verspricht eine Senkung von Fehltagen und der Kosten für arbeitsbedingte Verletzungen sowie eine Erhöhung der Produktivität.[438] Auch wenn die Verbesserung der Arbeitsgesundheit ein hehres Ziel ist, greift das System durch die permanente Erfassung und Bewertung von Bewegungen tief in die Autonomie von ArbeitnehmerInnen ein. Seit 2020 bietet Kinetic an, das gleiche tragbare Gerät auch zur Erfassung von Begegnungen für das „Contact Tracing" im Rahmen der Pandemiebekämpfung einzusetzen.[439]

[436] Abbildungen © Kinetic. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle: https://www.wearkinetic.com/kinetic-dashboard/ [14.2.2021]
[437] Ebd.
[438] https://www.wearkinetic.com/injury-reduction/ [14.2.2021]
[439] https://www.wearkinetic.com/contact-tracing/ [14.2.2021]

Der australische Hersteller dorsaVi bietet ein ähnliches Produkt an, sowohl für den Einsatz im Bereich Gesundheit, Rehabilitation und Sport als auch für die Arbeitswelt.[440] Dabei werden zwei Geräte getragen – etwa an Schulter und Rücken. Bilder von Videokameras können in die Auswertung mit einbezogen werden.[441] Die Firma verspricht, „anspruchsvolle" Körperhaltungen, repetitive Bewegungen sowie die Muskelaktivität von Belegschaften zu vermessen, um Arbeitssicherheit und -gesundheit zu verbessern, betont aber auch das Ziel der Erhöhung der Produktivität der ArbeitnehmerInnen.[442] Die Beschreibung legt nahe, dass das System nur temporär eingesetzt wird.[443]

6.7.2 Totalüberwachung für Sicherheit und Gesundheit mit „IBM Worker Insights"

IBM bietet mit „IoT Worker Insights" ein System an, das mit Hilfe von tragbaren Geräten und Sensoren am Körper dabei helfen soll, die Arbeitssicherheit und -gesundheit bei manuellen Tätigkeiten auf Baustellen oder in der Industrie zu verbessern sowie die Einhaltung von Sicherheitsregeln am Arbeitsplatz sicherzustellen.[444] Die Beschäftigten nutzen eine Smartphone-App, bei der sie sich zu Schichtbeginn anmelden. Sie werden dazu aufgefordert, die am Körper zu tragenden vernetzten Sensorgeräte anzulegen und einzuschalten. Wie folgende Abbildung (Mitte) zeigt, kann es sich dabei etwa um einen Helm, Schuhe, ein Armband und ein am Gürtel getragenes Gerät handeln:[445]

Abbildung 20: IBM-Arbeitsplatzsicherheit, Bedienoberflächen Führungskräfte und Beschäftigte. Quelle: Hersteller

Auf Schritt und Tritt. Die am Körper getragenen Geräte können mit einer Vielzahl an Sensoren bestückt sein, die ähnlich wie zeitgenössische Smartphones oder Fitness-Armbänder laufend Bewegungen und Lage des Geräts, Körperdaten wie die Herzfrequenz sowie andere Informationen über die Umgebung wie Temperatur, Feuchtigkeit, Luftdruck, Geräusche und Beleuchtung erfassen.[446] Das System von IBM erkennt in Folge unterschiedliche als sicherheitsrelevant eingestufte Überschreitungen von Grenzwerten, Vorfälle oder Verhaltensweisen. Dies reicht von der Erkennung von Stürzen, Unfällen, schlechter Luftqualität oder zu großer Hitze über das Ablegen von Sicher-

[440] https://www.dorsavi.com/uk/en/ [14.2.2021]
[441] https://www.dorsavi.com/uk/en/wp-content/uploads/sites/3/2020/12/dorsaVi-ViSafe-Fact-Sheet-US-A764.A.pdf [14.2.2021]
[442] https://www.dorsavi.com/uk/en/visafe/ [14.2.2021]
[443] https://www.dorsavi.com/uk/en/wp-content/uploads/sites/3/2020/12/dorsaVi-ViSafe-Fact-Sheet-US-A764.A.pdf [14.2.2021]
[444] IBM hat den Produktnamen inzwischen von „IoT Worker Insights" auf „Maximo Worker Insights" geändert: https://www.ibm.com/support/pages/iot-worker-insight-demonstration, https://www.ibm.com/docs/en/mwi?topic=product-overview [11.7.2021]
[445] Alle Abbildungen (c) IBM. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle links Standbild Video bei Minute 6:58, Mitte bei Minute 4:18, rechts bei Minute 4:37: https://www.youtube.com/watch?v=rV16qJGSVLY [11.7.2021]
[446] https://github.com/IBM/worker-insights, https://www.ti.com/tool/TIDC-CC2650STK-SENSORTAG [11.7.2021]

heitsausrüstung oder dem Betreten nicht erlaubter Areale bis zu Warnungen bei zu hoher Herzfrequenz, Dehydrierung, Bewegungslosigkeit. Überanstrengung oder Übermüdung.[447] Die Erkennung diese Vorfälle erfolgt mit Hilfe der KI-Plattform IBM Watson, die vom Betrieb an die eigenen Bedürfnisse angepasst werden kann.[448]

ArbeitnehmerInnen erhalten bei Vorfällen visuelle und akustische Hinweise und Warnungen und können bei Bedarf außerdem einen Panikknopf betätigen.[449] Nach der Anmeldung in der App sollen die Beschäftigten angeben, **wie viele Stunden sie geschlafen haben** und wie sie die Schlafqualität in der vergangenen Nacht einschätzen – wie in Abbildung 20 (rechts) ersichtlich. Führungskräfte haben Zugriff auf eine „Live"-Kartenansicht und sehen Statistiken über erkannte Vorfälle wie Stürze, Zutritte zu unzulässigen Arealen oder zu hoher Herzfrequenz im Zeitverlauf – wie Abbildung 20 (links) zeigt. Erkennt das System zu viele Vorfälle, kann etwa der Grenzwert für die Erkennung einer zu hohen Herzfrequenz hinaufgesetzt werden – wie das IBM-Demonstrationsvideo zeigt.[450]

Voneinander getrennt betrachtet ist der Einsatz einzelner Funktionen des Systems bei bestimmten Arbeitstätigkeiten sicherlich sinnvoll. Auch die Summe der Funktionen mag bei gefährlichen Arbeitstätigkeiten in gefährlichen Umgebungen in Einzelfällen gerechtfertigt sein, beinhaltet aber eine sehr weitgehende Überwachung von Körperdaten und Verhaltensweisen über den gesamten Arbeitstag hinweg und führt damit zu einer umfassenden digitalen Verhaltenskontrolle. Dies birgt ein hohes Missbrauchspotenzial. Generell stellt sich die Frage, wie zuverlässig körperliche Zustände wie Übermüdung oder Überanstrengung auf Basis von Körperdaten eingeschätzt werden können. Dass Beschäftigte sogar Informationen über Schlafdauer und -qualität angeben sollen, ist höchst fragwürdig. Damit geht die Verhaltenskontrolle über die Erfassung von Daten über die Arbeitszeit hinaus. Es stellt sich nicht zuletzt die Frage, ob Beschäftigte wirklich freiwillig angeben, dass sie kurz oder schlecht geschlafen haben.

[447] Min 2:16: https://www.youtube.com/watch?v=rV16qJGSVLY, https://www.ibm.com/docs/en/mwi?topic=shields-currently-available [11.7.2021]
[448] https://github.com/IBM/worker-insights [11.7.2021]
[449] Ebd.
[450] Min 9:27: https://www.youtube.com/watch?v=KxbGNrDvSPA [11.7.2021]

6.7.3 "Müdigkeitsmanagement" mit Daten über Tippverhalten und Mausbewegungen

Die Software „Performetric" wertet Daten über Tippverhalten und Mausbewegungen aus und verspricht, daraus laufend Kennzahlen über den Grad der mentalen Müdigkeit von Callcenter-MitarbeiterInnen zu berechnen. Der portugiesische Hersteller vermarket das ursprünglich für den eSport-Bereich – also für das professionelle Computerspiel – entwickelte System als „Software für mentales Müdigkeitsmanagement".[451] Eine in einem Produktvideo dargestellte Auswertung zeigt, wie der berechnete Müdigkeitsgrad ins Verhältnis mit Callcenter-Leistungskennzahlen wie der Zahl der abgearbeiteten Telefonate und deren durchschnittliche Länge gesetzt wird:[452]

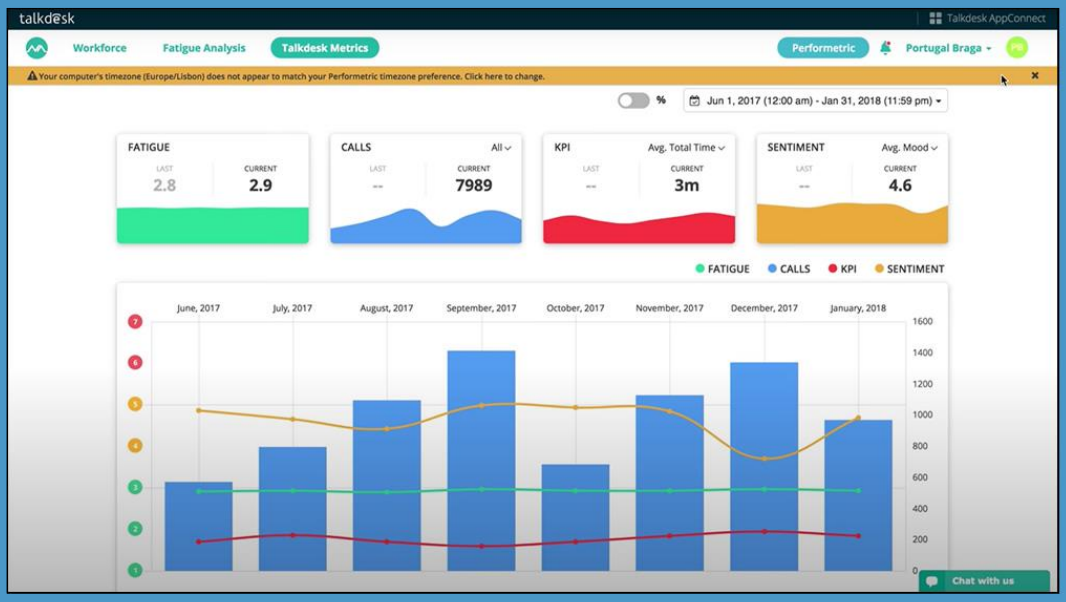


Abbildung 21: Auswertung des Müdigkeitsgrads von Beschäftigten bei Performetric. Quelle: Hersteller

Auswertungen können für die gesamte Belegschaft, für Teams oder Einzelpersonen durchgeführt werden.[453] ArbeitnehmerInnen können die Müdigkeitseinschätzungen selbst einsehen und bekommen Benachrichtigungen. Dies soll dabei helfen, „Burnout" zu vermeiden und „Leistung und mentale Gesundheit" zu verbessern. Laut Hersteller wird zur Berechnung des Müdigkeitsgrads für jede Person ein individuelles Profil erstellt. Gleichzeitig wird in irreführender Art und Weise behauptet, das System würde „keine privaten Nutzerdaten sammeln" und die Privatsphäre nicht beeinträchtigen.[454] Generell könne das Produkt das „Wohlbefinden" der Belegschaft steigern und dabei helfen, Schichten und Pausen besser zu planen. Performetric erlaubt laut Eigenangabe auch, Produktivität und Leistung mit mentaler Müdigkeit zu „korrelieren", um schlussendlich die Produktivität zu erhöhen und die Kosten zu senken.[455]

Durch die laufende Auswertung von Daten über Tippverhalten und Mausbewegungen greift das System tief in die Autonomie von ArbeitnehmerInnen ein, während völlig unklar bleibt, wie valide die Auswertungen überhaupt sind.

[451] https://performetric.gg/product [14.1.2021]
[452] Standbild aus Video © Performetrics. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle Video bei Minute 2:20: https://www.youtube.com/watch?v=ZIBswCs9MQM [14.1.2021]
[453] Ebd., Minute 1:16 und Minute 1:25
[454] https://performetric.gg/product [14.1.2021]
[455] https://performetric.gg/for-talkdesk [14.1.2021]

6.8 Automatisierte Routenplanung und Fuhrparkverwaltung

Folgende Abschnitte beschreiben ein System für das automatisierte Management von Zustellfahrten und Routenplanung sowie ein System eines österreichischen Anbieters für Fuhrparkverwaltung (siehe auch Abschnitt 5.3.8).

6.8.1 Automatisiertes Management von Zustellung mit Routenplanung

Routific ist eine von einem kanadischen Unternehmen angebotene cloudbasiertes Software, mit dem Betriebe die pünktliche Auslieferung von Essen oder Paketen steuern können. Das System verspricht, die Routen von ZustellerInnen nach Bedarf automatisiert zu „optimieren" und damit die Kosten pro Zustellung um „bis zu 40%" zu senken. Die ZustellerInnen nutzen eine Smartphone-App, die ihren Arbeitsalltag – von der Vorgabe von Routen über Navigation bis zum Nachweis der Auslieferung durch Unterschriften und Fotos – komplett organisiert und außerdem ihren Standort via GPS erfasst.[456] Die Standortdaten werden genutzt, um VerbraucherInnen über den Zeitpunkt der Zustellung zu informieren, können aber auch in einer Live-Ansicht dargestellt werden.[457] Folgende Abbildung zeigt die Bedienoberfläche für die Steuerung des Systems und eine Auswertung, in der Vorgesetzte Details über pünktliche, verspätete und nicht erfolgte Auslieferungen von ZustellerInnen einsehen können:[458]

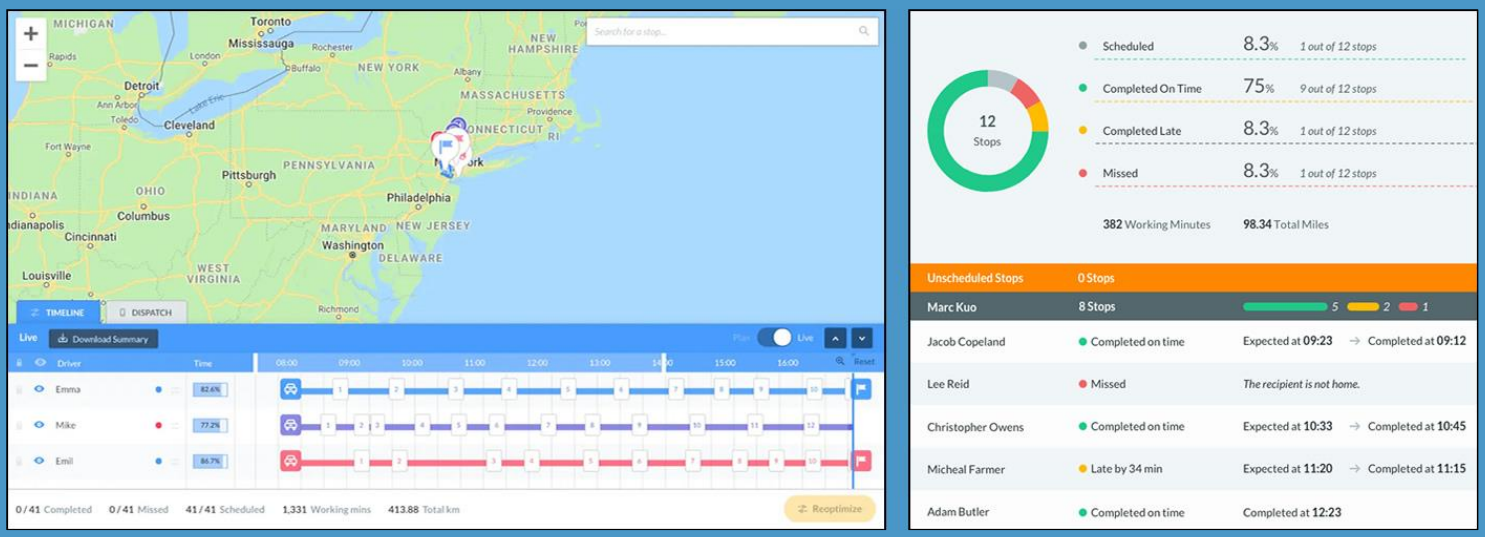


Abbildung 22: Automatisierte Routenplanung und Auswertungen bei Routific. Quelle: Hersteller

Das System berechnet auf der Grundlage von Zustelladressen und -zeitfenstern, Fahrzeugkapazitäten sowie den Schichtplänen der ZustellerInnen samt geplanter Pausen genaue Vorgaben für die anzufahrenden Adressen und Zeitpunkte. Die Routenplanung kann manuell geändert, aber auch in Echtzeit immer wieder neu optimiert werden.[459] Außerdem werden **Vorgabewerte für die Fahrgeschwindigkeit** einbezogen. Diese kann von Führungskräften für einzelne ZustellerInnen von „langsam" (z.B. nur 10% der „normalen" Geschwindigkeit) über normal (100%) bis „schnell" (bis zu 190% der „normalen" Geschwindigkeit) eingestellt werden kann. Die Möglichkeit,

[456] https://routific.com/ [14.2.2021]
[457] https://academy.routific.com/en/articles/1317924-live-tracking [14.2.2021]
[458] Abbildungen © Routific. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quellen: https://routific.com/ [14.2.2021], https://academy.routific.com/en/articles/1317937-driver-analytics-and-delivery-performance-reports [14.2.2021]
[459] https://routific.com/delivery-route-planner/ [14.2.2021]

Geschwindigkeitsvorgaben auf bis zu 190% hochschrauben zu könne, wird damit argumentiert, dass die vom externen Navigationsanbieter berechneten Durchschnittsgeschwindigkeiten oft „unterhalb der gesetzlich erlaubten Maximalgeschwindigkeit“ liegen würde.[460]

Auch die pro Auslieferung vor Ort zur Verfügung stehende Zeitdauer kann eingestellt werden.[461] Diverse Optionen für „flexible Schichten“, „zulässige Überzeiten“ und für die Minimierung der benötigten ArbeitnehmerInnen pro Schicht ermöglichen den Unternehmen Flexibilität und Kostenminimierung.[462] Das System stellt unterschiedliche Auswertungen zur Verfügung, die Kennzahlen über die Auslieferungstätigkeit sowie Details über Einzelpersonen darstellen, quantifizieren und vergleichen – und die sich damit potenziell für eine weitreichende Leistungskontrolle eignen. Die Leistungskontrolle erfolgt jedoch alleine schon durch die Vorgabe der Zustelladressen und -zeitpunkte samt Echtzeit-Rückmeldung an diejenigen Beschäftigten, die Arbeitstätigkeiten langsamer durchführen als geplant.

Datenverarbeitung für mehrere Zwecke und automatisierte Kontrolle von Arbeitstätigkeiten. Routific ist ein Musterbeispiel für ein System, das Tätigkeiten von ArbeitnehmerInnen engmaschig und automatisiert steuert und kontrolliert. Die Erfassung und Auswertung von Daten über Arbeitsschritte und Standorte dient dabei mehreren Zwecken gleichzeitig – von der Sicherstellung der pünktlichen Auslieferung und der Rückmeldung an die KundInnen bis zur Kontrolle der ArbeitnehmerInnen, der Maximierung der Arbeitsintensität und der Kostenoptimierung.

6.8.2 Fuhrparkverwaltung mit GPS-Tracking und Fahrzeugdaten

Der österreichische Anbieter Easytrack, der die Fuhrparkverwaltungs-Systeme des internationalen Herstellers Arvento vertreibt, die laut Eigenangabe global 860.000 Fahrzeuge überwachen[463], erfasst GPS-Standortdaten, Motor-Leerläufe, plötzliche Beschleunigungen/Bremsungen, gefahrene Routen, Arbeitszeiten und andere Informationen.[464] Vorgesetzte können E-Mail-Benachrichtigungen bekommen, wenn ein Beschäftigter zu schnell fährt[465], den Motor zu lange im Stand laufen lässt[466], das Fahrzeug außerplanmäßig stoppt[467] oder einen definierten Bereich verlässt („Geofencing“).[468] Als Zwecke der Datenverarbeitung betont Easytrack u.a. Ökologie und Sicherheit.

Manche Daten über Fahrten müssen gesetzlich verpflichtend aufgezeichnet werden, etwa die Lenk- und Ruhezeiten bei LKW-FahrerInnen[469] oder als Fahrtenbuch für das Finanzamt.[470] Eine rechtliche Einschätzung ist jenseits des Rahmens dieser Studie (siehe z.B. Haslinger et al 2020, S. 57ff). Die angebotenen Funktionen gehen jedenfalls sehr weit. Zudem wird betont, man könne das Gerät im Fahrzeug „gut versteckt verbauen“.[471] Easytrack wird für Branchen wie Transport, Bau, Handwerk oder Gesundheitswesen beworben und laut Eigenangabe von vielen österreichischen Firmen eingesetzt – darunter Conrad Electronic, Samariterbund Wien und Securitas.[472]

[460] https://academy.routific.com/en/articles/1317968-driver-driving-speed [14.2.2021]
[461] https://academy.routific.com/en/articles/1317975-project-settings [14.2.2021]
[462] https://docs.routific.com/v1.5.0/docs/api-reference [14.2.2021]
[463] https://www.easytrack.at/arvento-mobile-systems/ [3.6.2021]
[464] https://www.easytrack.at/fuhrparkmanagement/ [3.6.2021]
[465] Ebd.
[466] https://www.easytrack.at/green-driving/ [3.6.2021]
[467] https://www.easytrack.at/safe-driving/ [3.6.3021]
[468] https://www.easytrack.at/fragen-und-antworten-gps-ortung/ [3.6.2021]
[469] https://www.easytrack.at/tachograph/ [3.6.2021]
[470] https://www.easytrack.at/elektronisches-fahrtenbuch-3/ [3.6.2021]
[471] https://www.easytrack.at/fragen-und-antworten-gps-ortung/ [3.6.2021]
[472] https://www.easytrack.at/referenzen-und-partner/ [3.6.2021]

6.9 Überwachung von Socialmedia-Aktivitäten von Beschäftigten

Wie folgende Abschnitte zeigen, bieten international mehrere Unternehmen Produkte zur Auswertung von Socialmedia-Aktivitäten von Beschäftigten an – vor Neueinstellungen, aber auch für bestehendes Personal.

6.9.1 Auswertung für Qualifikationsprofile und zur Vorhersage von Kündigungsabsichten

Die US-Firma HiQ Labs bietet seit einigen Jahren Produkte an, die öffentlich zugängliche personenbezogene Profildaten automatisiert aus Socialmedia-Plattformen wie LinkedIn abruft und dazu zu nutzen, um Auswertungen über ArbeitnehmerInnen durchzuführen – etwa über Kündigungswahrscheinlichkeiten und Qualifikationen. Folgende Abbildung zeigt ein Beschäftigtenprofil mit **Scores für das Kündigungsrisiko** und anderen „Risikofaktoren“:[473]

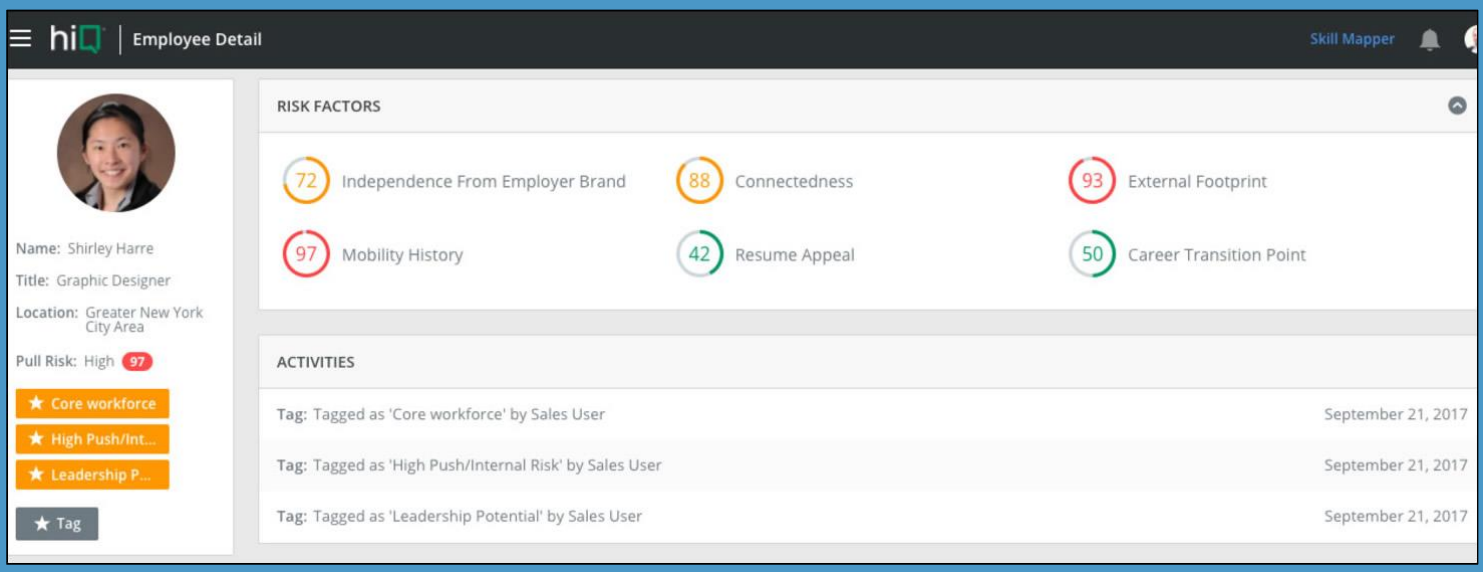


Abbildung 23: Profil mit Scores und Risikobewertungen für eine Arbeitnehmerin bei HiQ. Quelle: Hersteller

In einer Broschüre[474] werden einige dieser „Risikofaktoren“ näher beschrieben. Ausgewertet werden etwa der Grad der Identifikation mit der Marke des Arbeitgebers, der Grad der „Vernetzung“ sowie der externe digitale „Fußabdruck“ im Sinne der öffentlichen Sichtbarkeit durch Online-Aktivitäten. Öffentlich einsehbare Socialmedia-Profile werden im Hinblick darauf bewertet, wie attraktiv sie für andere Unternehmen wirken. Außerdem wird die Job-Mobilität ausgewertet – also vergangene Jobwechsel sowie Rollenwechsel innerhalb von Firmen.

Es ist anzunehmen, dass HiQ Labs in diese Auswertungen vorwiegend oder ausschließlich **Daten von LinkedIn** einbezieht – einer Socialmedia-Plattform, die zu Microsoft gehört und hauptsächlich auf berufliche Nutzung abzielt. HiQ Labs befindet sich wegen des automatisierten Abrufs von LinkedIn-Profildaten („Scraping“) seit 2016 in einem mehrjährigen Rechtsstreit mit LinkedIn.[475] HiQ Labs konnte zuletzt leider rechtlich durchsetzen, dass LinkedIn das

[473] Abbildung © hiQ Labs. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Quelle: https://www.hiqlabs.com/new-index [14.01.2021]
[474] https://static1.squarespace.com/static/5803b57737c581885cbd0667/t/5a638a5e71c10be0a05eb0ea/1516473156462/AMLL.hiQLabs.pdf [14.1.2021]
[475] Vgl. Keenan, James: What the HiQ vs. LinkedIn Case Means for Automated Web Scraping. CPO Magazine, 26.12.2019. Online: https://www.cpomagazine.com/data-privacy/what-the-hiq-vs-linkedin-case-means-for-automated-web-scraping/

automatisierte Abrufen von Profildaten in den USA nicht behindern darf, möchte den Fall aber vor den obersten Gerichtshof bringen.[476]

Die statistischen Modelle für die Auswertungen basieren laut HiQ Labs auf Trainingsdaten über „hunderttausende" ArbeitnehmerInnen aus unterschiedlichen Branchen.[477] Da zur Entwicklung derartiger statistischer Modelle die öffentlich zugänglichen Informationen mit Daten zur Kündigungswahrscheinlichkeit aus den Betrieben abgeglichen werden müssen, nutzt HiQ Labs offensichtlich Daten über Betriebe hinweg. Ein anderes Produkt des Unternehmens extrahiert aus öffentlich zugänglichen Daten Informationen über die „Skills" von ArbeitnehmerInnen und erstellt daraus **Qualifikationsprofile** von Belegschaften – für Personaleinsatzplanung, Talentmanagement und die ökonomische Bewertung ganzer Belegschaften bei Firmenübernahmen.[478]

6.9.2 Erkennung von Betrug, Sicherheitsbedrohungen, Mobbing und Streiks

Die US-Firma Pegasus Knowledge Solutions verkauft Datenanalyse-Software mit einem Schwerpunkt auf Personalverwaltung und bietet ebenfalls an, Personaldaten aus verschiedenen Quellen mit **externen Daten** zu integrieren, um einen „360 Grad Blick" auf Beschäftigte zu ermöglichen.[479] Neben der Analyse von Qualifikationen, Engagement, Kündigungswahrscheinlichkeiten und der Erkennung von Betrug durch ArbeitnehmerInnen wird angeboten, die Stimmungslage in der Belegschaft auszuwerten („Sentiment Analysis").[480] Als Alternative zu Umfragen wird die Einbeziehung von Socialmedia-Daten von Plattformen wie Facebook, Twitter, LinkedIn oder Glassdoor beworben.[481] [482] Darüber hinaus wird vorgeschlagen, Socialmedia-Daten zur Prognose von Kündigungen einzusetzen.[483]

Das US-Datenanalyseunternehmen Social Sentinel wertet nach eigenen Angaben „in Echtzeit" und automatisiert „Milliarden an Konversationen" auf populären Socialmedia-Plattformen aus[484], um Sicherheitsbedrohungen und psychische Krisen zu erkennen, und zwar sowohl für Schulen als auch für Arbeitgeber.[485] Einbezogen werden unter anderem Postings auf Facebook und Instagram.[486] Die Angebote für Arbeitgeber reichen von der Erkennung von Sicherheitsbedrohungen, sexueller Belästigung und Mobbing über die Analyse der Stimmungslage in der Belegschaft bis zum Schutz der Reputation des Unternehmens.[487] Social Sentinel wurde kürzlich von Navigate360 übernommen, einer US-Firma, deren Sicherheitslösungen nach eigenen Angaben von 6500 Schulen, 5000 Polizeibehörden und 4400 Unternehmen eingesetzt wird.[488]

International bieten viele Firmen an, vor einer Neueinstellung teil- oder vollautomatisiert die Socialmedia-Aktivitäten von BewerberInnen zu überprüfen. Manche davon bieten auch an, laufend die Socialmedia-Aktivitäten des

[476] Errick, Kirsten (2020): LinkedIn Petitions CFAA Data Scraping Case to Supreme Court. Law Street, 15.3.2020. Online: https://lawstreetmedia.com/tech/linkedin-petitions-cfaa-data-scraping-case-to-supreme-court/
[477] https://static1.squarespace.com/static/5803b57737c581885cbd0667/t/59c44d5ee5dd5bcfde0dc232/1506037087308/predictive_accuracy.pdf [14.1.2021]
[478] https://www.hiqlabs.com/new-index [14.1.2021]
[479] https://www.pksi.com/products/awa/ [14.1.2021]
[480] https://www.pksi.com/wp-content/uploads/Advanced-Workforce-Analytics-Overview.pdf [14.1.2021]
[481] Ebd.
[482] https://www.pksi.com/third-party-data-for-workforce-analytics/ [14.1.2021]
[483] Ebd.
[484] https://www.socialsentinel.com/our-solution/ [14.1.2021]
[485] https://navigate360.com/social-sentinel-joins-navigate360/ [14.1.2021]
[486] https://www.socialsentinel.com/legal-social-media-partners/ [14.1.2021]
[487] https://www.socialsentinel.com/industries/corporate/ [14.1.2021]
[488] https://navigate360.com/company/ [14.1.2021]

bestehenden Personals zu beobachten. Das US-Unternehmen Social Intelligence stellt etwa automatisiert umfassende Reports über die Socialmedia-Aktivitäten einer Person zusammen und bewertet sie in Hinblick auf rassistische oder sexistische Aussagen, sexuell explizite Kommunikation, Gewaltdrohungen oder „potenziell illegale Aktivitäten". Die Reports können für Hintergrund-Überprüfungen vor Neueinstellungen genutzt werden, aber auch für bestehendes Personal. Als Rechtfertigung dient unter anderem das Schlagwort „Compliance".[489] Auch Fama, wiederrum eine US-Firma, bietet automatisiertes Socialmedia-Screening von BewerberInnen[490] sowie die laufende Beobachtung von „Risiken in der Belegschaft" an.[491] Dabei wird eine Art von Profiling durchgeführt, bei der die Socialmedia-Kommunikation anhand vieler negativer wie auch positiver Merkmale bewertet wird.[492]

Auch einige Firmen, die „Social Media Monitoring" für Marketingzwecke und Unternehmenskommunikation anbieten, bewerben ihre Produkte ebenso als Werkzeug zur Beobachtung von ArbeitnehmerInnen.[493]

Unternehmen wie das in Wien beheimatete Startup Prewave bieten an, auf Basis von Socialmedia-Daten **Streiks und andere „Risiken" für die Lieferkette** vorherzusagen (Grill und Steiner 2018). Auch in diesem Fall werden wie bei allen oben beschriebenen Produkten nach eigenen Angaben ausschließlich öffentlich zugängliche Informationen ausgewertet.

Es ist davon auszugehen, dass Unternehmen oft noch viel weiter gehen. Wie 2020 bekannt wurde, hat der globale Konzern Amazon etwa **„private" Facebook-Diskussionsgruppen infiltriert** und teilautomatisiert ausgewertet, in denen sich ArbeitnehmerInnen aus den USA, Spanien und Großbritannien organisiert haben (Gurley und Cox 2020).

[489] https://www.socialintel.com/solutions/how-it-works/ [10.2.2021]
[490] https://fama.io/about-fama-screening-technologies/ [10.2.2021]
[491] https://fama.io/product/ [10.2.2021]
[492] http://www.reactivecanvas.com/project.php?project=1 [10.2.2021]
[493] Siehe z.B. https://awario.com/blog/how-to-use-social-listening-for-hr/ [10.2.2021], http://snaptrends.com/upcoming-webinar-using-social-media-secure-employees-assets-bottom-line/ [10.2.2021]

7. Fallstudien über Systeme in konkreten Betrieben

Die beiden Fallbeispiele in diesem Kapitel dokumentieren den Einsatz datenverarbeitender System in zwei konkreten Unternehmen – auf Basis existierender Literatur und öffentlich zugänglicher interner Dokumente.

7.1 Algorithmische Kontrolle in Amazon-Verteilzentren

Der Onlinehandels- und Plattform-Gigant Amazon hat laut Eigenangabe seinen Personalstand von 800.000 Beschäftigten Ende 2019 auf 1,3 Millionen Ende 2020 gesteigert – exklusive Leih- und Saisonarbeit.[494] Mit Stand Mai 2021 betreibt der Konzern laut einem Marktforschungsunternehmen 238 große Logistik- und Paketverteilzentren in den USA, 29 in Deutschland und 3 in Österreich. Inklusive kleinerer Sortier- und Auslieferungsstationen werden global über 1500 Standorte betrieben.[495] In den USA beschäftigt Amazon rund 22% aller ArbeitnehmerInnen im Sektor privater Warenlager und Verteilzentren – wiederrum exklusive Saisonarbeitskräfte.[496]

Seit Jahren wird darüber berichtet, dass es mit den Arbeitsbedingungen in diesen Logistik- und Verteilzentren in vielen Ländern nicht unbedingt zum Besten steht. Die Bandbreite reicht von Kündigungen von schwangeren Arbeitnehmerinnen[497] oder bei Kritik[498] über kurzfristige und unverlässliche Schichteinteilung[499], hohe körperliche Belastung und Arbeitsintensität[500], Plastikflaschen als Toilettenersatz und extreme Sicherheitsmaßnahmen[501] bis zu gefährlichen Arbeitsbedingungen[502] und hohen Verletzungsraten (vgl. Evens 2019). Auch ein ehemaliger Mitarbeiter im Verteilzentrum in Niederösterreich hat 2019 von Überwachung, erniedrigenden Vorschriften und Disziplinierungsmaßnahmen, hohen Leistungsvorgaben, gefährliche Arbeitsbedingungen sowie unsicheren Beschäftigungsverhältnissen über eine Leiharbeitsfirma berichtet[503] – die Gewerkschaft wurde aktiv.[504]

7.1.1 Automatisierte Kündigungen wegen zu geringer Produktivität?

2019 wurde bekannt, dass in einem US-Amazon-Verteilzentrum mit 2.500 Beschäftigten im Jahr bis September 2018 an die 300 ArbeitnehmerInnen dezidiert wegen zu geringer „Produktivität“ gekündigt wurden – und das zum Teil automatisiert. Dies sind über 10% der Belegschaft in einem Jahr. Amazon selbst hat diese Kündigungen in

[494] https://s2.q4cdn.com/299287126/files/doc_financials/2020/q4/Amazon-Q4-2020-Earnings-Release.pdf
[495] MWPVL (2021): Amazon Global Supply Chain and Fulfillment Center Network. Online: https://www.mwpvl.com/html/amazon_com.html [17.5.2021]
[496] International Brotherhood of Teamsters, Communications Workers of America, United Food and Commercial Workers International Union, Service Employees International Union, Change to Win (2020): Petition for the Investigation of Amazon.com, Inc., S. 15, 27.2.2020. Online: http://www.changetowin.org/wp-content/uploads/2020/02/Petition-for-Investigation-of-Amazon.pdf
[497] Ng, Alfred; Rubin, Ben Fox (2019): Amazon fired these 7 pregnant workers. Then came the lawsuits. CNET, 6.5.2019. Online: https://www.cnet.com/features/amazon-fired-these-7-pregnant-workers-then-came-the-lawsuits/
[498] Picchi, Aimee (2019): Amazon accused of firing warehouse worker who criticized "robot"-like treatment. CBS News, 21.3.2019. Online: https://www.cbsnews.com/news/amazon-accused-of-firing-warehouse-worker-who-criticized-robot-like-treatment/
[499] Burin, Margaret (2019): ‘They resent the fact I’m not a robot’. ABC News, 26.2.2019. Online: https://www.abc.net.au/news/2019-02-27/amazon-australia-warehouse-working-conditions/10807308?nw=0
[500] Selby, Alan (2017): Timed toilet breaks, impossible targets and workers falling asleep on feet: Brutal life working in Amazon warehouse. Mirror, 25.11.2017. Online: https://www.mirror.co.uk/news/uk-news/timed-toilet-breaks-impossible-targets-11587888
[501] Pollard, Chris (2018): Rushed Amazon warehouse staff pee into bottles as they’re afraid of ‘time-wasting’. The Sun, 15.4.2018. Online: https://www.thesun.co.uk/news/6055021/rushed-amazon-warehouse-staff-time-wasting/
[502] Sainato, Michael (2019): 'Go back to work': outcry over deaths on Amazon's warehouse floor. The Guardian, 18.10.2019. Online: https://www.theguardian.com/technology/2019/oct/17/amazon-warehouse-worker-deaths
[503] Bruckner, Regina (2019): Amazon-Mitarbeiter prangert harsche Bedingungen in Austro-Niederlassung an. Standard, 12.6.2019. Online: https://www.derstandard.at/story/2000104750084/amazon-mitarbeiter-prangert-bedingungen-in-grossebersdorf-an
[504] ÖGB (2019): Skandal bei Amazon-Österreich. Online: https://www.oegb.at/themen/soziale-gerechtigkeit/steuern-und-konjunktur/skandal-bei-amazon-oesterreich

Dokumenten detailliert beschrieben, die im Zuge einer arbeitsrechtlichen Auseinandersetzung mit einem ehemaligen Mitarbeiter erstellt wurden. Der Konzern betont in den Dokumenten, man habe den von der arbeitsrechtlichen Auseinandersetzung betroffenen Mitarbeiter nicht etwa wegen „gesetzlich geschützter Aktivitäten" gekündigt, sondern ausschließlich wegen mangelhafter Produktivität – und dokumentiert dazu akribisch, wie oft dies in besagtem Verteilzentrum vorkomme. Laut Amazon sei ein System im Einsatz, das die „individuellen Produktivitätsraten" jedes Beschäftigten überwache und bei zu geringen Werten „ohne Zutun einer Führungskraft automatisiert Verwarnungen oder Kündigungen" erzeuge. Führungskräfte könnten allerdings bei Bedarf eingreifen (Lecher 2019).

In Österreich hat die Futurezone darüber berichtet. Amazon hat nichts davon dementiert und folgendes festgehalten: „Wie alle Unternehmen haben auch wir Erwartungen hinsichtlich der Leistung unserer Mitarbeiter - dies allerdings ausschließlich mit Blick auf die operative Planbarkeit der Einhaltung der Kundenversprechen. Bei uns werden Produktivitätsrichtwerte nach objektiven Gesichtspunkten festgelegt und über längere Zeiträume evaluiert. Hierbei wird insbesondere auch die durchschnittliche Leistung der Belegschaft selbst berücksichtigt."[505] Amazon betont also, man würde bei der Festlegung der „Produktivitätsrichtwerte" insbesondere die „durchschnittliche Leistung der Belegschaft" berücksichtigen. Würde der Konzern nun jährlich 10% der Belegschaft wegen zu geringer Leistung kündigen, würde diese Durchschnittsleistung und damit die Leistungsvorgaben klarerweise immer weiter ansteigen.

7.1.2 Sekundengenaue Steuerung und Kontrolle von Arbeit

Beschäftigte, die in den Verteilzentren von Amazon Produkte bearbeiten, werden nicht nur auf Schritt und Tritt überwacht, sondern arbeiten unter kleinteiliger Anleitung und Kontrolle durch IT-Systeme (vgl. Staab und Nachtwey 2016). Sie erfüllen unterschiedliche Rollen – von sogenannten „Receivern", die die von Händlern und Herstellern zugelieferte Produkte in Kisten sortieren, über „Stower", die Waren in Regale einsortieren, „Picker", die bestellte Produkte aus den Regalen holen bis zu „Packern", die Pakete für den Versand zusammenstellen.[506] Je nach Verteilzentrum nimmt der Grad der Robotisierung zu. Die von den Beschäftigten zurückzulegenden Wegstrecken reduzieren sich und verlagern sich auf stationäre Tätigkeiten (Del Ray 2019). Bei den verbleibenden Beschäftigten wird praktisch jeder Arbeitsschritt vorgegeben und vermessen.

Menschliche Roboter. Daten über einzelne Arbeitsschritte werden hauptsächlich durch die tragbaren Geräte erfasst, mit denen jedes bearbeitete Produkt gescannt wird, aber auch durch Knöpfe, mit denen auf stationären Arbeitsplätzen etwa eine volle Kiste signalisiert wird (ebd.). Eine Journalistin, die aus Recherchegründen in einem US-Verteilzentrum gearbeitet hat, vergleicht die Handscanner mit einem „digitalen Manager", der auf dem Display nach jedem Tätigkeitsschritt eine neue Arbeitsanweisung erteile und gleichzeitig die verbleibenden Sekunden herunterzähle, die für den nächsten Handgriff vorgesehen sind (Guendelsberger 2019). Diese auf dem Display herunterzählende „Time zu Pick" wird oft beschrieben und abgebildet – von Kanada[507] bis Großbritannien.[508]

[505] Futurezone (2019): Computer entscheidet bei Amazon, wer rausgeschmissen wird, 26.4.2019. Online: https://futurezone.at/digital-life/computer-entscheidet-bei-amazon-wer-rausgeschmissen-wird/400477054

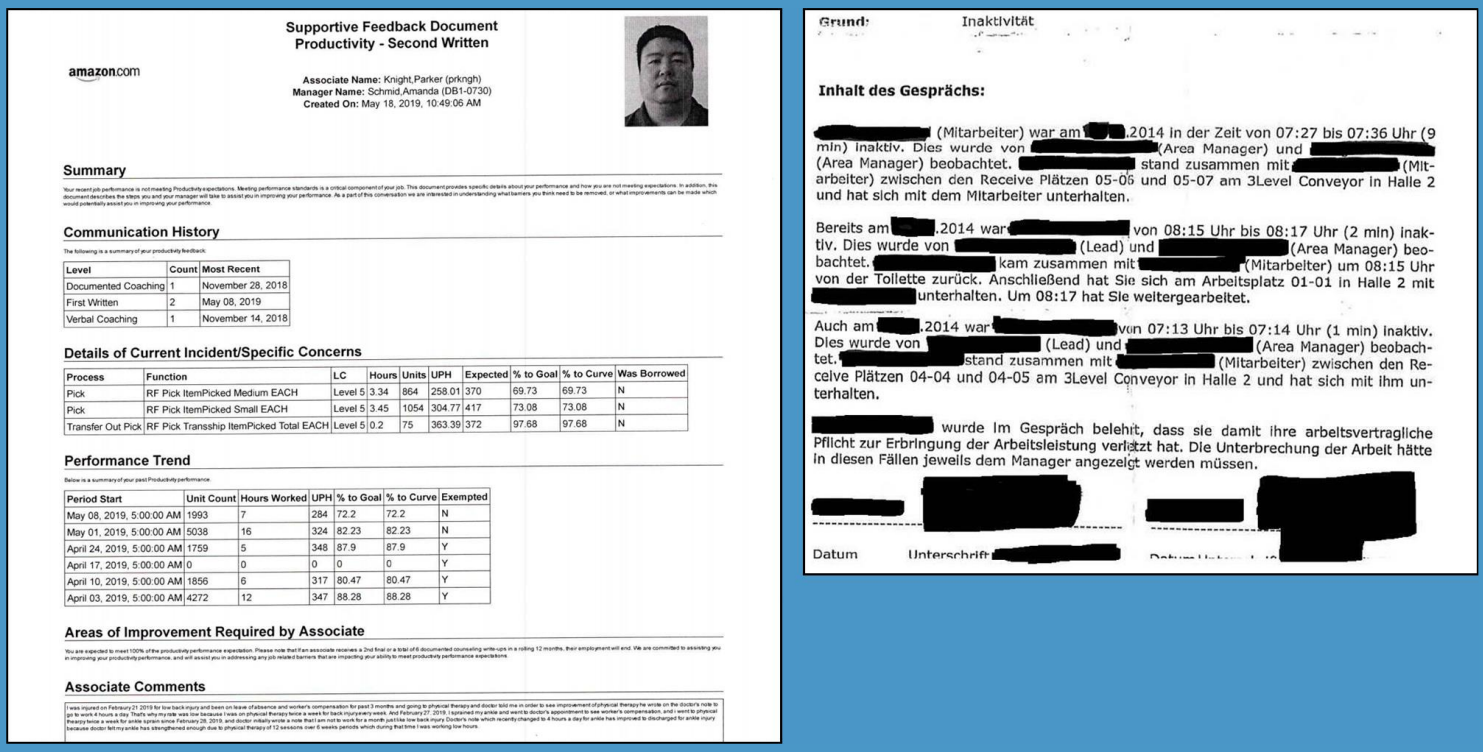
[506] Vgl. Fan 2020 sowie: Melchior, Laura (2015): Ein Blick hinter die Amazon-Kulissen. com! Professional, 19.10.2015. Online: https://www.com-magazin.de/news/amazon/blick-amazon-kulissen-1034456.html

[507] Thompson, Mitchell (2020): Amazon warehouse workers in Canada pushed into dangerous race against time. Ricochet, 16.11.2020. Online: https://ricochet.media/en/3372/amazon-warehouse-workers-in-canada-pushed-into-dangerous-race-against-time

[508] Kelly, Lorraine (2016): Amazombies: Seven seconds to find an item, every move filmed and blistering 12-hours shifts with timed toilet breaks. Daily Mail, 3.12.2016. Online: https://www.dailymail.co.uk/news/article-3997864/Amazombies-Seven-seconds-item-filmed-blistering-12-hours-shifts-timed-toilet-breaks-Christmas-order-does-worker-elves.html

Sekundengenauer Takt. Ein ehemaliger „Picker“ in den USA beschreibt die Rolle von Kennzahlen wie die bearbeiteten Produkte pro Stunde und die „Taktrate“ in Sekunden pro Produkt. Zu Beginn habe seine Vorgabe bei 350 Produkten pro Stunde und 7 Sekunden pro Produkt gelegen. Er habe anfangs nur 250 Produkte pro Stunde und 11 Sekunden geschafft, später dann 400 Produkte pro Stunde bei 8 Sekunden pro Produkt. Bei zu niedriger Taktrate wäre eine Benachrichtigung auf dem Bildschirm seiner Station erschienen. Außerdem wurde seine Position in einem Ranking aller Picker angezeigt. Anfangs habe er im Vergleich zu den anderen in der 20. bis 30. Perzentile gelegen, später in der 80. Perzentile. Außergewöhnliche Ereignisse wie besonders große, fehlende oder auf den Boden gefallene Produkte wurden nicht berücksichtigt und hätten negativen Einfluss auf seine Leistungswerte gehabt. Während ihn zwar niemand davon abgehalten habe, außerhalb der vorgesehen 30minütigen Pausen auf die Toilette zu gehen, habe das natürlich ebenfalls desaströse Auswirkungen auf seine Leistungswerte gehabt (Fan 2020).

Kleinteilige Vorgabe und Kontrolle von Arbeitsleistung. Werden die Leistungsvorgaben nicht erfüllt, erhalten US-Amazon-Beschäftigte Verwarnungen, die detaillierte Berichte über ihre Produktivität enthalten (Evens 2019). Folgende Abbildung (links) zeigt die zweite Verwarnung eines Arbeitnehmers namens Parker Knight, der 2019 in einem Logistikzentrum im US-Bundesstaat Oregon gearbeitet hat, wegen Nichterfüllung der Leistungsvorgaben:[509]



Supportive Feedback Document
Productivity - Second Written

amazon.com

Associate Name: Knight,Parker (prkngh)
Manager Name: Schmid,Amanda (DB1-0730)
Created On: May 18, 2019, 10:49:06 AM

Summary

Communication History

Level	Count	Most Recent
Documented Coaching	1	November 28, 2018
First Written	2	May 08, 2019
Verbal Coaching	1	November 14, 2018

Details of Current Incident/Specific Concerns

Process	Function	LC	Hours	Units	UPH	Expected	% to Goal	% to Curve	Was Borrowed
Pick	RF Pick ItemPicked Medium EACH	Level 5	3.34	864	258.01	370	69.73	69.73	N
Pick	RF Pick ItemPicked Small EACH	Level 5	3.45	1054	304.77	417	73.08	73.08	N
Transfer Out Pick	RF Pick Transship ItemPicked Total EACH	Level 5	0.2	75	363.39	372	97.68	97.68	N

Performance Trend

Period Start	Unit Count	Hours Worked	UPH	% to Goal	% to Curve	Exempted
May 08, 2019, 5:00:00 AM	1993	7	284	72.2	72.2	N
May 01, 2019, 5:00:00 AM	5038	16	324	82.23	82.23	N
April 24, 2019, 5:00:00 AM	1759	5	348	87.9	87.9	Y
April 17, 2019, 5:00:00 AM	0	0	0	0	0	Y
April 10, 2019, 5:00:00 AM	1856	6	317	80.47	80.47	Y
April 03, 2019, 5:00:00 AM	4272	12	347	88.28	88.28	Y

Areas of Improvement Required by Associate

Associate Comments

Grund: Inaktivität

Inhalt des Gesprächs:

[redacted] (Mitarbeiter) war am [redacted].2014 in der Zeit von 07:27 bis 07:36 Uhr (9 min) inaktiv. Dies wurde von [redacted] (Area Manager) und [redacted] (Area Manager) beobachtet. [redacted] stand zusammen mit [redacted] (Mitarbeiter) zwischen den Receive Plätzen 05-06 und 05-07 am 3Level Conveyor in Halle 2 und hat sich mit dem Mitarbeiter unterhalten.

Bereits am [redacted].2014 war [redacted] von 08:15 Uhr bis 08:17 Uhr (2 min) inaktiv. Dies wurde von [redacted] (Lead) und [redacted] (Area Manager) beobachtet. [redacted] kam zusammen mit [redacted] (Mitarbeiter) um 08:15 Uhr von der Toilette zurück. Anschließend hat Sie sich am Arbeitsplatz 01-01 in Halle 2 mit [redacted] unterhalten. Um 08:17 hat Sie weitergearbeitet.

Auch am [redacted].2014 war [redacted] von 07:13 Uhr bis 07:14 Uhr (1 min) inaktiv. Dies wurde von [redacted] (Lead) und [redacted] (Area Manager) beobachtet. [redacted] stand zusammen mit [redacted] (Mitarbeiter) zwischen den Receive Plätzen 04-04 und 04-05 am 3Level Conveyor in Halle 2 und hat sich mit ihm unterhalten.

[redacted] wurde im Gespräch belehrt, dass sie damit ihre arbeitsvertragliche Pflicht zur Erbringung der Arbeitsleistung verletzt hat. Die Unterbrechung der Arbeit hätte in diesen Fällen jeweils dem Manager angezeigt werden müssen.

Datum Unterschrift [redacted]

Abbildung 24: Verwarnung wegen geringer Produktivität (US), Inaktivitätsprotokoll (DE). Quellen: Reveal News / Verdi

Aus dem Dokument ist zum Beispiel ersichtlich, dass Knight am 1. Mai 2019 eine Schicht von 16 Stunden gearbeitet hat, in denen er insgesamt 5038 Produkte bewältigt hat. Mit 324 abgearbeiteten Produkten pro Stunde hat er jedoch

[509] Beide Abbildungen (c) Amazon. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken. Links eine Verwarnung eines Amazon-Beschäftigten, publiziert im Rahmen der Reportage „Behind the Smiles“ (https://revealnews.org/article/behind-the-smiles/), PDF-Dokument: https://revealnews.org/wp-content/uploads/2019/11/Parker-Knight-productivity-report.pdf, Rechts Amazon-„Inaktivitätsprotokoll“, publiziert von Verdi 2015, zugänglich z.B. via: https://www.tagesspiegel.de/wirtschaft/tarifkonflikt-beim-versandhaendler-amazon-ueberwacht-mitarbeiter-minutengenau/11499762.html
und stammen laut der Website einer Grafikagentur aus dem Handbuch „Zonar 2nd Edition“, S. 10 und S. 26. Quelle: https://www.mawide-sign.de/projekte/zalando-zonar/ [15.5.2021]

nur 82,23% der Zielvorgabe erreicht. Laut Verwarnung – die euphemistisch als „unterstützende Feedback-Dokumente“ bezeichnet werden – habe die Leistung von Knight nicht den „Produktivitätserwartungen“ entsprochen. Er müsse 100% dieser Zielvorgaben erfüllen, ansonsten werde sein Beschäftigungsverhältnis nach maximal sechs Verwarnungen automatisch enden. In einer weiteren Verwarnung – der letzten Verwarnung vor der Kündigung – wurde festgehalten, dass er „nur“ 97,9% bzw. 98,45% der Zielvorgaben erreicht habe. Einige Tage später wurde er gekündigt – formal wegen einer früheren Auseinandersetzung über einen Krankenstand. Die Unerbittlichkeit des von Amazon intern als „ADAPT“ bezeichneten Systems wird bei diesem Fall besonders deutlich, da es sich bei Parker Knight um eine bereits zuvor körperlich eingeschränkte Person handelte. Während der Beschäftigung bei Amazon war er zuerst wegen einer Rückenverletzung und dann wegen einer Verletzung des Fußgelenks in ärztlicher Behandlung. In seinem Kommentar zur finalen Verwarnung erklärt er, er wäre wohl körperlich zu eingeschränkt und zu alt, um mehr als die erreichten 98,45% der Leistungsvorgabe zu schaffen (Evens 2019, Evens 2019b).

ADAPT steht für „Associate Development and Performance Tracker“, also ein System zur Nachverfolgung von „Entwicklung und Leistung“ der Beschäftigten (Goldberg 2019). Wie die Zielvorgaben gesetzt werden, ist nicht transparent. Laut einer für einen Bericht interviewten Mitarbeiterin in einem Logistikcenter im US-Bundesstaat Minneapolis werden die zu erreichenden Leistungswerte oft überraschend geändert. Sie und andere Beschäftigte seien jede Woche besorgt, welche Rate in der nächsten Woche verlangt werden würde und ob sie diese wohl erreichen könnten (Hanley und Hubbard 2020, S. 10). Auch britische ArbeitnehmerInnen in Amazon-Logistizentren berichten von permanenten Anpassungen bzw. plötzlichen Erhöhungen der Vorgaben (Organise 2018, S. 6).

7.1.3 Überwachung unproduktiver Zeit – „Time Off Task“

Neben der detaillierten Vorgabe und Kontrolle von Leistungswerten überwacht Amazon auch die sogenannte „Time Off Task“ (kurz: „TOT“), also die Zeit, in der Beschäftigte aus Sicht des Konzerns keine produktiven Arbeitstätigkeiten verrichten.

Sobald die für die Bearbeitung eines Produkts zur Verfügung stehenden Sekunden abgelaufen sei, werde die restliche Zeit zur „Time Off Task“ gezählt – so eine kanadische Arbeitnehmerin in einem Bericht. Pro Schicht stünde eine „Time Off Task“ von insgesamt 30 Minuten zur Verfügung. Dies inkludiere aber auch Wege von Regal zu Regal. Wenn der Handscanner eine Beschäftigte etwa zum anderen Ende der Halle schicke, zähle dieser fünfminütige Weg zur „Time Off Task“. Auch wenn somit eine bestimmte Zeit für den Gang zur Toilette, das Nachfüllen der Wasserflasche oder ein Gespräch mit dem Vorgesetzten zur Verfügung stünde, erzeuge diese Kennzahl eine Atmosphäre der Angst. Manchmal würden Beschäftigte bei Überschreitung der „Time Off Task“ eine Warnung auf dem Display des Scanners erhalten – oder aber verbale oder schriftliche Verwarnungen. Diese „TOT Scores“ würden sogar in Gemeinschaftsbereichen ausgehängt, um Beschäftigte unter Druck zu setzen (PressProgress 2020). In einem US-Logistikzentrum war in einer Schicht von 11,5 Stunden neben einer 30minütigen Mittagspause eine maximale „Time Off Task“ von 18 Minuten vorgesehen. Dies inkludiere Toilettengänge, aber auch wenn jemand „langsamer gehe als es der Algorithmus diktiert“, werde „Time Off Task“ berechnet (Guendelsberger 2019).

7.1.4 Situation in Deutschland und Österreich

Deutschland. Es ist nicht im Detail bekannt, ob und wie die für die USA und mehrere andere Länder beschriebenen Praktiken in deutschen und österreichischen Amazon-Verteilzentren eingesetzt wurden bzw. werden. Es ist aber zu vermuten, dass zumindest Teile des Systems in Betrieb sind. Schon 2015 hat die deutsche Gewerkschaft Verdi sogenannte „Inaktivitätsprotokolle“ veröffentlicht, die ArbeitnehmerInnen vorgelegt wurden. Wie in Abbildung 24 (rechts) ersichtlich, wurde einer Mitarbeiterin in einem derartigen Dokument vorgeworfen, sie sei an bestimmten

Tagen im Jahr 2014 jeweils für einige Minuten „inaktiv“ gewesen – einmal „von 0:27 bis 07:36 (9min), einmal „von 8:15 bis 08:17 (2min“) und einmal „von 07:13 bis 07:14 (1 min)“. Sie wäre dabei jeweils von Führungskräften „beobachtet“ worden, habe sich mit anderen Beschäftigten „unterhalten“ und hätte damit „ihre arbeitsvertragliche Pflicht zur Erbringung der Arbeitsleistung verletzt“. Die aufgezeichneten Daten über einzelne Minuten der angeblichen „Inaktivität“ deuten auf die in den vorangehenden Abschnitten beschriebene „Time of Task“ hin.

Diese absurden Vorhaltungen wegen „Inaktivität“ legen nahe, dass Amazon schon 2014 auch in Deutschland die Arbeitsleistung minutengenau überwacht und ausgewertet hat. Amazon sprach von einem „Einzelfall“, bei dem „ein Vorgesetzter fehlerhaft gehandelt“ habe.[510] Laut einem deutschen Gewerkschafter lägen „andere Informationen und mündliche Rückmeldungen vor“, die belegen, dass dies „kein Einzelfall“ gewesen sei – und es sei auch „nicht nur an einem Standort passiert“. Auch wenn so getan worden wäre, also wären diese Dokumente so „ähnlich wie Abmahnungen, die man an die Personalakte anheftet“, wären sie arbeitsrechtlich „wertlos“. Sie wären aber insbesondere ArbeitnehmerInnen ausgehändigt worden, die befristet beschäftigt waren oder an Streiks teilgenommen hätten. Beschäftigte seien damit unter Druck gesetzt worden.[511] Staab und Nachtwey (2016) schreiben von regelmäßigen Personalgesprächen, in denen Beschäftigte „mit detaillierten Kenntnissen und Daten über ihre individuelle Arbeitsleistung konfrontiert werden“.

Im Jahr 2020 zeigte eine Recherche des NDR, dass Amazon auch in Deutschland eine permanente Leistungskontrolle auf Basis sekundengenauer Handscanner-Daten durchführt. Laut einem Interview mit einem Vorarbeiter hätten Führungskräfte Zugriff auf Daten über jeden Arbeitsschritt und über die durchschnittliche Rate der gescannten Pakete. Wäre die Rate zu niedrig, würde er als Vorarbeiter Gespräche mit den Beschäftigten führen – und dabei folgende Fragen stellen: „Unterhält sich der Mitarbeiter vielleicht zu lange, ist er nicht am Platz, zu oft auf der Toilette?“. An sogenannten „Release Days“ („Tagen der Freisetzung“) würde befristeten ArbeitnehmerInnen mit dauerhaft zu niedrigen Raten mitgeteilt, dass deren Vertrag nicht verlängert werde. Diese Kündigungen würden auf Basis von Leistungsdaten erfolgen – der Prozess sei „komplett standardisiert“ – und im Beisein von Sicherheitspersonal. Eine ehemalige Arbeitnehmerin berichtet, sie wäre mehrmals von Vorgesetzten darauf angesprochen worden, wo sie denn zu bestimmten Uhrzeiten gewesen sei – offensichtlich auf Basis von Handscanner-Daten. Die niedersächsische Datenschutzbehörde hat eine Untersuchung eingeleitet (Friedrich und Jolmes 2020).

Österreich. Ein ehemaliger Mitarbeiter im Amazon-Verteilzentrum in Großebersdorf ging 2019 mit Hilfe der Gewerkschaft GPA an die Öffentlichkeit und sagt, dass auch in Österreich die Arbeitsleistung mittels Handscanner ausgewertet werde und dass Beschäftigte gehen müssten, wenn sie nicht produktiv genug sind. Die Vorgaben von Amazon seien aber gar nicht zu erfüllen. Er spricht von vier ArbeitnehmerInnen, die wegen mangelhafter Leistung gekündigt worden wären.[512] Ein Schichtführer, der sich in Folge der medialen Aufmerksamkeit ebenfalls öffentlich zu Wort gemeldet hat, hat die Vorwürfe bestätigt und betont: „Wir können alle Daten einsehen“.[513]

Die Berichte aus Deutschland und Österreich legen nahe, dass die Leistungskontrolle hierzulande nicht offen durchgeführt wird, sondern versteckt – dass Beschäftigte also nicht direkt mit kontinuierlichen Rückmeldungen über ihre

[510] Amjahid, Mohamed (2015): Amazon überwacht Mitarbeiter minutengenau. Tagesspiegel, 13.3.2015. Online: https://www.tagesspiegel.de/wirtschaft/tarifkonflikt-beim-versandhaendler-amazon-ueberwacht-mitarbeiter-minutengenau/11499762.html

[511] Brodnig, Ingrid (2015): Kritik an Amazon: „Die Mitarbeiter werden regelmäßig überwacht“. Profil, 23.03.2015. Online: https://www.profil.at/wirtschaft/kritik-amazon-verdi-mitarbeiter-5569932

[512] Bruckner, Regina (2019): Amazon-Mitarbeiter prangert harsche Bedingungen in Austro-Niederlassung an. Standard, 12.6.2019. Online: https://www.derstandard.at/story/2000104750084/amazon-mitarbeiter-prangert-bedingungen-in-grossebersdorf-an

[513] Wiener Zeitung (2019): Streit um Arbeitsbedingungen bei Amazon geht weiter. 14.6.2019. Online: https://www.wienerzeitung.at/nachrichten/wirtschaft/international/2014091-Streit-um-Arbeitsbedingungen-bei-Amazon-geht-weiter.html

Leistung samt transparenter Androhung automatisierter Verwarnungen und Kündigungen unter Druck gesetzt werden, diese Daten bei mangelhafter Leistung aber trotzdem für Sanktionen bis hin zur Kündigung genutzt werden. Im Detail bleibt unklar, wie weitgehend die aus den USA und anderen Ländern dokumentierten Praktiken hierzulande eingesetzt werden.

7.1.5 Arbeit als Computerspiel – „Gamification" im Logistikzentrum

Parallel zur sekundengenauen Vermessung und Kontrolle einzelner Arbeitsschritte hat Amazon 2017 in den USA begonnen, die Arbeit in den Logistikzentren in ein Computerspiel zu verwandeln.

Mit Stand 2021 können Beschäftigte in 20 US-Bundesstaaten eines von sechs Spielen wie zum Beispiel „Picks in Space" wählen, die direkt mit ihren Arbeitstätigkeiten gesteuert werden – also etwa dem holen, sortieren oder ablegen von Produkten. Sie können dabei mit anderen Beschäftigten oder gar anderen Standorten in einen Wettbewerb treten und virtuelles Geld verdienen, das in kleine Belohnungen eingetauscht werden kann. Amazon betont, die Teilnahme wäre optional und das Programm wäre nicht dazu gedacht, Arbeitsleistung zu steuern oder zu erhöhen. Der Konzern ist allerdings stark auf maximale Produktivität ausgerichtet und es ist kaum anzunehmen, dass dieses Ziel nicht zumindest indirekt in die Gestaltung eingebaut ist. Beschäftigte nehmen das Programm zum Teil als willkommene Ablenkung vom monotonen Arbeitsalltag wahr, andere beschreiben den dystopischen Charakter.

Unter dem Schlagwort „Gamification" versuchen Unternehmen seit Jahren, Spielmechanismen in die Arbeitswelt zu integrieren, um Beschäftigte zu motivieren und deren Verhalten in die gewünschte Richtung zu beeinflussen (vgl. Abschnitt 5.4.9). Wie andere Firmen nutzt Amazon auch schon länger klassische Anreizmechanismen wie etwa tägliche Gewinnspiele, die Preise für die effizientesten Teams versprechen (Martineau und Di Stefano 2021).

7.1.6 Lückenloses System automatisierter Steuerung?

Staab und Nachtwey (2016) sehen in den Verteil- und Logistikzentren von Amazon ein außergewöhnlich hohes Maß an technischer Prozesskontrolle. Die Handscanner wären weit mehr als mobile Aufzeichnungs- oder Überwachungswerkzeuge. Sie würden darüber hinaus „jeden noch so kleinen Arbeitsschritt" unmittelbar vorgeben. Damit entstehe ein „beinahe lückenloses System automatisierter Steuerung, aus dem die Spielräume für die autonome Ausgestaltung der Arbeitsprozesse durch die Beschäftigten fast vollständig getilgt" sind. Das System sei mit einem mobilen Fließband zu vergleichen, das die räumlich verstreuten Beschäftigten über die Handscanner mit einer Steuerungs-Software verkopple, welche deren Aufgaben bis ins Detail reguliere. Die Folgen seien eine Intensivierung von Arbeit, ein Verlust von Autonomie und eine qualitative Abwertung von Tätigkeiten. Peter Wedde (2017, S. 18) sieht die Beschäftigten durch die permanente Kontrolle von Leistung und Arbeitsgeschwindigkeit in einem „Dauerakkord". Für „kleine Freiheiten" wie etwa kurze Gespräche mit KollegInnen oder kleine Trink- oder Verschnaufpausen wäre in einem derart vollständig durchorganisierten System kein Platz mehr.

Der extreme Druck, der durch rigide Leistungsvorgaben und die Überwachung „unproduktiver" Zeit samt automatisierter Verwarnungen oder gar Kündigungen entsteht, kann außerdem zu menschenunwürdigen Arbeitsbedingungen führen. In einer Umfrage unter britischen Amazon-Beschäftigten haben 74% angegeben, sie würden Toilettenbesuche vermeiden, um die vorgegebenen Raten zu erfüllen (Organise 2018). Wie mehrfach gezeigt wurde, kann sich dieser Druck auch auf Arbeitssicherheit und -gesundheit auswirken (vgl. Evens 2019, Evens 2020, Jabsky und

Obernauer 2019). Nicht zuletzt wurden die Leistungsaufzeichnungen gegen kritische Beschäftigte eingesetzt.[514] [515] [516] Der hohe Grad an Standardisierung von Arbeitsschritten in Kombination mit zentraler Steuerung und Kontrolle macht es zudem einfacher, Personal zu ersetzen (vgl. Kellogg et al 2020, S. 380), an Leiharbeitsfirmen auszulagern (vgl. Schörpf et al 2018, S. 9) oder etwa den Personalstand nach betrieblichem Bedarf kurzfristig zu erhöhen und zu senken. So hatte Amazon in Deutschland 2015 rund 15.000 Beschäftigte, zur Weihnachtszeit kamen vorübergehend noch einmal 10.000 dazu.[517] Im Verteilzentrum in Niederösterreich war 2019 ein Großteil der Belegschaft über eine Leiharbeitsfirma angestellt.[518]

[514] Palmer, Annie (2020): Amazon warehouse worker says she was written up in July for taking too many breaks from work. CNBC, 17.7.2020. Online: https://www.cnbc.com/2020/07/17/amazon-worker-claims-company-wrote-her-up-for-tot-policy-in-july.html

[515] Ongweso Jr, Edward (2020). Rights Groups Demand Lawmakers Stop Amazon's Workplace Surveillance. Vice, 14.10.2020. Online: https://www.vice.com/en/article/jgxy7k/rights-groups-demand-lawmakers-stop-amazons-workplace-surveillance

[516] Brodnig, Ingrid (2015): Kritik an Amazon: „Die Mitarbeiter werden regelmäßig überwacht". Profil, 23.03.2015. Online: https://www.profil.at/wirtschaft/kritik-amazon-verdi-mitarbeiter-5569932

[517] Ebd.

[518] Bruckner, Regina (2019): Amazon-Mitarbeiter prangert harsche Bedingungen in Austro-Niederlassung an. Standard, 12.6.2019. Online: https://www.derstandard.at/story/2000104750084/amazon-mitarbeiter-prangert-bedingungen-in-grossebersdorf-an

7.2 Umfassendes Bewertungssystem bei Zalando

Die Hans-Böckler-Stiftung des DGB hat 2019 eine Studie über die Einführung eines sehr umfassenden Kontrollsystems beim deutschen Versandhandelsriesen Zalando veröffentlicht, die in folgendem Abschnitt zusammengefasst wird (vgl. Staab und Geschke 2020).[519] Das intern als „**Zonar**" bezeichnete System kommt für 5000 Beschäftigte[520] vorwiegend im Bürobereich zum Einsatz und sortiert sie unter Einbeziehung laufender gegenseitiger Bewertungen von Beschäftigten in drei Gruppen: **Low, Good und Top Performer**. Diese Einteilung der Belegschaft in drei Gruppen wird laut Studie für Bewertungsgespräche, die Verteilung von Aufstiegsoptionen und die Gewährung oder Versagung gruppenspezifischer Lohnerhöhungen genutzt (ebd., S. 10). Während sogenannte horizontale Bewertungen – also Bewertungen nicht nur durch Vorgesetzte, sondern auch durch KollegInnen – bei Führungskräften schon länger üblich sind, dehnt Zalando dieses Instrument auf alle Beschäftigten aus (ebd., S. 17).

Die Studie beschreibt auf Basis von Interviews mit Zalando-MitarbeiterInnen und der Analyse von Präsentations- und Schulungsmaterialien die Entwicklung und Anwendung des Systems von der Pilotphase 2016 und der unternehmensweisen Einführung 2017 bis ins Jahr 2019 (ebd., S.12-13, 23).[521] Zalando hat jede Zusammenarbeit verweigert (ebd., S. 6). Dennoch bietet die Studie einen guten Einblick in Funktionsweise und Auswirkungen eines algorithmisch strukturierten Bewertungssystems bei einem Leitunternehmen der Digitalisierung in Deutschland, das einerseits an die Tradition des sogenannten „360-Grad-Feedback" anschließt und andererseits die Produktbewertungs-Mechanismen des kommerziellen Internets in die betriebliche Sphäre spiegelt (ebd., S. 10).

7.2.1 Funktionsweise – Laufende gegenseitige Bewertungen

Das System „Zonar" bei Zalando kombiniert laut Studie oftmalige situationsbezogene Echtzeitbewertungen mit umfassenden halbjährlichen Leistungs- und Entwicklungsbeurteilungen.

Bei den Echtzeitbewertungen stehen mehrere Varianten zur Verfügung – von schnellen Punktebewertungen ohne viel Kontext via App durch Vorgesetzte, KollegInnen oder Untergebene – das sogenannte „In the Moment" Feedback" – bis zu tiefergehenden Bewertungen zwischen Beschäftigen, die täglich intensiv zusammenarbeiten – das sogenannte „Deep Dive" Feedback (ebd., S. 19-22). Wird eine Person bzw. die Zusammenarbeit mit der Person bewertet, muss neben einem Freitext in mehreren Kompetenz- und Themenbereichen jeweils ein Rating zwischen einem und fünf Sternen vergeben werden – ähnlich wie bei den Produktbewertungen in Online-Shops (ebd., S. 24).

Bei den halbjährlichen Leistungs- und Entwicklungseinschätzungen erfolgt neben einer Beurteilung durch die direkten Vorgesetzten eine umfangreiche Beurteilung durch eine KollegIn, mit der im letzten halben Jahr häufig und eng zusammengearbeitet wurde. Dabei soll die Leistungsentwicklung im Kontext von Arbeitsaufgaben und Projekten bewertet werden. Im Anschluss stuft das System die Beschäftigten auf Basis verschiedener quantitativer Bewertungen als Low, Good oder High Performer ein. Direkte Vorgesetzte können eine eigene Einstufung vornehmen und argumentieren, erstellen einen Leistungs- und Entwicklungsbericht und können den Beschäftigten als „beför-

[519] Die Studie wurde im Oktober 2019 erstveröffentlicht und nach einem Rechtsstreit 2020 aktualisiert. Wir beziehen uns auf die 2020 veröffentlichte Version der Studie. Im Literaturverzeichnis sind beide Versionen angeführt.

[520] Zalando (2019): Unser Statement zur Studie der Hans-Böckler-Stiftung, 19.11.2019. Online, https://corporate.zalando.com/de/newsroom/de/news-storys/unser-statement-zur-studie-der-hans-boeckler-stiftung

[521] Hans Böckler Stiftung (2019: Wenn Beschäftigte ähnlich wie Käufe im Online-Shopping geranked werden - neue Studie untersucht Software bei Zalando, Pressemitteilung 20.11.2019. Online: https://www.boeckler.de/de/pressemitteilungen-2675-wenn-beschaeftigte-aehnlich-wie-kaeufe-im-online-shopping-gerankt-werden-neue-studie-18612.htm

derungsbereit“ vorschlagen. Bei widersprüchlichen Bewertungen entscheidet ein Fallprüfungskomitee („People Review Commitee“, kurz PRC). Schlussendlich erfolgt ein Entscheidungs- und Entwicklungsgespräch mit der ArbeitnehmerIn und der Zyklus beginnt von vorne (ebd., S. 19-22). Die Beschäftigten erhalten eine Visualisierung, die die eigenen Leistungsbewertungen zusammenfasst und in ein Verhältnis zu Durchschnittswerten stellt (ebd., S. 39).

Folgende Ausschnitte aus einem internen Handbuch für die Zonar-Version 2 zeigen die einzelnen Schritte des halbjährlichen Bewertungszyklus und die vier „Hauptentscheidungen“, die damit über Beschäftigte getroffen werden sollen: **Leistung** (bzw. „ob eine Leistungsverbesserung erforderlich ist“), **Rollenerfüllung** (im Verhältnis zu „Erwartungen und Anforderungen“), **Beförderungsbereitschaft** (bzw. Empfehlung oder Nicht-Empfehlung einer Beförderung) sowie **Vergütung** (bzw. „ob und in welcher Höhe“ eine Gehaltserhöhung erfolgen soll):[522]

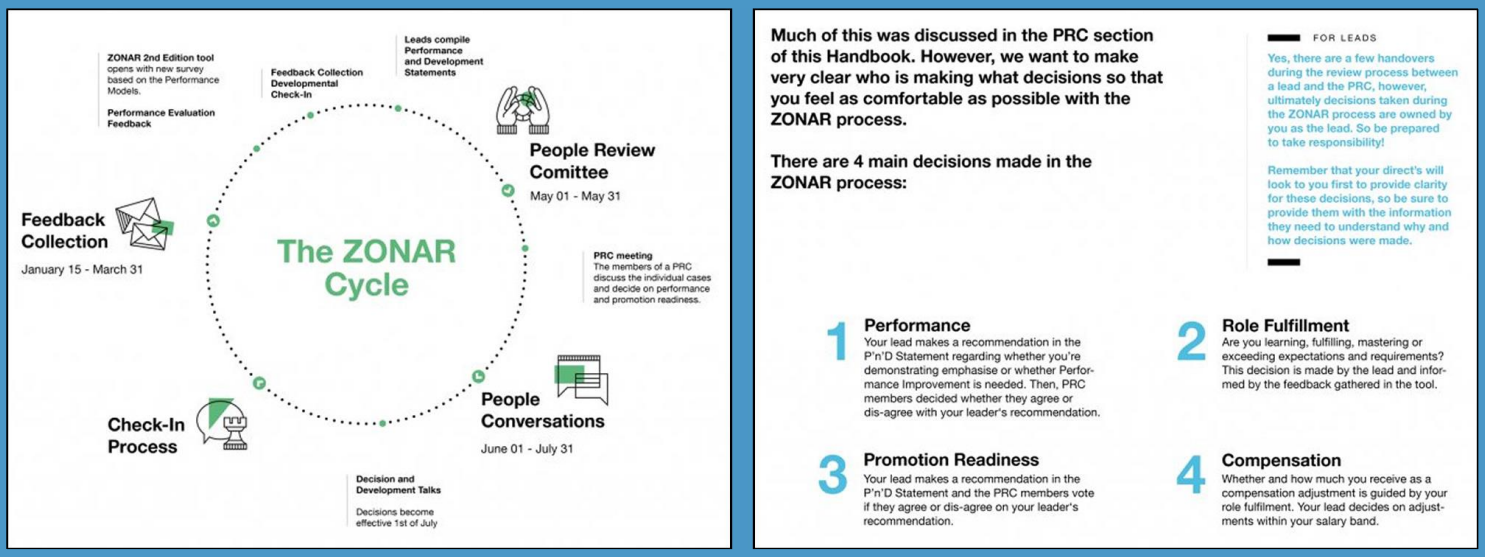


Abbildung 25: Ausschnitte aus dem internen Handbuch von Zalando’s Zonar-System. Quelle: Grafikagentur/Hersteller

7.2.2 Auswirkungen auf Beschäftigte – „System der kompletten Kontrolle“?

Während Zalando das System als Werkzeug zur persönlichen Karriereentwicklung versteht – und es gar als Instrument der Mitbestimmung im Unternehmen darstellt – nehmen die für die Studie interviewten ArbeitnehmerInnen Zonar als „360-Grad-Überwachung“, als „System der kompletten Kontrolle“ oder gar als „Stasi-System“ wahr.

Das Gefühl, permanent von KollegInnen bewertet zu werden, erhöhe laut Studie den **Arbeitsdruck und -stress**, führe zu gegenseitigem Misstrauen und habe negative Auswirkungen auf **Betriebsklima und Arbeitsqualität** (ebd., S. 29f; 43). Beschäftigte würden dazu angehalten, permanent Belege für die Bewertungen zu sammeln. Vorgesetzte könnten weitere Nachforschungen dazu anstellen (ebd., S. 46f). Generell würden Bewertungen durch KollegInnen potenziell die gesamte Persönlichkeit umfassen. Subjektive Faktoren wie Sympathien oder Antipathien könnten Ergebnisse verzerren (ebd., S. 38) und damit zu „quantifizierter“ **Willkür** führen (ebd., S. 31; 38; 40).

[522] Beide Abbildungen (c) Zalando/mawidesign. Die Abbildung(en) dienen als Beleg für die im Rahmen dieser Studie untersuchten Firmenpraktiken und stammen laut der Website einer Grafikagentur aus dem Handbuch „Zonar 2nd Edition“, S. 10 und S. 26. Quelle: https://www.mawidesign.de/projekte/zalando-zonar/ [15.5.2021]

Darüber hinaus arbeitet die Studie folgende Eigenschaften und Auswirkungen des Systems heraus:

- **Umfassendes Kontrollsystem.** Zonar sei ein „äußerst ambitioniertes Kontrollinstrument“ und ein „umfassendes System des algorithmischen Managements“ (ebd., S. 11; 56).
- **Leistungsdruck durch Verstärkung innerbetrieblicher Konkurrenz.** Die Konkurrenz um gute Bewertungen und damit verknüpfte Privilegien wie Aufstiegschancen oder Gehaltserhöhungen verstärkt sich alleine durch die rigide Einordnung der Belegschaft in drei Klassen. Diese suggerieren Vergleichbarkeit und erzeugen damit Leistungsdruck, Selbstdisziplinierung und Stress. Der hochkompetitive Charakter verstärkt sich nochmals durch die kontinuierlichen Bewertungen durch KollegInnen sowie durch die Zugänglichmachung von Leistungsauswertungen im Vergleich zu Durchschnittswerten (ebd., S. 29f; 37; 39f).
- **Verschleierung vertikaler Kontrolle.** Bewertungen unter KollegInnen verschieben vertikale Kontrolle – also zwischen Vorgesetzten bzw. dem Betrieb einerseits und den ArbeitnehmerInnen andererseits – auf eine horizontale Ebene. Dies trage zur Verschleierung vertikaler Kontrolle bei (ebd., S. 28; 36).
- **Legitimierung betrieblicher Ungleichheit.** Durch die Einordnung der Belegschaft in drei Gruppen samt damit verbundener Privilegien und Sanktionen schafft und legitimiert das System betriebliche Ungleichheit in einer Form, die zuvor so nicht bestand (ebd., S. 34).
- **Unterminierung von Solidarität unter den Beschäftigten.** Die Verschiebung von Kontrolle auf eine horizontale Ebene, die Verstärkung innerbetrieblicher Konkurrenz sowie die Legitimierung betrieblicher Ungleichheit unterminiert potenziell die Solidarität unter den Beschäftigten (vgl. ebd., S. 29).
- **Scheinobjektive Gestaltung im Interesse des Betriebs.** Das System gibt vor, es sei ein „objektives“ Messverfahren. Dies sei nicht der Fall, denn durch die spezifische Gestaltung von Datenerhebung und -auswertung würden die Ergebnisse im betrieblichen Interesse verzerrt und geformt (ebd., S. 31).
- **Lohnrepression.** Da sich die Leistungsbewertungen direkt oder indirekt auf die Entlohnung auswirken können und das System so gestaltet sei, dass gute Bewertungen verknappt werden, diene es der Kostensenkung und Lohnrepression. Laut Studie wird die Vergabe von guten oder sehr guten Bewertungen erschwert, Beschäftigte werden von Vorgesetzten dazu angehalten, negativer zu urteilen (ebd., S. 43). Die Hälfte der abgegebenen Bewertungen muss obligatorisch negativ sein, schlechte Bewertungen würden damit „regelrecht erzwungen“. Die Zahl der „Top Performer“ werde so systematisch gering gehalten (ebd., S. 34). In einem Fall erhielt ein Beschäftigter Aufgaben auf einer höheren Hierarchieebene, wegen der Leistungseinstufung als lediglich „Good Performer“ aber keine entsprechende Gehaltsposition (ebd., S. 44).
- **Systematische Intransparenz.** Funktionsweise und Logiken der Bewertungsalgorithmen seien strukturell intransparent, das System sei in vieler Hinsicht eine „Blackbox“ und erzeuge damit ein Gefühl der Machtlosigkeit bei den Beschäftigten (ebd., S. 46f).
- **Datenschutzrechtliche Legalität?** Es bestehen Zweifel an der rechtlichen Zulässigkeit des Systems, insbesondere in Hinblick auf unverhältnismäßige Profilbildung und Überwachung, Informations- und Transparenzpflichten und generell in Bezug auf die Rechtsgrundlage der Datenverarbeitung (ebd., S. 51ff).
- **Betriebswirtschaftliche Effektivität?** Nicht zuletzt bestehen „deutliche Zweifel“ daran, ob das System überhaupt den Zweck eines „effizienzsteigernden betrieblichen Kontrollinstruments“ erfüllen kann. Es habe zahlreiche Nebenwirkungen, die sich potenziell negativ auf die Produktivität der Beschäftigten auswirken und die „Erträge“ durch den Einsatz des Systems ließen sich angesichts des hohen Aufwands kaum messen (ebd., S. 58f).

7.2.3 Rechtliche Schritte gegen Studie

Zalando hat jede Zusammenarbeit mit den Studienautoren verweigert, bezweifelt die Repräsentativität der Studie, unterstellt „Einseitigkeit“ und „mangelnde Neutralität“[523] und ist rechtlich gegen die Autoren vorgegangen. Wie im Vorwort einer aktualisierten Version der Studie beschrieben, wollte der Konzern via Abmahnung acht Aussagen aus der Studie entfernen lassen und war bei einer davon erfolgreich. Die Autoren dürfen nicht mehr behaupten, dass sie „keine Hinweise darauf finden [konnten], dass hier irgendeine Form der Mitbestimmung [durch Betriebsräte] erfolgte“. Sie hatten zwar im Zuge der Forschungsarbeit eine Frage dazu an Zalando gestellt. Ihre Frage war aber laut Gericht nicht konkret genug. Zalando hat ohnehin keine der Fragen der Autoren beantwortet (ebd., S. 6f).

Die Autoren dürfen im Kapitel **„Betriebsratsfeindlichkeit“** jedoch weiterhin das „grundsätzlich mitbestimmungsfeindliche Gebaren des Unternehmens“ kritisieren und festhalten, dass Zalando nur „sehr fragmentierte Betriebsräte für gewisse Abteilungen“ besitze und „formale Strukturen der Mitbestimmung“, die eine Partizipation an Entscheidungen zu „Zonar“ erzwingen könnten, nur „sehr begrenzt vorhanden“ wären (ebd., S. 48ff). Erst im Oktober 2020 wurde bei Zalando erstmals ein Betriebsrat nach deutschem Recht gewählt.[524]

7.2.4 Intervention der Berliner Datenschutzbehörde

Nach Veröffentlichung der Studie hat die Berliner Datenschutzbehörde eine Prüfung eingeleitet, deren Verlauf im Jahresbericht der Behörde grob umrissen wird (BInBDI 2021, S. 123-126). Zalando wurde aufgefordert, diverse Änderungen vorzunehmen. Dem sei Zalando laut Behörde nachgekommen, das System sei nach den vorgenommenen Änderungen nun datenschutzrechtlich zulässig.

So werde eine Person nun von nur mehr drei Personen bewertet, die bewertete Person habe ein Vetorecht, und es erfolge keine Bewertung auf einer „Punkteskala“ mehr. Die Bewertungsdaten selbst sind nicht mehr über mehrere Zyklen hinweg einsehbar, das Ergebnis darf allerdings weiterhin für die Dauer des Beschäftigungsverhältnisses gespeichert werden. Grundsätzlich schreibt die Behörde, dass Beschäftigte bei derartigen Systemen „nicht nur bei Begegnungen mit der Chefin oder dem Chef jederzeit damit rechnen“ müssten, dass „ihr Verhalten das nächste Zeugnis beeinflusst, sondern auch bei jeder Begegnung mit einer anderen Person des Unternehmens, da auch diese Begegnungen Auswirkungen auf die nächste Beurteilung und damit auch auf das weitere Berufsleben haben könnten. Die Folge kann ein permanenter Überwachungsdruck und Stress sein, der sich aus der Sorge um das berufliche Fortkommen ergibt.“ Während einzelne der durch die Behörde erzwungenen Änderungen durchaus signifikant erscheinen, werden bei anderen die Grenzen des Datenschutzrechts sichtbar – wenn die Behörde etwa festhält, dass Beschäftigte nach wie vor keine Nachteile zu befürchten hätten, wenn sie am System nicht teilnehmen. Ob dies angesichts des Machtungleichgewichts im Betrieb wirklich sichergestellt werden kann, darf bezweifelt werden.

Datenschutzrecht ist bei der Frage nach der Zulässigkeit eines derartigen Systems natürlich nicht das einzige Kriterium. Zentraler Hebel für betriebliche Mitbestimmung ist neben dem Datenschutz vielmehr das Arbeitsrecht, in Deutschland das Betriebsverfassungsgesetz (vgl. Däubler 2017, S. 75), in Österreich das Arbeitsverfassungsgesetz (vgl. Haslinger et al 2020, S. 131).

---

[523] Zalando (2019): Unser Statement zur Studie der Hans-Böckler-Stiftung, 19.11.2019. Online, https://corporate.zalando.com/de/newsroom/de/news-storys/unser-statement-zur-studie-der-hans-boeckler-stiftung

[524] Kaleta, Philip (2020): 5.000 Mitarbeiter der Zalando SE wählen erstmals einen Betriebsrat – per Brief. Business Insider, 6.10.2020. Online: https://www.businessinsider.de/bi/5-000-mitarbeiter-der-zalando-se-waehlen-erstmals-einen-betriebsrat-per-brief/

8. Interviewbasierte Fallstudien über Betriebe in Österreich

Als Teil des Projekts[525], das auch zur vorliegenden Studie geführt hat, hat Hans Christian Voigt auf der Grundlage von leitfadengestützten Interviews mit BetriebsrätInnen zwischen Dezember 2019 und Juni 2020 eine kleinere explorative Untersuchung über den konkreten Einsatz digitaler Überwachungs-, Steuerungs- und Kontrollsysteme in österreichischen Betrieben durchgeführt.

Die Auswahl der GesprächspartnerInnen und Fallbeispiele wurde zwischen Hans Christian Voigt, Wolfie Christl, der Projektsteuerungsgruppe und ExpertInnen aus den Gewerkschaften abgestimmt. Die ursprünglich geplanten Gruppendiskussionen und Betriebsbesuche mussten wegen der Corona-Krise bis auf eine Ausnahme durch Einzelinterviews ersetzt werden. Den GesprächspartnerInnen wurde Anonymität zugesichert. Die konkreten Betriebe und zum Teil auch die diskutierten Software-Lösungen bleiben ungenannt, um die GesprächspartnerInnen zu schützen. Insgesamt wurden acht Gespräche mit zehn BetriebsrätInnen aus acht Unternehmen geführt. Die Fallbeispiele beschreiben die Perspektive und Erfahrungen der ArbeitnehmerInnenvertretung. Neben den eingesetzten Systemen wurden die Auswirkungen auf den betrieblichen Alltag und der Umgang des Betriebsrats damit diskutiert.

In mehreren Fallbeispielen spielen rechtliche Aspekte in Hinblick auf Datenschutz und Mitbestimmung eine Rolle. In Österreich benötigt die Geschäftsführung eines Betriebs bei der Einführung bestimmter Arten datenverarbeitender Systeme zwingend die Zustimmung der ArbeitnehmerInnen oder deren Vertretung. Ist ein Betriebsrat vorhanden, werden Zustimmung und Einsatz der Systeme durch einen Vertrag zwischen Geschäftsführung und Betriebsrat geregelt – der sogenannten Betriebsvereinbarung (vgl. Haslinger et al 2020, S. 155). Neben dem Abschluss separater Betriebsvereinbarungen für separate technische Systeme wurde seit einiger Zeit damit begonnen, sogenannte Rahmenbetriebsvereinbarungen zu verhandeln, die betrieblichen Datenschutz über Systeme hinweg regeln – und die dann durch Anhänge für einzelne Systeme und Anwendungen ergänzt werden (ebd., S. 231). Unternehmen haben zudem diverse Informationspflichten gegenüber Beschäftigten und Betriebsrat (ebd., S. 138).

In den folgenden Abschnitten werden die im Rahmen der Untersuchung von Hans Christian Voigt entstandenen Fallbeispiele knapp zusammengefasst.

8.1 Beispiel Außendienst, Montage und Wartung im Anlagenbau

Dieses Fallbeispiel zeigt auf Basis von Interviews mit BetriebsrätInnen aus zwei konkurrierenden Unternehmen der gleichen Branche, die Teil global agierender Firmen sind, wie massiv das Smartphone und andere technische Systeme den Arbeitsalltag im Außendienst bei Montage, Wartung und Störungsdienst verändert haben.

Bei der Einführung der ersten Mobiltelefone hatten die Beschäftigten noch fixe Zuständigkeiten und Routen und haben sich die Arbeit selbst eingeteilt. Annahme, Ablehnung oder Erledigung von Aufträgen wurden mit rudimentären SMS-Codes an die Zentrale zurückgemeldet. Diese Meldungen waren nicht überprüfbar. Heute werden alle Bewegungen, Zeiträume und Arbeitsschritte via **Smartphone-App** dokumentiert. Eine Karte in der Zentrale zeigt, wer gerade woran arbeitet. GPS-Ortung erfolgt nur auf freiwilliger Basis und ist nicht entscheidend, denn das mobile

[525] Siehe Kapitel 0

System zur Abwicklung von Aufträgen kennt Arbeitszeiten und Standorte auch ohne GPS-Ortung im Detail. Das mobile System ist an SAP angebunden.

Gleichzeitig werden die durchzuführenden Arbeitsschritte immer genauer vorgegeben. In einem Betrieb wird seit kurzem ein KI-System eingesetzt, das Arbeitsschritte auf Basis von Messdaten definiert, die die Anlagen selbsttätig in die Zentrale senden. Aus dem Industriebetrieb werde ein Hardware- und Softwarebetrieb, der eine Plattformlösung anbietet, die alles vernetzt. Die Kundenbetriebe, die die Anlagen betreiben, möchten die WartungsmitarbeiterInnen zunehmend wie die eigene Belegschaft steuern und kontrollieren und haben in einem Betrieb Echtzeit-Zugriff auf Daten über durchgeführte Arbeiten und durchführende ArbeitnehmerInnen. Dafür wird eine eigene Schnittstelle als Leistungspaket angeboten. Damit werden Beschäftigtendaten bzw. digitale Kontrolle zum Produkt des Unternehmens. Die Kundenbetriebe drängen in einem weiteren Schritt sogar auf die Nutzung von „smarten" Geräten, die komplett unter der Kontrolle des Kundenbetriebs stehen, durch die WartungsmitarbeiterInnen.

In den Interviews werden folgende Auswirkungen auf Beschäftigte und Mitbestimmung deutlich:

- **Reduktion von Autonomie, Selbstbestimmung und Sinnstiftung** aufgrund immer genauerer Vorgaben für einzelne Arbeitsschritte. Es wird von eine digitale „Starrheit" wahrgenommen, die kaum Korrekturmöglichkeiten zulasse. Ältere Beschäftigte haben sich früher als „Experten" mit umfangreichem Wissen über die betreuten Anlagen und die benötigte Zeit für Tätigkeiten wahrgenommen. Dieses Wissen läge jetzt in den technischen Systemen. Die Komplexität der Systeme und laufende Updates machen sie intransparent, erschweren Mitbestimmung und erzeugen Unbehagen und Ohnmacht.
- **Beschleunigung und Verdichtung von Arbeit**, da sich die für einzelne Tätigkeiten zur Verfügung stehende Zeit im Lauf der Jahre auf einen Bruchteil reduziert hat.
- **Umfassende Leistungs- und Verhaltenskontrolle.** Das Smartphone habe die Überwachung und Kontrolle der Belegschaft entscheidend verschärft. Die Ausweitung der Datenerfassung habe dazu geführt, dass die benötigte Zeit für Tätigkeiten und Arbeitsschritte bei teils wöchentlichen Gesprächen auf Minuten– oder gar Sekundenniveau diskutiert werde. Führungskräfte bekämen Vorgaben für Kennzahlen und machen Druck, Zeit für Tätigkeiten oder laut System nicht notwendige Serviceschritte einzusparen.
- **Herausforderungen für den Betriebsrat.** Wegen der hohen Komplexität musste für die Verhandlung einer Betriebsvereinbarung ein technischer Experte beigezogen werden. Während für die mobilen Systeme Betriebsvereinbarungen vorhanden sind, fehlt diese für das angebundene SAP-System in einem Betrieb bis heute. Updates werden aus der Konzernzentrale im Ausland gesteuert und erfolgen am Betriebsrat vorbei.

8.2 Beispiel Sozial- und Gesundheitsbereich

Dieses Fallbeispiel basiert auf Interviews mit BetriebsrätInnen aus drei Organisationen im Sozial- und Gesundheitsbereich mit unterschiedlichen Tätigkeitsbereichen – von der Betreuung und Pflege in Häusern mit vielen KlientInnen über den Betrieb von Laboren mit medizinischen Apparaten bis zur Verwaltung einer Rettungsorganisation.

Intransparenz. Keiner der drei Betriebe kommt seinen **Informationspflichten** nach. Die Betriebsräte sind unsicher, welche datenverarbeitenden Systeme überhaupt im Einsatz sind. Ihnen liegen keine Beschreibungen der verarbeiteten Daten und Verarbeitungszwecke vor. Sie werden vor der Einführung neuer Systeme nicht informiert.

In zwei der drei Betriebe wurden Daten für **unzulässige Auswertungen und Leistungsbeurteilungen** genutzt. So wurden Beschäftigte etwa mit Auswertungslisten von Krankenständen und mit Ranglisten auf Basis von Daten

medizinischer Geräte und Fehlerprotokolle unter Druck gesetzt. Die Geschäftsführung streitet diese offensichtlichen Missbrauchsfälle ab. Der Betriebsrat ist hingegen als Gremium nicht entschlossen genug aufgestellt, um die Rechte der Belegschaft durchzusetzen. Im dritten Betrieb ist einigen Jahren ein System im Einsatz, das sehr umfangreiche und detaillierte **Daten über einzelne Arbeitsschritte** erfasst, unter anderem um Leistungen für KlientInnen genauer abzurechnen und Extraleistungen abseits der Pauschale verrechnen zu können. Das System wird einerseits als arbeitserleichternd erlebt. Andererseits zwängt es die Komplexität des Arbeitsalltags in ein rigides Raster vorgegebener **Kategorien von Tätigkeiten**, die einige notwendige Tätigkeiten schlecht oder gar nicht abbildet, keine menschlichen Bedürfnisse wie Toilettenbesuche kennt und durch Vorgaben für **Normzeiten für Tätigkeiten** Druck ausübt. Der befragte Betriebsrat nimmt an, dass die Daten aktuell darüber hinaus nicht zur Leistungskontrolle verwendet werden, sieht aber künftiges Missbrauchspotenzial und mangelndes Problembewusstsein im Betriebsratsgremium.

Herausforderungen für den Betriebsrat. Neben der Intransparenz der eingesetzten Systeme liegt für die Mehrzahl der Systeme keine Betriebsvereinbarungen vor, obwohl angenommen wird, dass diese rechtlich erforderlich wären. Die Geschäftsführungen behaupten zumeist mit fragwürdigen Begründungen, dass keine Betriebsvereinbarungen erforderlich wären – etwa weil ein System gesetzlich verpflichtend sei, es vom TÜV überprüft worden wäre oder nur im Probebetrieb sei. Dies führt immer wieder zu Verunsicherung bei den BetriebsrätInnen. In einem Betrieb ist nach zehn Jahren nun eine Rahmenbetriebsvereinbarung[526] in Arbeit.

Mängel bei IT-Infrastruktur, Datensicherheit und sonstigen Abläufen. Den Interviews zu Folge ist die Beschaffung von IT-Systemen teils von Planlosigkeit geprägt, ihr Betrieb von laufenden Fehlern. In einem Fall müssten die Beschäftigten die Logik eines technischen Systems umgehen, um der Organisation das eigentlich geforderte Vier-Augen-Prinzip zu ersparen. In allen drei Betrieben gäbe es kaum Beschränkungen für den Zugriff auf sensible Daten von KlientInnen oder Beschäftigten. Sollte das zutreffen, wäre das ein an grobe Fahrlässigkeit grenzender Mangel in Hinblick auf Datensicherheit. In einem Betrieb müssen die Beschäftigten laufend in einer Web-Oberfläche mittels Klick neue oder geänderte Regeln für Arbeitsabläufe – sogenannte „Standard Operating Procedures“ (SOP)[527] – signieren, bevor die Arbeit im System fortgesetzt werden kann. Da für das Studium der Regeln keine Arbeitszeit vorgesehen sei, entstehe ein Effekt wie beim „wegklicken“ von Nutzungsvereinbarungen.

8.3 Beispiel “Smart Factory”

Dieses Fallbeispiel zeigt, wie eine Belegschaftsvertretung in einem österreichischen Industriebetrieb mit mehreren tausend Beschäftigten, der Teil eines internationalen Konzerns ist, trotz einer vielfältigen und sich permanent verändernden Landschaft datenverarbeitender Systeme laufend betriebliche Mitbestimmung durchsetzt. Im Unternehmen gibt es zwei Betriebsratsorgane. Neben dem Arbeiterbetriebsrat in der mechanischen Fertigung, die die Montage von Motoren und die Bearbeitung von Bauteilen umfasst, gibt es im administrativen Bereich einen Angestelltenbetriebsrat.[528] Das Fallbeispiel basiert auf einem Gespräch mit drei BetriebsrätInnen aus beiden Bereichen.

Fertigung. Die Interviewpartner kennen Schlagwörter wie „Smart Factory“ oder „Industrie 4.0“ erst seit wenigen Jahren. Die Computerisierung der Produktion begann jedoch lange zuvor und wird nicht als sprunghafte Entwicklung wahrgenommen, sondern als kontinuierlicher, sich beschleunigender Prozess. Während vor der Einführung

[526] Vgl. Haslinger et al 2020, S. 231

[527] Siehe z.B. https://de.wikipedia.org/wiki/Standard_Operating_Procedure

[528] Arbeiterbetriebsrat/Angestelltenbetriebsrat siehe z.B. Kozak, Wolfgang (2012): Wichtiges aus dem Angestelltenrecht. VÖGB/AK, März 2012. Online: https://www.wu.ac.at/fileadmin/wu/o/we4u/text/ar-14.pdf

erster Systeme für die rechnergestützte Fertigung in den 1990er Jahren Daten über Abläufe und Maschinen händisch mit Listen erfasst wurden, wurden die Anlagen danach zunehmend vernetzt. Heute wird in der Produktion eine Vielzahl von automatisiert erfassten Betriebsdaten genutzt. Fast monatlich werden neue datenverarbeitende Systeme eingeführt. Im Rahmen der Instandhaltung werden Daten aus der ganzen Produktionskette analysiert, um Fehler zu finden – möglichst schon bevor eine Anlage ausfällt. Daten über Werkstücke stehen genauso zur Verfügung wie Daten über den Motor in der Montageanlage. Die Beschäftigten verwenden Barcode-Lesegeräte, die in den Handschuh integriert sind – also tragbare Geräte, die potenziell detaillierte Daten über Arbeitstätigkeiten erfassen. Sie können aber wahlweise die alten stationären Scanner am Federzug verwenden. Generell werden Arbeitsschritte immer mehr von technischen Systemen vorgegeben. In der „Smart Factory" existieren aber parallel zu sehr neuen Technologien immer noch ältere Systeme und Abläufe – von veralteten Monitoranzeigen bis zu ausgedruckten Checklisten. Auch wenn viele Anwendungen inzwischen Teil einer konzernweit zentralisierten IT-Infrastruktur sind, gibt es immer noch ältere Systeme, die nur schwer vernetzt und integriert werden können.

Büro- und Wissensarbeit. Im Bereich abseits der Produktion wird Software für Projektmanagement wie Microsoft Project eingesetzt, die allein wegen ihrer Funktionsweise erfasst, wer wie lange für welche Tätigkeit benötigt. Microsoft 365 und Software für agiles Management bieten nun potenziell noch mehr Auswertungsmöglichkeiten.

Mitbestimmung. Die zwei Betriebsratsorgane aus dem Arbeiter- und Angestelltenbereich haben ein gemeinsames Datenschutz-Gremium installiert, das monatlich tagt und neu einzuführende datenverarbeitende Systeme bewertet. Bei Bedenken wird die Einführung abgelehnt, ansonsten wird mit der Geschäftsführung ein Anhang zur Rahmenbetriebsvereinbarung verhandelt und deren Einhaltung mit Einsichtsrechten kontrolliert. Bei der Einführung von Handschuhen mit integrierten vernetzten Geräten wurde etwa ausverhandelt, dass die Nutzung nicht verpflichtend sei und alternativ die alten stationären Barcode-Lesegeräte verwendet werden können. In manchen Monaten werden zwei bis drei neue Anwendungen verhandelt. Mitunter würde ein neues System für einige Tage oder Wochen ohne Genehmigung laufen. Durch die gute Zusammenarbeit mit der Belegschaft würden derartige Vorfälle aber schnell entdeckt. Der Betriebsrat würde in solchen Fällen hart durchgreifen und die Anwendung sofort abschalten lassen, um ernstgenommen zu werden. Im Angestelltenbereich wäre dies allerdings schwieriger.

Bei der Einführung neuer Systeme durch die Konzernmutter werde mit deren Betriebsrat zusammengearbeitet. Die Zentralisierung der IT habe die Standardisierung vorangetrieben und gleichzeitig die Dynamik der Entwicklung verringert, da schnelle Anpassungen nicht mehr so einfach möglich sind. Grundsätzlich gäbe es ein Bewusstsein dafür, dass unzulässige Verknüpfungen oder Auswertungen der umfassenden Datenbestände hohe Risiken bergen. Man sei aber optimistisch, den Überblick zu behalten und Missbrauch verhindern zu können. Selbst wenn sich die Einführung problematischer Systeme nicht ganz verhindern lasse, so lässt sich zumindest regelnd eingreifen. Man sieht die größere Zahl neuer Systeme sogar als Verbesserung der Verhandlungsposition, da sich der Betriebsrat eine Zustimmung mit Zugeständnissen an die Belegschaft „abkaufen" lassen könne.

Wahrnehmungen der Beschäftigten. Der Stress an den manuellen Arbeitsplätzen, der heute etwa durch eine Konkurrenz zwischen Teams und Abteilungen entstehe, wäre im Lauf der Jahre nicht gestiegen. Ältere Beschäftigte hätten aber früher viel eigenverantwortlicher gearbeitet und haben bei der Einführung neuer Systeme eine höhere Sensibilität gegenüber möglichem Missbrauchspotenzial in Hinblick auf Überwachung, Steuerung und Kontrolle. Jüngeren würden Systeme, die vieles vorgeben und bei denen Vorgesetzte viele Einblicke bekommen, selbstverständlich erscheinen. Im Bereich der Instandhaltung führen Fehlersuche unter Zeitdruck sowie laufender Rechtfertigungsdruck zu großen psychischen Belastungen. Generell werden neue Systeme meist positiv und als Arbeitser-

leichterung wahrgenommen. Der Betriebsrat sieht als zentrale Aufgabe, zu verhindern, dass damit Druck auf Beschäftigte aufgebaut wird. Im Angestelltenbereich führen unter anderem digital vernetzte standortübergreifende Teams zu einer Arbeitsverdichtung.

Einem Interviewpartner zu Folge wären die erfassten Produktionsdaten dazu geeignet, den Betrieb zu „spiegeln" und damit anderswo in der Welt neue Betriebsstätten hochzuziehen. Man könnte damit dieses Wissen, das durch die Datenerfassung entsteht, als Ausdruck der **Datenmacht des Konzerns** verstehen, die umgekehrt potenziell die Verhandlungsmacht der Belegschaft schwächt.

8.4 Beispiel Banken- und Finanzbranche

Dieses Fallbeispiel zeigt auf Basis eines Interviews mit einem Betriebsrat, wie eine Belegschaftsvertretung eines österreichischen Tochterunternehmens eines internationalen Bankkonzerns gleich zweimal hintereinander die Einführung invasiver cloudbasierter Personalverwaltungssysteme verhindern konnte – unter anderem weil durch ein gutes Verständnis technischer und rechtlicher Fragen eine starke Verhandlungsposition vorhanden war.

Personalverwaltungssystem zur Beurteilung von Beschäftigten. Vor einigen Jahren hat die Personalabteilung, die nicht im Tochterunternehmen, sondern in der Konzernzentrale angesiedelt ist, die Einführung einer neuen Personalverwaltungssoftware mit Funktionen zur Beurteilung von Beschäftigten vorangetrieben, die systematisch Daten zu Zielvereinbarungen, Einschätzungen von Vorgesetzten rund um Mitarbeitergespräche und Daten zu innerbetrieblicher Weiterbildung verarbeiten sollte. Das Produkt wurde in allen anderen Tochterunternehmen des Konzerns eingeführt. Im Betrieb des Interviews wurde die Zustimmung zur Einführung mit drei Argumenten verweigert:

- Die Personalabteilung des Konzerns konnte keinen überzeugenden Zweck für die Einführung darlegen.
- Das cloudbasierte System übertrage personenbezogene Daten an Server in den USA und könne in der EU datenschutzrechtlich nicht rechtskonform betrieben werden.[529]
- Das – im unteren Preissegment vergleichbarer Anwendungen angesiedelte – Produkt biete weder angemessene Funktionen zur Verhinderung des Zugriffs auf Beschäftigtendaten durch Unbefugte noch könne ausreichend überprüft werden, wer darauf zugegriffen hat und welche Auswertungen durchgeführt wurden.

Ein Jahr danach wurde dieses System konzernweit durch eine DSGVO-kompatible Anwendung aus der EU ersetzt. Auch hier war keine laufende Prüfung von Datenzugriffen und Auswertungen durch den Betriebsrat möglich. Die Lösung wurde daher im Betrieb des Interviewpartners wieder nicht eingeführt. Im restlichen Konzern läuft hingegen nun auch ein Modul im Testbetrieb, das gegenseitige Bewertungen zwischen ArbeitnehmerInnen ermöglicht.

Microsoft 365. Der Betriebsrat sieht aber die Notwendigkeit, andere mächtige cloudbasierte Systeme wie Microsoft 365 besser zu regeln – etwa mit einer schon lange angestrebten Rahmenbetriebsvereinbarung[530]. Diese wird allerdings von der Geschäftsführung verweigert – wegen dafür notwendige Aufarbeitung von über Jahre gewachsenen technischen Systemen und Datenverarbeitungspraktiken im Konzern, wie der Interviewpartner vermutet.

[529] Vgl. Datenübermittlung in die USA, Haslinger et al 2020, S. 261ff
[530] Vgl. Haslinger et al 2020, S. 231

8.5 Beispiel Plattform-Zustelldienst

Dieses Fallbeispiel basiert auf einem Interview mit einer ehemaligen BetriebsrätIn eines österreichischen Plattform-Zustelldiensts, der Teil eines internationalen Unternehmens ist, und der die Arbeitstätigkeiten von FahrradbotInnen in der Essenszustellung mittels Smartphone-App steuert und kontrolliert. Es bezieht sich auf den Zeitraum bis 2019.

Algorithmisches Management. Die FahrerInnen arbeiten in definierten Schichten und bekommen in dieser Zeit via App Zustellaufträge zugewiesen, müssen diese via App bestätigen und bekommen dann via App die Anweisung, zu einem Gastronomiebetrieb an einem bestimmten Ort zu fahren. Sie müssen dort via App bestätigen, welche Produkte sie abzuholen haben und laut erneuter Anweisung via App das Essen an die BestellerInnen ausliefern, wo die erfolgte Lieferung via App bestätigt werden muss. Wird danach nicht unmittelbar ein neuer Zustellauftrag zugewiesen, sollen die FahrerInnen warten, sich zum Startpunkt zurückbegeben oder in Regionen mit vielen Aufträgen fahren. Für die App wird das private Smartphone genutzt. Der Standort wird kontinuierlich mittels GPS erfasst. Die österreichische Betreiberfirma beschäftigt ArbeitnehmerInnen als reguläre Angestellte, als freie DienstnehmerInnen und als selbstständige SubunternehmerInnen. Dem Interviewpartner zu Folge funktioniert die App für alle Arten von Arbeitsverhältnissen nahezu gleich. Das zu Grunde liegende System wird global eingesetzt.

Automatisierte Leistungssteuerung und Sanktionen. Zustellaufträge können nicht abgelehnt, müssen aber bestätigt werden. Wird ein Schritt in der App nicht schnell genug bestätigt, wird die Schicht als Sanktion automatisiert beendet, auch wenn die FahrerInnen noch arbeitsbereit sind. Außerdem erfolgt ein wöchentliches Ranking der Beschäftigten nach ihrer Leistung. In die Reihung fließen die Anzahl der ausgelieferten Bestellungen pro Stunde sowie unerwünschtes Verhalten wie verspätete Zustellungen ein. Die bestgereihten vierzig FahrerInnen haben als erste die Möglichkeit, Schichten für die Folgewoche auszuwählen. Danach können die nächsten vierzig FahrerInnen ihre Dienstzeiten auswählen und so weiter. Die Leistungsbewertung führt damit zu Vorrechten bei der Wahl der Arbeitszeiten und wirkt sich zudem auf den Verdienst aus. Neben einem Sockelgehalt bestimmen bei Angestellten die zurückgelegten Kilometer und bei freien DienstnehmerInnen die Zahl der abgearbeiteten Zustellaufträge darüber, ob man im Monat auf einen Bruttolohn von etwas über acht Euro komme – oder auf elf Euro und darüber hinaus. Damit bestimmt zu einem gewissen Grad die Leistung über den Verdienst. Wenn nun höhere Leistung zu Vorrechten bei der Auswahl von Schichten mit hohen Bestellfrequenzen führt, verstärkt sich die Leistungsabhängigkeit des Verdiensts nochmals. Die kontinuierliche Ortung via GPS birgt eine zusätzliche Überwachungsdimension, ist für diese Art der Leistungskontrolle aber nicht entscheidend. In der Vergangenheit wurden bereits automatisierte Kündigungen durch das System ausgesprochen, dies sei aber vorerst zurückgenommen werden.

TeamleaderInnen, Kommunikation und unbezahlte Arbeitszeit. Die App übernimmt die Zeiterfassung. Die Arbeitszeit beginnt mit dem Einloggen und endet mit dem letzten Auftrag. Während der Schicht sind Pausen vorgesehen. Aufträge können allerdings in Pausen hineinfallen. Länger aktive FahrerInnen können zu sogenannten TeamleaderInnen und damit zu Führungskräften werden. Während diese früher Teams von 20 FahrerInnen geleitet haben, sind es nun über 100 Personen. Sie schulen neue FahrerInnen ein und verwalten Whatsapp-Gruppen für die Kommunikation in den Teams. Die Nutzung der externen Kommunikationsplattform Whatsapp hat für den Betriebsrat den Vorteil, dass die KollegInnen wegen der Sichtbarkeit ihrer Telefonnummern erreichbar sind. Während Zustellaufträge früher durch DisponentInnen in der Berliner Konzernzentrale zugewiesen wurden, erfolgt das heute automatisiert. Deren Rolle ist nun auf die Behandlung von Problemen wie Fehler oder Unfälle reduziert. Andere Formen der Kommunikation mit dem Arbeitgeber – etwa über Krankenstände, Urlaube, Fragen der Lohnverrechnung oder Sanktionen wie die Beendigung von Schichten oder gar Sperrungen – erfolgen via E-Mail und Ticketing-System

und außerhalb der Arbeitszeit. Kommunikationsbedarf ergibt sich auch durch die Fehleranfälligkeit der App. Es kommt häufig zu Updates der App, die sie vereinzelt unbrauchbar gemacht haben. Besprechungen mit TeamleaderInnen wurden im Lauf der Zeit nahezu ganz wegrationalisiert, finden aber ebenfalls in der Freizeit statt.

Der Interviewpartner vermutet, dass die Datensammlung ein wesentlicher Teil des Geschäftsmodells der Plattform darstellt. Mittelfristig wird erwartet, dass Automatisierung und Zentralisierung weiter zunehmen. In Ländern wie Spanien oder in der Ukraine gäbe es gar keine regionalen Tochterbetriebe mehr, sondern nur mehr die App und Selbstständige, die sie nutzen.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Adler-Bell, Sam und Miller, Michelle (2018): The Datafication of Employment. Report, Century Foundation, 19.12.2018. Online: https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge

Ajunwa, Ifeoma; Crawford, Kate; Schultz, Jason (2017). Limitless worker surveillance. California Law Review. 105. 735-776. DOI: 10.15779/Z38BR8MF94

Angerler, Eva; Komar, Andrea; Spitz, Verena; Spinka, Fritz; Wolff, Helmut (2018): Zielvereinbarungen. Kennzahlen, Konkurrenz, Kostendruck. Marktorientierte Leistungssteuerung im Betrieb. Broschüre der GPA-djp Abteilung Arbeit & Technik, Mai 2018

Angerler, Eva; Lohmeyer, Michael; Peissl, Walter; Spinka, Fritz (2018b): Arbeitswelt 4.1 - Aspekte der Digitalisierung. Worauf BetriebsrätInnen achten sollen und wie sie die innerbetriebliche Digitalisierung mitgestalten können. Broschüre der GPA-djp Abteilung Arbeit & Technik, Mai 2018. Online: https://www.gpa.at/content/dam/gpa/downloads/themen/datenschutz/Arbeitswelt%204.1.pdf

Baader, Galina (2019): Aufdeckung von Fraud im Einkaufsprozess durch die Kombination des Red Flag Ansatzes mit Process Mining. Dissertation, Technische Universität München, Fakultät für Informatik, 2019. Online: http://mediatum.ub.tum.de/doc/1459272/130413.pdf

Ball, Kirstie (2010): Workplace Surveillance: An Overview. Labor History, 51(1) pp. 87–106. DOI: 10.1080/00236561003654776

Banks, David A. (2020): Automatic for the Bosses. Workers may be more affected by robots taking their bosses' jobs than their own. Reallifemag, 9.7.2020. Online: https://reallifemag.com/automatic-for-the-bosses/

Besner, Linda (2018). Ambient Cruelty. The ability to ruin a stranger's life is a feature, not a bug of consumer rating systems. Real Life Magazine, 17.12.2018. Online: https://reallifemag.com/ambient-cruelty/

BInBDI, Berliner Beauftragter für Datenschutz und Informationsfreiheit (2021): Datenschutz und Informationsfreiheit. Jahresbericht 2020. 8.4.2021, S. 123-126. Online: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2020-Web.pdf

Bogen, Miranda und Rieke, Aaron (2018): Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias. Upturn, December 2018. Online: https://www.upturn.org/reports/2018/hiring-algorithms/

Bröckling, Ulrich (2003): Das demokratisierte Panopticon. Subjektivierung und Kontrolle im 360-Feedback. In: Honneth, Axel/Saar, Martin (Hrsg.), Michel Foucault. Zwischenbilanz einer Rezeption. Frankfurter Foucault-Konferenz 2001. Frankfurt/Main: Suhrkamp, S. 77–93.

Brustein, Joshua (2019): Warehouses Are Tracking Workers' Every Muscle Movement. Bloomberg, 5.11.2019. Online: https://www.bloomberg.com/news/articles/2019-11-05/am-i-being-tracked-at-work-plenty-of-warehouse-workers-are

Cannon, Camilla (2019): Recorded for Quality Assurance. The datafication of affect in the call-center industry. Real Life Magazine, 19.9.2019. Online: https://reallifemag.com/recorded-for-quality-assurance/

Christl, Wolfie (2017): Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. Report by Cracked Labs, June 2017. Online: http://crackedlabs.org/en/corporate-surveillance

Christl, Wolfie und Spiekermann, Sarah (2016): Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy. Facultas, Vienna 2016. Online: http://crackedlabs.org/en/networksofcontrol

Claes, Jan und Poels, Geert (2014): Merging event logs for process mining: A rule based merging method and rule suggestion algorithm. Expert Syst. Appl. 41, 16 (November 2014), 7291–7306. DOI: 10.1016/j.eswa.2014.06.012

Cyphers, Bennett und Gullojune, Karen (2020): Inside the Invasive, Secretive "Bossware" Tracking Workers. Electronic Frontier Foundation, 30.6.2020. Online: https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers

Däubler, Wolfgang (2017): Gläserne Belegschaften. Das Handbuch zum Beschäftigtendatenschutz. 7., umfassend überarbeitete und aktualisierte Auflage 2017. Bund Verlag.

de Barros Lima, Â. (2020): A web-based application to integrate building management system sensor data and building information model data to support facility management tasks. Master thesis. Online: https://research.tue.nl/files/165165631/Barros_Lima_1294814.pdf

De Stefano, Valerio (2019): 'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection. Comparative Labor Law & Policy Journal, Vol. 41, No. 1, 2019, DOI: 10.2139/ssrn.3178233

De Stefano, Valerio (2020): Algorithmic Bosses and What to Do About Them: Automation, Artificial Intelligence and Labour Protection. In: Marino D., Monaca M. (Hrsg): Economic and Policy Implications of Artificial Intelligence. Studies in Systems, Decision and Control, vol 288. Springer, Cham. DOI: 10.1007/978-3-030-45340-4_7

Del Rey, Jason (2019): How robots are transforming Amazon warehouse jobs — for better and worse. Vox, 11.12.2019. Online: https://www.vox.com/recode/2019/12/11/20982652/robots-amazon-warehouse-jobs-automation

Drumm, Hans Jürgen (2008): Personalwirtschaft, Springer-Verlag Berlin Heidelberg, 2008

Dzieza, Josh (2020): How hard will the robots make us work? The Verge, 27.2.2020: Online: https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon

Eckert, Claudia (2013): IT-Sicherheit: Konzepte - Verfahren - Protokolle. 8. Auflage. Oldenbourg, 2013.

Edwards, Lilian; Martin, Laura; Henderson, Tristan (2018): Employee Surveillance: The Road to Surveillance is Paved with Good Intentions. 18. August 2018). DOI: 10.2139/ssrn.3234382

Evans, Will (2019): Behind the Smiles. Amazon's internal injury records expose the true toll of its relentless drive for speed. Reveal News, 25.11.2019. Online: https://revealnews.org/article/behind-the-smiles/

Evans, Will (2019b): Verwarnungen mit Produktivitätswerten für einen Amazon-Beschäftigten. Dokumente publiziert im Rahmen der Reportage "Behind the Smiles" von Reveal News, 25.11.2019. Online: https://revealnews.org/wp-content/uploads/2019/11/Parker-Knight-productivity-report.pdf

Evans, Will (2020): How Amazon hid its safety crisis. Reveal News, 29.9.2020. Online: https://revealnews.org/article/how-amazon-hid-its-safety-crisis/

Fan, Ryan (2020): Here's What It's Like to Work in an Amazon Warehouse Right Now. OneZero, 20.8.2020. Online: https://onezero.medium.com/heres-what-it-s-like-to-work-in-an-amazon-warehouse-right-now-e7f8590264b5

Faßauer, Gabriele (2008): Arbeitsleistung, Identität und Markt. Eine Analyse marktförmiger Leistungssteuerung in Arbeitsorganisationen. VS Verlag für Sozialwissenschaften, 2008.

Ferreira, A.T.; Araújo, A.M.; Fernandes, S.; Miguel, I.C. (2017): Gamification in the Workplace: A Systematic Literature Review. In: Rocha Á., Correia A., Adeli H., Reis L., Costanzo S. (eds) Recent Advances in Information Systems and Technologies. WorldCIST 2017. Advances in Intelligent Systems and Computing, vol 571. Springer, Cham. DOI: 10.1007/978-3-319-56541-5_29

FIPA / B.C. Freedom of Information and Privacy Association (2015): The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology. March 2015. Online: https://fipa.bc.ca/wp-content/uploads/2018/01/CC_report_lite.pdf

Fleenor, John W.; Prince, Jeffrey M. (1997): Using 360-degree feedback in organizations. Greensboro, North Carolina (US): Center for Creative Leadership. Online: https://www.researchgate.net/publication/317284725_Using_360-degree_feedback_in_organizations

Fried, Louis (1994). Information security and new technology. Potential Threats and Solutions. Information Systems Management, 11:3, 57-63, DOI: 10.1080/07399019408964654

Friedrich, Sebastian und Jolmes, Johannes (2020): Amazon: Der Vorgesetzte sieht alles. NDR, 15.10.2020. Online: https://daserste.ndr.de/panorama/archiv/2020/Amazon-Der-Vorgesetzte-sieht-alles,amazon430.html

Fritsch, Clara (2012): Kannst du's nicht messen, kannst du's vergessen. Vom Sinn und Unsinn betrieblicher Kennzahlen. Broschüre der GPA-djp Abteilung Arbeit & Technik, März 2012

Fritsch, Clara (2017): Sozial? Digital? Oder von beidem ein bisschen? Personalentwicklung in der digitalen Arbeitswelt. Broschüre der GPA-djp Abteilung Arbeit & Technik, März 2017. Online: https://www.gpa.at/themen/digitalisierung/sozial--digital--oder-von-beidem-ein-bisschen-

Fritsch, Clara (2020): Der Datenschutz im Betrieb. Präsentationsfolien für Seminar der GPA-djp. Online: https://bildung.gpa-djp.at/files/2019/04/Clara-Fritsch-Der-Datenschutz-im-Betrieb-01-2020.pdf

Fritsch, Clara (2020b): Whistleblowing. Wenn ArbeitnehmerInnen Missstände aufdecken: Online: https://www.gpa.at/content/dam/gpa/downloads/themen/datenschutz/Whistleblowing.pdf

Fritsch, Clara (2021): Die wunderbare Welt von Microsoft und wie sie der Betriebsrat mitgestalten kann. Broschüre der GPA-djp Abteilung Arbeit & Technik, Februar 2021. Online: https://www.gpa.at/content/dam/gpa/downloads/themen/digitalisierung/Die_wunderbare_Welt_von_Microsoft.pdf

Frühbrodt, Timo (2018): Überwachung von Arbeitnehmern im Betrieb. Eine Technikfolgenabschätzung digitalisierter Informations- und Kommunikationssysteme, Bachelorarbeit Informatik, Universität Hamburg 2018

Gabrielle, Vincent (2018): The dark side of gamifying work. Fast Company, 1.11.2018. Online: https://www.fastcompany.com/90260703/the-dark-side-of-gamifying-work

Gilbreth, Frank Bunker und Gilbreth, Lillian Moller (1919). Fatigue Study, the Elimination of Humanity's Greatest Unnecessary Waste: A First Step in Motion Study. The Macmillan Company, New York.

Goldenberg, Rachel (2019): Perils of Amazon robots that hire, fire. The Lawyer's Daily, LexisNexis Canada. Online: https://www.lexisnexis.ca/en-ca/ihc/2019-06/perils-of-amazon-robots-that-hire-fire.page

GPA-djp (2012): Grenzenlose Freiheit? Datenschutz und Überwachung im Außen- und Mobildienst. Broschüre der GPA-djp Interessensgemeinschaften work@external, August 2012.

Greenfield, Rebecca (2018): Your Raise Is Now Based on Next Year's Performance. Bloomberg, 9.12.2018. Online: https://www.bloomberg.com/news/articles/2018-07-09/your-raise-is-now-based-on-next-year-s-performance

Grill, Gabriel und Steiner, Alexander (2018): Arbeitskämpfe auf Social Media: Zwischen Streikorganisation und Streikvorhersage. Netzpolitik, 3.9.2018. Online: https://netzpolitik.org/2018/digitale-arbeitskaempfe-auf-social-media-zwischen-streikorganisation-und-streikvorhersage

Gronau, Norbert (2010): Enterprise Resource Planning. Architektur, Funktionen und Management von ERP-Systemen. Oldenbourg Verlag München

Guendelsberger, Emily (2019): I Worked at an Amazon Fulfillment Center; They Treat Workers Like Robots. Time Magazine, 29.7.2019. Online: https://time.com/5629233/amazon-warehouse-employee-treatment-robots/

Gurley, Lauren Kaori (2021): Amazon Drivers Are Instructed to Drive Recklessly to Meet Delivery Quotas. Vice, 6.5.2021. Online: https://www.vice.com/en/article/xgxx54/amazon-drivers-are-instructed-to-drive-recklessly-to-meet-delivery-quotas

Gurley, Lauren Kaori (2021): Amazon's Cost Saving Routing Algorithm Makes Drivers Walk Into Traffic. Vice, 2.6.2021. Online: https://www.vice.com/en/article/5db95k/amazons-cost-saving-routing-algorithm-makes-drivers-walk-into-traffic

Gurley, Lauren und Cox, Joseph (2020): Inside Amazon's Secret Program to Spy On Workers' Private Facebook Groups. Vice, 2.9.2020. Online: https://www.vice.com/en/article/3azegw/amazon-is-spying-on-its-workers-in-closed-facebook-groups-internal-reports-show

Gürses, Seda und Van Hoboken, Joris (2017): Privacy After the Agile Turn. In: Jules Polonetsky, Omer Tene, and Evan Selinger (2017) (Hrsg): Cambridge Handbook of Consumer Privacy. Cambridge University Press, 2017. Online: https://osf.io/ufdvb/

Hanley, Daniel A. und Hubbard, Sally (2020): Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing Worker Power. Report, Open Markets Institute, September 2020. Online: https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/5f4cffea23958d79eae1ab23/1598881772432/Amazon_Report_Final.pdf

Haslinger, Susanne; Krisch, Andreas; Riesenecker-Caba, Thomas (2020): Beschäftigtendatenschutz. Handbuch für die betriebliche Praxis. 2. Auflage 2020. ÖGB Verlag.

Höller, Heinz-Peter und Wedde, Peter (2018): Die Vermessung der Belegschaft. Mining the Enterprise Social Graph. Hans-Böckler-Stiftung, Mitbestimmungspraxis Nr. 10, Januar 2018. Online: https://www.boeckler.de/pdf/p_mbf_praxis_2018_010.pdf

Huselid, Mark (2018): The science and practice of workforce analytics: Introduction to the HRM special issue. Human Resource Management. DOI: 57. 679-684. 10.1002/hrm.21916

Ivanova, Mirela; Bronowicka, Joanna; Kocher, Eva; Degner, Anne: Foodora and Deliveroo: The App as a Boss? Working Paper der Forschungsförderung der Hans-Böckler-Stiftung Nr. 107, Dezember 2018. Online: https://www.boeckler.de/de/faust-detail.htm?sync_id=8278

Jabsky, Marina und Obernauer, Charlene (2019): Time Off Task. Pressure, Pain, and Productivity at Amazon. New York Committee for Occupational Safety and Health, Online: https://media.business-humanrights.org/media/documents/files/documents/amazon_worker_report_10_15.pdf

Kavanagh, Michael J. und Johnson, Richard David (Hrsg.) (2018). Human Resource Information Systems: Basics, Applications, and Future Directions. SAGE Publications, Fourth Edition 2018.

Kayhan, V.O., Chen, Z.., French, K.A. et al (2018): How honest are the signals? A protocol for validating wearable sensors. Behav Res 50, 57–83. DOI: 10.3758/s13428-017-1005-4

Kellogg, Katherine C.; Valentine, Melissa A.; Christin, Angèle (2020): Algorithms at Work: The New Contested Terrain of Control. ANNALS, 14, 366–410, DOI: 10.5465/annals.2018.0174

Kiesche, Eberhard und Wilke, Matthias (2012): Neue Überwachungsformen in Call-Centern. Computer und Arbeit, 2012. Online: https://www.dtb-beratung.de/fileadmin/veroeffenlichungen/2018/Kiesche_Wilke_12_04_CuAWeb_Stimmungsanalyse.pdf

Koops, Bert-Jaap (2021): The concept of function creep, Law, Innovation and Technology, 13:1, 29-56, DOI: 10.1080/17579961.2021.1898299

Krause, Rüdiger (2017): Digitalisierung und Beschäftigtendatenschutz. Forschungsbericht 482, Bundesministerium für Arbeit und Soziales, April 2017. Online: https://www.bmas.de/SharedDocs/Downloads/DE/Publikationen/Forschungsberichte/fb482-digitalisierung-und-beschaeftigtendatenschutz.html

Kristiansen, Kristian Helbo; Valeur-Meller, Mathias A.; Dombrowski, Lynn; Holten Moller, Naja L. (2018): Accountability in the Blue-Collar Data-Driven Workplace. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18). Association for Computing Machinery, New York, NY, USA, Paper 332, 1–12. DOI: 10.1145/3173574.3173906

Kurbel, Karl (2013): Enterprise Resource Planning and Supply Chain Management: Functions, Business Processes and Software for Manufacturing Companies. Springer, Berlin Heidelberg.

Lecher, Colin (2019): How Amazon automatically tracks and fires warehouse workers for 'productivity'. The Verge, 25.4.2019. Online: https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

Leopold, Nils; Meints, Martin (2008): Profiling in Employment Situations (Fraud). In: Hildebrandt M., Gutwirth S. (Hrsg): Profiling the European Citizen. Springer, Dordrecht.

Levy, Karen E. C. (2015): The Contexts of Control: Information, Power, and Truck-Driving Work. The Information Society, 31:2, 160-174, DOI: 10.1080/01972243.2015.998105

Levy, Karen und Barocas, Solon (2018): Privacy at the Margins| Refractive Surveillance: Monitoring Customers to Manage Workers. International Journal Of Communication, 12, 23. https://ijoc.org/index.php/ijoc/article/view/7041

Loi, Michele (2021): People Analytics muss den Menschen zugutekommen. Eine ethische Analyse datengesteuerter algorithmischer Systeme im Personalmanagement. Hans Böckler Stiftung, Study 450, April 2021. Online: https://algorithmwatch.org/de/wp-content/uploads/2021/05/p_study_hbs_450_loi.pdf

Lyon, David (2003): Surveillance as social sorting: Computer codes and mobile bodies. In: Lyon, D. (Ed.): Surveillance as social sorting: Privacy, risk, and digital discrimination. Routledge, London, New York.

Lyon, David (2007): Surveillance Studies: An Overview. Polity Press, Cambridge 2007

Martineau, Paris und Di Stefano, Mark (2021): Amazon Expands Effort to 'Gamify' Warehouse Work. The Information, 15.3.2021. Online: https://www.theinformation.com/articles/amazon-expands-effort-to-gamify-warehouse-work

Mateescu, Alexandra und Nguyen, Aiha (2019): Workplace Monitoring & Surveillance. Data & Society, Februar 2019. Online: https://datasociety.net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf

Mateescu, Alexandra und Nguyen, Aiha (2019b): Algorithmic Management in the Workplace. Data & Society, Februar 2019. Online: https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf

Metcalf, Jacob (2018): When verification is also surveillance. EVV devices could intrusively track Medicaid recipients. Data & Society, 27.2.2018. Online: https://points.datasociety.net/when-verification-is-also-surveillance-21edb6c12cc9

Moore, Phoebe V. (2018): The Quantified Self in Precarity: Work, Technology and What Counts. London, Routledge.

Moore, Phoebe V.; Upchurch, Martin; Whittaker, Xanthe (2018b) (Hrsg): Humans and Machines at Work. Monitoring, Surveillance and Automation in Contemporary Capitalism. Palgrave Macmillan, 2018.

Mormann, Hannah (2016): Das Projekt SAP. Zur Organisationssoziologie betriebswirtschaftlicher Standardsoftware. Transcript Verlag, Bielefeld.

Murphy, Kevin R. (2020): Performance evaluation will not die, but it should. Hum Resour Manag J. 2020; 30: 13– 31. DOI: 10.1111/1748-8583.12259

Neupane, K.; Haddad, R.; Chen, L. (2018): Next Generation Firewall for Network Security: A Survey. SoutheastCon 2018, 2018, pp. 1-6, DOI: 10.1109/SECON.2018.8478973

Newman, Nathan (2016): UnMarginalizing Workers: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace. August 5, 2016. DOI: 10.2139/ssrn.2819142

Norwegian Consumer Council (2020): Out of Control. How consumers are exploited by the online advertising industry. 14.1.2020. Online: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/

Office of Technology Assessment (1987), The Electronic Supervisor: New Technology, New Tensions, OTA-CIT-333, U.S. Congress, Washington DC, September 1987. Online: https://ota.fas.org/reports/8708.pdf

Oguntala, George; Abd-Alhameed, Raed; Jones, Stephen; Noras, James; Patwary, Mohammad; Rodriguez, Jonathan (2018): Indoor location identification technologies for real-time IoT-based applications: An inclusive survey, Computer Science Review, Volume 30, 2018, Pages 55-79, DOI: 10.1016/j.cosrev.2018.09.001

Olguín, Daniel; Gloor, Peter; Pentland, Alex. (2009): Capturing Individual and Group Behavior with Wearable Sensors. AAAI Spring Symposium - Technical Report. 68-74. Online: https://hd.media.mit.edu/tech-reports/TR-626.pdf

Ongweso Jr, Edward (2021): The leaked pamphlet asks workers to "monitor your urine color" and alter their lifestyle so they don't get injured on the job. Vice, 1.6.2021. Online: https://www.vice.com/en/article/epnvp7/amazon-calls-warehouse-workers-industrial-athletes-in-leaked-wellness-pamphlet

Organise (2018): Amazon: What's It like Where You Work? Amazon Warehouse Employee survey, London. Online: https://static1.squarespace.com/static/5a3af3e22aeba594ad56d8cb/t/5ad098b3562fa7b8c90d5e1b/1523620020369/Amazon+Warehouse+Staff+Survey+Results.pdf

Pasquale, Frank (2019): Quantifying Love. Reputational currency, like China's Social Credit Score, rebrands repression as rational nudging. And these algorithmic governance models are spreading. Boston Review, 4.4.2019. Online: http://bostonreview.net/print-issues-politics/frank-pasquale-quantifying-love

Peissl, Walter (2007): Die Bedrohung von Privacy. Ein grenzüberschreitendes Phänomen und seine Behandlung im Kontext internationaler Technikfolgenabschätzung. In: Bora, Alfons; Bröchler, Stephan; Decker, Michael (Hrsg): Technology Assessment in der Weltgesellschaft, edition sigma 2007, S. 277 - 288

Pilarski, B.; Decker, J.; Klein, M., Tornack, C.; Schumann, Matthias (2016): IT-gestütztes Human Capital Management. HMD 53, 755–770, 2016. DOI: 10.1365/s40702-016-0262-5

Poncin, W.; Serebrenik, A.; Brand, M. v. d. (2011): Process Mining Software Repositories. 15th European Conference on Software Maintenance and Reengineering, 2011, pp. 5-14, DOI: 10.1109/CSMR.2011.5

Posner, Miriam (2019): The Software That Shapes Workers' Lives. The New Yorker, 13.9.2019. Online: https://www.newyorker.com/science/elements/the-software-that-shapes-workers-lives

Prassl, Jeremias (2018): Humans as a Service: The Promise and Perils of Work in the Gig Economy. Oxford University Press.

PressProgress (2020): Amazon's Hi-Tech System for Tracking its Canadian Workers Poses a 'Public Health Hazard', Experts Warn. 23.4.2020. Online: https://pressprogress.ca/amazons-hi-tech-system-for-tracking-its-canadian-workers-poses-a-public-health-hazard-experts-warn/

Ram, P.; Rodriguez, P.; Oivo, M. (2018): Software Process Measurement and Related Challenges in Agile Software Development: A Multiple Case Study. In: Kuhrmann M. et al. (Hrsg): Product-Focused Software Process Improvement. PROFES 2018. Lecture Notes in Computer Science, vol 11271. Springer, Cham. DOI: 10.1007/978-3-030-03673-7_20

Reissner, Gert-Peter (2003): „Performance-Management"-Konzepte und betriebliche Mitbestimmung, DRdA 2003. Online: https://www.drda.at/api/v1/drda/article/286_DRDA_3/pdf

Riesenecker-Caba, Thomas (2020): Technikgestaltung und Datenschutz. Präsentationsfolien für Seminar der GPA-djp. Online: https://bildung.gpa-djp.at/files/2019/04/Thomas-Riesenecker-Caba-Technikgestaltung-und-Datenschutz-01-2020.pdf

Riesenecker-Caba, Thomas und Astleithner Franz (2021): Verarbeitung personenbezogener Beschäftigtendaten und Grenzen betrieblicher Mitbestimmung in einer digitalisierten Arbeitswelt. FORBA, Mai 2021. Online: https://www.forba.at/wp-content/uploads/2021/06/Verarbeitung-persbez-Daten-und-MitbestimmungFORBA-Bericht2021_DigiFonds.pdf

Riesenecker-Caba, Thomas und Bauernfeind, Alfons (2011): Verwendung personenbezogener Daten und Grenzen betrieblicher Mitbestimmung: Datenschutz in der Arbeitswelt. Studie der FORBA im Auftrag der AK Wien und Fachgewerkschaften, August 2011. Online: https://www.forba.at/wp-content/uploads/files/557-Sozialpolitik_in_Diskussion_12.pdf

Risak, Martin und Lutz, Doris (2017) (Hrsg): Arbeit in der Gig-Economy. Rechtsfragen neuer Arbeitsformen in Crowd und Cloud. ÖGB Verlag, 2017. Website zum Buch: https://www.gig-economy.at/

Rogoway, Mike (2020): Major Tech Company Using Facial Recognition to ID Workers. The Oregonian, 11.3.2020. Online: https://www.govtech.com/public-safety/major-tech-company-using-facial-recognition-to-id-workers.html

Rosenbaum, Eric (2019): IBM artificial intelligence can predict with 95% accuracy which workers are about to quit their jobs. CNBC, 3.4.2019. Online: https://www.cnbc.com/2019/04/03/ibm-ai-can-predict-with-95-percent-accuracy-which-employees-will-quit.html

Rosenblat, Alex (2019): Uberland: How Algorithms Are Rewriting the Rules of Work. University of California Press, 2019

Rosenblat, Alex und Stark, Luke (2016): Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers. International Journal of Communication 10(2016), 3758–3784. https://ijoc.org/index.php/ijoc/article/view/4892

Rosenkrantz, Holly (2019): Performance Reviews. Sage Business Researcher, Issue: Performance Reviews. Online: https://businessresearcher.sagepub.com/sbr-2022-109219-2918905/20190311/performance-reviews?download=pdf

Rossiter, Ned (2016): Software, Infrastructure, Labor. A Media Theory of Logistical Nightmares. Routledge.

Sánchez-Monedero, Javier und Dencik, Lina (2019): The datafication of the workplace. Working Paper. Cardiff, Data Justice Project, 2019. Online: https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-The-datafication-of-the-workplace.pdf

SAP (2017): Total Workforce Performance Management. SAP White Paper, 2017. Online: https://assets.cdn.sap.com/sap-com/docs/2017/09/740a8490-d17c-0010-82c7-eda71af511fa.pdf

SAP (2018): SAP SuccessFactors Performance and Goals. Technical and Functional Specifications. Broschüre, 2018. Online: https://assets.cdn.sap.com/agreements/product-policy/css/service-specifications/sap-successfactors-performance-and-goals-english-v2-2019.pdf

Schafheitle, Simon; Weibel, Antoinette; Ebert, Isabel; Kasper, Gabriel; Schank, Christoph; Leicht-Deobald, Ulrich (2020): No Stone Left Unturned? Toward a Framework for the Impact of Datafication Technologies on Organizational Control. AMD, 6, 455–487, DOI: 10.5465/amd.2019.0002

Schörpf, Philip; Astleithner, Franz; Schönauer, Annika; Flecker, Jörg (2020): Entwicklungstrends Digitaler Arbeit II. FORBA Projektbericht im Auftrag der Arbeiterkammer Wien, September 2020. Online: https://wien.arbeiterkammer.at/service/studien/digitalerwandel/Entwicklungstrends_Digitaler_Arbeit_II.html

Schörpf, Philip; Schönauer, Annika; Flecker, Jörg (2018): Entwicklungstrends digitaler Arbeit. FORBA Forschungsbericht im Auftrag der Arbeiterkammer Wien, 2018. Online: https://wien.arbeiterkammer.at/service/studien/digitalerwandel/Entwicklungstrends_digitaler_Arbeit.html

Selig, Henny (2017): Continuous Event Log Extraction for Process Mining. Degree project information and communication in technology, KTH Royal Institute of Technology, Stockholm. Online: https://www.diva-portal.org/smash/get/diva2:1119380/FULLTEXT01.pdf

Sen, Arun und Sinha, Atish P. (2005): A comparison of data warehousing methodologies. Commun. ACM 48, 3 (March 2005), 79–84. DOI: 10.1145/1047671.1047673

Sharma, A.; Sharma, S., Dave, M. (2015): Identity and access management - a comprehensive study. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 1481-1485, DOI: 10.1109/ICGCIoT.2015.7380701

Shehab, E.M.; Sharp, M.W.; Supramaniam, L.; Spedding, T.A. (2004): Enterprise resource planning. Business Process Management Journal, 10(4), 359–386. DOI: 10.1108/14637150410548056

Silverman, Jacob (2016). Big Bother Is Watching. Why Slack is designed to never give you any. The Baffler, December 2016. Online: https://thebaffler.com/salvos/big-bother-slack-silverman

Simpson, William R. und Foltz, Kevin E. (2018): Enterprise End-point Device Management. Proceedings of The World Congress on Engineering 2018, 4-6 July, 2018, London, U.K., pp331-336. Online: http://www.iaeng.org/publication/WCE2018/WCE2018_pp331-336.pdf

Sin, Katrina und Muthu, Loganathan (2015): Application of Big data in education data mining and learning analytics - a literature review. ICTACT Journal on Soft Computing. 05. 1035-1049. 10.21917/ijsc.2015.0145

Sommer, Katrin (2014): Personalinformationssysteme im radikalen Wandel. Successfactors von SAP – das schwarze Mitarbeiterdatenloch. Computer und Arbeit, 6/2014. Online: https://cdn.website-editor.net/a50dcf1494a74939ade1f7ea0afeb0ce/files/uploaded/Personalsysteme%2520im%2520radikalen%2520Wandel.pdf

Sommer, Katrin (2017): Herausforderung Workday. Computer und Arbeit, 2/2017. Online: https://cdn.website-editor.net/a50dcf1494a74939ade1f7ea0afeb0ce/files/uploaded/Herausforderung%2520Workday.pdf

Sommmer, Katrin (2018): Personal 4.0 mit SAP SuccessFactors, Workday HCM & Co. Mitbestimmungsrechte des Betriebsrats. Whitepaper, Technologieberatungsstelle beim DGB NRW, April 2018. Online: https://www.tbs-nrw.de/fileadmin/Shop/Broschuren_PDF/successfactors_personal_4_0.pdf

Staab, Philipp und Geschke, Sascha-Christopher (2019): Ratings als arbeitspolitisches Konfliktfeld. Das Beispiel Zalando. Study / edition der Hans-Böckler-Stiftung, vol. 429, October 2019. Online: https://www.researchgate.net/publication/336513640_Ratings_als_Arbeitspolitisches_Konfliktfeld_Das_Beispiel_Zalando_Study_der_Hans-Bockler-Stiftung_Nr_429

Staab, Philipp und Geschke, Sascha-Christopher (2020): Ratings als arbeitspolitisches Konfliktfeld. Das Beispiel Zalando. Study / edition der Hans-Böckler-Stiftung, vol. 429, März 2020. Online: https://www.boeckler.de/de/faust-detail.htm?sync_id=HBS-007864

Staab, Philipp; Nachtwey, Oliver (2016): Die Digitalisierung der Dienstleistungsarbeit. Aus Politik und Zeitgeschichte 66 (18/19), S. 24-31. Online: https://www.bpb.de/apuz/225692/die-digitalisierung-der-dienstleistungsarbeit?p=all

Stern, Sandra; Schönauer, Annika; Holtgrewe, Ursula (2010) (Hrsg): Service um jeden Preis? Arbeiten im Callcenter. Erfahrungsberichte und Organisationsmöglichkeiten. ÖGB Verlag, Wien, 2010.

Sulzbacher, Markus (2020): Von Lernsieg bis Apple: Online-Reviews setzen Menschen unter massiven Druck. Der Standard, 10.3.2020. Online: https://www.derstandard.at/story/2000115538692/von-lernsieg-bis-apple-online-reviews-setzen-menschen-unter-massiven

Taylor, Frederick (1911): The Principles of Scientific Management. Harper & Brothers, New York.

Taylor, Linnet; Floridi, Luciano; van der Sloot, Bart (Hrsg) (2017). Group Privacy. New Challenges of Data Technologies. Springer, 2017

Tippett, Elizabeth; Charlotte S. Alexander; Eigen, Zev J. (2018): When Timekeeping Software Undermines Compliance. Yale Journal of Law and Technology 19, no. 1, January 14, 2018. Online: https://digitalcommons.law.yale.edu/yjolt/vol19/iss1/1

United Workers Union (2020): Technology and Power. Understanding issues of insecure work and technological change in Australian workplaces. August 2020. Online: https://www.unitedworkers.org.au/wp-content/uploads/2020/08/Technology-and-Power-UWU-Submission.pdf

Vacca, John R. (2017) (Hrsg): Computer and Information Security Handbook. Third Edition. Morgan Kaufmann, 2017

Van Oort, Madison (2019): The Emotional Labor of Surveillance: Digital Control in Fast Fashion Retail. Critical Sociology, 45(7–8), pp. 1167–1179. DOI: 10.1177/0896920518778087

Van Oort, Madison (2019b): Employing the Carceral Imaginary: An Ethnography of Worker Surveillance in the Retail Industry. In: Ruha Benjamin (Hrsg): Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life, Duke University Press 2019.

Voigt, Hans Christian (2021): Digitale Überwachung und Kontrolle in österreichischen Betrieben. Bericht über eine explorative Untersuchung mit Fallbeispielen auf Basis von Interviews. Eine Studie von Cracked Labs, Wien, September 2021. Online: https://crackedlabs.org/dl/CrackedLabs_Voigt_UeberwachungArbeitsplatzAT.pdf

Wedde, Peter (2017): Beschäftigtendatenschutz in der digitalisierten Welt. Wiso Diskurs 09/2017, Friedrich-Ebert-Stiftung. Online: http://library.fes.de/pdf-files/wiso/13578.pdf

Wedde, Peter (2020): Automatisierung im Personalmanagement – arbeitsrechtliche Aspekte und Beschäftigtendatenschutz. AlgorithmWatch, 2.3.2020. Online: https://algorithmwatch.org/de/wp-content/uploads/2020/03/AlgorithmWatch_AutoHR_Gutachten_Arbeitsrecht_Datenschutz_Wedde_2020.pdf

Williams et al (2018): Stable scheduling increases productivity and sales: The Stable Scheduling Study. University of California Hastings College of the Law, University of Chicago School of Social Service Administration, UNC Kenan-Flagler Business School. Online: https://worklifelaw.org/publications/Stable-Scheduling-Study-Report.pdf

Wood, Alex J. (2020): Despotism on Demand. How Power Operates in the Flexible Workplace. ILR Press.

Wright, Greg (2015): Employee Feedback Apps on the Rise. Using Technology for Real-Time Employee Performance Reviews. SHRM, 14.9.2015. Online: https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/employee-feedback-apps.aspx

Wu, Lynn; Waber, Benjamin N.; Aral, Sinan; Brynjolfsson, Erik; Pentland, Alex (2008): Mining Face-to-Face Interaction Networks using Sociometric Badges: Predicting Productivity in an IT Configuration Task. 7. Mai 2008. Online: https://ssrn.com/abstract=1130251

Yamin, Muhammad Mudassar und Katt, Basel (2019): Mobile device management (MDM) technologies, issues and challenges. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP '19). Association for Computing Machinery, New York, NY, USA, 143–147. DOI: 10.1145/3309074.3309103