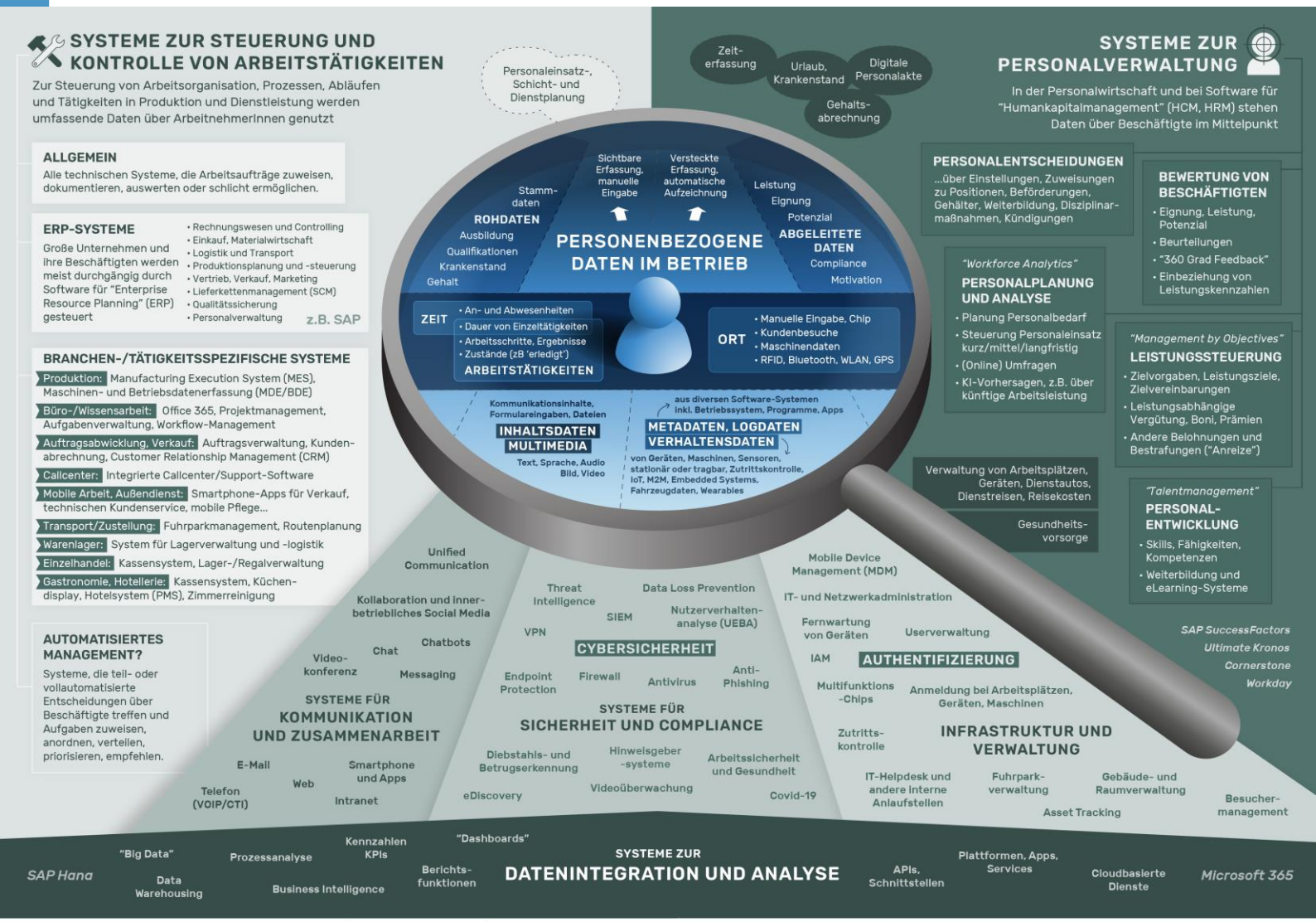
Landkarte betrieblicher Datenpraktiken und Systeme

Ein kompakter Überblick über Systeme, die personenbezogene Daten über Beschäftigte verarbeiten

Wolfie Christl, Cracked Labs (4/2023) | © CC BY-SA 4.0

Die Landkarte gibt einen systematischen Überblick darüber, welche Arten technischer Systeme im Betrieb personenbezogene Daten über Beschäftigte verarbeiten – und welche Arten von Beschäftigtendaten erfasst werden.



Die Landkarte zeigt sechs Kategorien von Systemen. Wie bei jeder Systematik ist die Grenzziehung zwischen den Kategorien unscharf. Manche Softwarepakete bieten Funktionen, die mehrere Kategorien abdecken. Die Systematik soll jedoch dabei helfen, etwas mehr Überblick in die Vielfalt datenverarbeitender Systeme im Betrieb zu bringen.

Die Systematik wurde von Wolfie Christl unter Einbeziehung von ExpertInnen aus der gewerkschaftlichen Beratungspraxis im Rahmen der Studie „Digitale Überwachung und Kontrolle am Arbeitsplatz“ (2021) entwickelt. Die Studie enthält viele Quellen zum Thema und ist online frei zugänglich: https://crackedlabs.org/daten-arbeitsplatz

Die folgenden Seiten geben einen komprimierten Überblick über die Verarbeitung personenbezogener Daten im Betrieb und die in der Landkarte angeführten Kategorien technischer Systeme, die Beschäftigtendaten verarbeiten.

1. Verarbeitung „personenbezogener“ Daten über Beschäftigte

Was sind personenbezogene Daten? Fast jede Information, die in irgendeiner Weise mit einer Person in Verbindung gebracht werden kann. Laut DSGVO sind personenbezogene Daten „**alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen**“. Identifizierbar ist eine Person laut DSGVO dann, wenn sie „direkt oder indirekt“ identifiziert werden kann, insbesondere dann, wenn ein „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“ möglich ist. **Damit definiert die DSGVO den Begriff sehr breit**. Beinahe jede Nutzung von Computern, Programmen, vernetzten Geräten, Fahrzeugen oder Maschinen im Betrieb kann zur Verarbeitung personenbezogener Daten führen.

Bei der Erfassung personenbezogener Daten kann unterschieden werden zwischen:

- **Transparent erfasste Daten** werden sichtbar und im vollen Bewusstsein der Betroffenen erfasst bzw. aktiv an- oder eingegeben, z.B. Bewerbungsdaten, Eingabe der Arbeitszeit, Eingabe in ein Formularfeld einer App.
- **Versteckt bzw. automatisch erfasste Daten.** Die Erfassung erfolgt unsichtbar und ohne Zutun der Betroffenen, z.B. Aufzeichnung von Verhaltensdaten bei der Nutzung von Computern, Smartphones oder Maschinen.

Außerdem kann unterschieden werden zwischen:

- **Rohdaten** werden direkt in der Form verarbeitet, in der sie erfasst werden, z.B. Stammdaten, Daten zur Arbeitszeit, Inhalt einer E-Mail, digitales Protokoll über die Nutzung von Programmen oder Websites.
- **Abgeleitete Daten** entstehen durch Weiterverarbeitung von Rohdaten, von einfachen Schlussfolgerungen (z.B. Schluss vom Rohdatum „Uhrzeit des Arbeitsbeginns“ auf das abgeleitete Datum „verspäteter Arbeitsbeginn“) bis hin zu komplexen Analysen, Einschätzungen oder Vorhersagen (z.B. über Leistung, Eignung, Potenzial).

Zudem gibt es die wichtige Unterscheidung zwischen:

- **Inhaltsdaten.** Inhalte von Kommunikationsvorgängen oder Dateien in Form von Text, Bild, Ton oder Video, z.B. der Text einer E-Mail, Word-Datei, Formulareingabe, Suchbegriff oder der Textinhalt eines Telefonats.
- **Metadaten, Logdaten und Verhaltensdaten.** Inhaltsdaten sind nur die Spitze des Eisbergs. Oft viel relevanter sind Daten, deren Erfassung wenig sichtbar erfolgt und deren Bedeutung sich oft nicht auf den ersten Blick erschließt, von Kommunikations-Metadaten (z.B. „wer telefoniert wann mit wem“) bis zu Logdaten von Programmen, Apps, vernetzten Geräten, Maschinen, Fahrzeugen oder Sensoren, die Zeitpunkte von Aktivitäten und weitere Daten aufzeichnen – vom Chipkarten-Zutrittskontrollsystem bis Microsoft 365.

Grundsätzlich verdienen folgende Arten personenbezogener Daten über Beschäftigte besondere Aufmerksamkeit:

- **Zeit.** Sobald Zeitdaten erfasst werden, die über An- und Abwesenheiten hinausgehen, etwa Zeitpunkte von Aktivitäten, wird aus der Zeiterfassung schnell eine Erfassung von Daten über Arbeitstätigkeiten.
- **Arbeitstätigkeiten.** Jede Erfassung von Zeitpunkten, die sich auf Tätigkeiten beziehen, ihrem Beginn und Ende, Informationen über Zustände (z.B. „in Bearbeitung“, „erledigt“), Bearbeitungsschritte oder Ergebnisse sind im Grunde Daten über Arbeitstätigkeiten, von der Ankunftszeit beim Kunden bis zum Zeitpunkt eines Anrufs, der Speicherung einer Word-Datei oder der Nutzung eines Bedienelements einer Maschine.
- **Ort.** Bewegungsdaten können nicht nur direkt erfasst, sondern auch abgeleitet werden (z.B. Kundenbesuch)

2. Systeme zur Steuerung und Kontrolle von Arbeitstätigkeiten

Fast alle technischen Systeme zur Steuerung und Unterstützung von Arbeitsorganisation, Abläufen und Tätigkeiten verarbeiten heute beiläufig oder gezielt eine Vielzahl personenbezogener Daten über Beschäftigte, die zur Überwachung, Kontrolle und Optimierung von Arbeitsleistung und für andere Zwecke eingesetzt werden können. Jedes digitale System, das Arbeitsaufträge zuweist, Fortschritte und Ergebnisse dokumentiert oder eine Arbeitstätigkeit überhaupt erst ermöglicht, speichert heute **Logdaten mit Zeitstempeln**. Jede Aufzeichnung von Zeitpunkten, zu denen Arbeitsschritte beginnen oder enden, ermöglicht etwa Rückschlüsse über Beschäftigte und ihre Arbeit.

„Enterprise Resource Planning" (ERP). Mittlere und große Firmen und ihre Beschäftigten werden meist von mächtigen ERP-Systemen wie **SAP** gesteuert. Sie strukturieren Arbeitsabläufe und zeichnen Daten über Arbeitsschritte auf, die Gegenstand des jeweiligen Moduls sind, z.B. Rechnungswesen/Controlling, Einkauf, Material-/Lagerwirtschaft, Logistik/Transport, Lieferkettenmanagement (SCM), Produktionsplanung/-steuerung, Vertrieb/Marketing/Verkauf, Kundenservice, Qualitätssicherung, Personalverwaltung. Auf Basis von **Ereignisprotokollen** lässt sich nachvollziehen, wer wann welche Tätigkeiten durchgeführt hat, wie schnell und mit welchen Ergebnissen.

Beispiele für **branchen- und tätigkeitsspezifische Systeme**, die Arbeit steuern und Beschäftigtendaten verarbeiten:

- **Produktion:** Systeme für **Manufacturing Execution** (MES) planen und steuern die Fertigung auf Minuten/Sekunden-Ebene. Sie überwachen Abläufe, Ergebnisse, Abweichungen, Qualität und Anwesenheiten und verarbeiten an vielen Stellen Beschäftigtendaten, u.a. durch die **Maschinen- und Betriebsdatenerfassung**.
- **Büro und Wissensarbeit.** Seit **Microsoft 365** speichern Office, Outlook, Teams und andere Anwendungen viele Daten über Verhalten und Kommunikation in der Cloud. Berichtsfunktionen und technische Schnittstellen ermöglichen potentiell Zugriff. Jede Software zur Verwaltung von Arbeitsaufgaben dokumentiert digital, wie Beschäftigte arbeiten – von **Task- und Projektmanagement** bis **Workflow-Management**.
- **Auftragsabwicklung, Ein- und Verkauf, Kundenbetreuung.** Systeme für Angebots- und Auftragsverwaltung, Kundenabrechnung und **Customer Relationship Management** (CRM) speichern Daten über alle Aktivitäten und diejenigen, die sie durchführen. Eine Spezialform sind **Callcenter-Systeme**, die sehr weitgehende Funktionen zur digitalen Kontrolle von Kommunikation, Kundensupport und anderen Arbeitsabläufen bieten.
- **Außendienst und mobile Arbeit.** Ob Verkauf, technischer Kundenservice oder mobile Pflege – die **Smartphone-App** wird immer mehr zur Kommando- und Kontrollzentrale. Neben der Zeiterfassung werden für Dokumentation oder Kundenabrechnung Daten über Dauer/Ergebnisse von Tätigkeiten erfasst, manchmal auch Arbeitsaufträge erteilt. Derartige Apps sind meist an andere Systeme angebunden, z.B. ERP/SAP oder CRM.
- **Transport, Zustellung und Fahrten.** Elektronische Fahrtenbücher und **Fuhrparkverwaltung** speichern Verhaltens- und Bewegungsdaten, automatisierte **Routenplanungssysteme** steuern den gesamten Arbeitsalltag.
- **Warenlager und Logistikzentren.** **Lagerverwaltungssysteme** steuern und kontrollieren jede Bewegung gelagerter Einheiten – mit Bildschirmanweisungen und Barcodescannern oder anderen Technologien z.B. RFID.
- **Einzelhandel, Gastronomie und Hotellerie.** Kassendaten können zur Leistungskontrolle eingesetzt werden. Küchendisplays steuern und kontrollieren Kochtätigkeiten, Hotelverwaltungssysteme die Zimmerreinigung.

Wo Systeme Arbeit nicht nur vermessen, sondern (teil)automatisiert Arbeitsaufträge, -aufgaben und -schritte vorgeben, zuweisen, priorisieren, verteilen, empfehlen – oder dabei gar Zeitdruck ausüben – sprechen wir von **automatisiertem Management**. Darüber hinaus relevant sind Systeme zur **Personaleinsatzplanung und -disposition**, von Dienstplan- und Schichtplanung bis zur Zuweisung von Beschäftigten zu Tätigkeiten und Projekten.

3. Systeme zur Personalverwaltung

Bei Systemen zur Personalverwaltung (HRM, HCM, PIS, HRIS) stehen Daten über Beschäftigte im Mittelpunkt. Grundfunktionen beinhalten immer schon die Verwaltung von **An- und Abwesenheiten** (Kommen, Gehen, Urlaub, Krankenstand), **Personalakten**, **Stammdaten**, **Gehaltsabrechnung**, disziplinären **Verfehlungen** und **Personalentscheidungen**. Sie sind Mittel der **Personalsteuerung und -planung**. Aktuelle cloudbasierte Systeme wie **SAP SuccessFactors** oder **Workday** knüpfen daran an, gehen aber weit darüber hinaus. Sie sollen dabei helfen, die Belegschaft zu bewerten und zu „optimieren" und ermöglichen eine enge Verzahnung von Unternehmensstrategie, Personalsteuerung und Maßnahmen, die am Ende einzelne Beschäftigte betreffen, von Neueinstellungen über Gehaltsentscheidungen bis zu Weiterbildung und Aufstiegsmöglichkeiten. Die Einführung aktueller Systeme führt oft zur erstmaligen Einführung unternehmensweiter Personalsteuerung entlang eines jährlichen Fahrplans mit Zielvereinbarungen, Leistungsbeurteilungen, digital dokumentierten Gesprächen und daraus folgenden Entscheidungen.

Bewertung von Beschäftigten. Die Systeme bieten Funktionen zur Bewertung von **Arbeitsleistung** und „Potenzial" von ArbeitnehmerInnen. **Beurteilungen** durch Vorgesetzte – beim „**360-Grad-Feedback**" auch durch KollegInnen oder gar Kunden – werden in Zahlen verwandelt. Damit können ganze Belegschaften in gute und schlechte Beschäftigte sortiert werden. Auch **Leistungskennzahlen** über Arbeitstätigkeiten und -ergebnisse sowie eine Bewertung von Kompetenzen, Fähigkeiten – und damit der **Eignung** – können einbezogen werden. **Skill-Datenbanken** erstellen umfassende Beschäftigtenprofile. Neuere Systeme versprechen, mit Daten und „**KI**" die künftige Arbeitsleistung, die künftige Eignung für Jobs oder Fördermaßnahmen oder mögliche Kündigungen **vorherzusagen**.

Leistungssteuerung. Wenn **Zielvorgaben** oder **Zielvereinbarungen** mit der Bewertung des **Grads der Zielerreichung** und Maßnahmen wie Anreizen, Belohnungen und Bestrafungen kombiniert werden, entsteht schnell ein umfassendes Kontrollsystem (z.B. **Management by Objectives**, MBO). Das System kann für **Entscheidungen** über Entlohnung, Beförderungen und die Zuweisung zu Positionen, Projekten und Fördermaßnahmen genutzt werden – oder für die Disziplinierung bis hin zur Kündigung. Zur Leistungssteuerung werden neben **leistungsabhängiger Vergütung** und Boni auch **nichtmaterielle Anreize** genutzt, z.B. Spielmechaniken wie Wettbewerbe, Ranglisten, „Abzeichen" oder Punktesysteme. Leistungssteuerung kann auch über **Druck auf Gruppen** und Teams erfolgen.

Personalentwicklung, Skills und betriebliche Weiterbildung. Unter Schlagwörtern wie **Talent Management** werden Bewertungen von Beschäftigten für **Entscheidungen über innerbetriebliche Karrieren und Weiterbildung** genutzt – von der Einstellung an. Während manchen Beschäftigten eine vielleicht vorteilhafte Qualifizierung verwehrt wird, können „Schulungsbedarf" und „Coaching" auch zum **Disziplinierungsinstrument** werden. Daten aus **digitalen Lernplattformen** (z.B. eLearning-Kurse, Tests) können in Beschäftigtenbewertungen zurückfließen.

Personalplanung. Als Grundlage für die kurz-, mittel- und langfristige **Personaleinsatzplanung** werden unter Schlagwörtern wie **Workforce Management** vielfältige Daten analysiert, um den künftigen **Personalbedarf** bzw. Nicht-Bedarf abzuschätzen und daraus Maßnahmen wie Neueinstellungen, Personalabbau, Umstrukturierungen oder Zielvorgaben abzuleiten. Auch Daten über Qualifikationen, Skills, Eignung und Leistung können einfließen.

Weitere Funktionen reichen von der **digitalen Personalakte** über die **Verwaltung von Arbeitsplätzen, Geräten, Dienstautos, Dienstreisen und Reisekosten** und **Online-Umfragen** bis zur **Gesundheitsvorsorge**. Die **Grenzen zu anderen betrieblichen Systemen verschwimmen**, wenn etwa die Zeiterfassung zur Tätigkeitserfassung wird (z.B. für Kundenabrechnung), Daten über „Skills" für Dienstpläne oder die Zuweisung zu Arbeitsaufgaben genutzt werden oder wenn Leistungskontrolle direkt in den Arbeitsprozess integriert wird (z.B. Zeitvorgaben für Aufgaben).

4. Systeme für Kommunikation und Zusammenarbeit

Zwischenmenschliche Kommunikation ist grundrechtlich besonders geschützt und spielt gleichzeitig bei vielen Arbeitstätigkeiten eine wesentliche Rolle. Technische Systeme, die Kommunikation und damit Zusammenarbeit ermöglichen, sind daher besonders sensibel. Neben den Kommunikationsinhalten ermöglichen auch Metadaten über Kommunikationsvorgänge (z.B. „wer kommuniziert wann mit wem") vielfältige Rückschlüsse auf Verhalten.

Telefon, E-Mail, Chat, Video. Wer digitale Kommunikationsinfrastruktur wie **E-Mail** oder die zu Grunde liegenden Netzwerke wartet, betreibt oder kontrolliert, hat potenziell Zugriff auf die übertragenen Informationen. Auch Telefonie wird in Betrieben heute digital über „Voice over Internet Protocol" (**VoIP**) abgewickelt. Zur Gewährleistung der **IT-Sicherheit** werden Aktivitäten wie Website-Aufrufe oder E-Mail-Versand protokolliert, überwacht und gefiltert – um etwa den Zugriff auf nicht vertrauenswürdige Websites zu unterbinden, Spam-Nachrichten auszusondern, Trojaner und Viren zu erkennen und Cyberangriffe zu verhindern. Dies kann fließend in eine Kommunikationsüberwachung zur Erkennung von „internen Bedrohungen", Betrug, Korruption und anderen unerwünschten Verhaltensweisen übergehen. Sobald Endgeräte wie **Smartphones** vom Betrieb gewartet werden, können Kommunikationsdaten direkt vom Gerät aus ausgewertet werden. Inwieweit Betriebe Zugriff auf Daten von cloudbasierten Plattformen etwa für **Chat- und Videokommunikation** haben, hängt vom Anbieter und anderen Faktoren ab.

Kommunikation und Zusammenarbeit. Unter Schlagwörtern wie „**Unified Communications**" werden Produkte vermarket, die mehrere Kanäle wie Sprachtelefonie, Video und Echtzeit-Chats bzw. Messaging miteinander verbinden. Viele Anbieter fügen auch noch das Schlagwort „**Collaboration**" hinzu, um den Aspekt der Zusammenarbeit zu betonen. Systeme wie **Slack** (Salesforce), **Teams** (Microsoft) oder **WebEx** (Oracle) begleiten oft den ganzen Arbeitsalltag und haben sich zu mächtigen **Plattformen** entwickelt, die mit **Apps** und **Chatbots** von Drittherstellern erweitert und an andere betriebliche Systeme angebunden werden können. Damit können Kommunikationsvorgänge **digital strukturiert und (teil)automatisiert** werden. Aus der Kommunikationssoftware wird so schnell ein System zur Verwaltung von **Arbeitsaufgaben und -abläufen**. Andere Systeme vermarkten sich als **innerbetriebliche soziale Netzwerke** und erfüllen Teile dessen, was früher das **Intranet** erfüllt hat – also interne Kommunikation, **Wissensmanagement** oder Verwaltung der eigenen Beschäftigtendaten. Microsoft deckt mit **Outlook**, **SharePoint** und **Teams** viele Bereiche der betrieblichen Kommunikation ab und verbindet sie mit anderen Produkten des cloudbasierten Systems **Microsoft 365** – von Office und Dateibearbeitung bis **CRM** und IT-Sicherheit.

Zugriff auf Kommunikationsdaten. Neben Überwachung für Zwecke der **IT-Sicherheit, Betrugserkennung und „Compliance"** werden Kommunikationsdaten immer öfter für andere Zwecke ausgewertet. Aktuelle Callcenter-Systeme nutzen sie im Namen von **Kundenzufriedenheit**, **Qualitätssicherung** und gar für die Bewertung der Arbeitsleistung – bis hin zur Vermessung von **Stimmung und Emotionen** in Gesprächen. Microsoft bietet Berichtsfunktionen wie **Viva Insights** (früher: **Workplace Analytics**) und **Productivity Score**, die betriebliche Kommunikationsdaten von E-Mail und Chat bis Video, Kalendereinträge, Dateibearbeitungsvorgänge, Programmnutzung und Personaldaten über die Position/Rolle im Betrieb für **exzessive Auswertungen** nutzen. Neben Metadaten über Kommunikationsvorgänge werden auch Inhalte analysiert (z.B. Betreffzeilen). Verfügbare Auswertungen reichen von der Zeit, die Beschäftigte mit Videokonferenzen, Besprechungen und E-Mails verbringen bis zu den kommunikativen „Netzwerken" zwischen ArbeitnehmerInnen oder der „Qualität" von Besprechungen. Andere Berichte werten Schlüsselwörter in Betreffzeilen aus. Abseits vorgefertigter Berichte können Betriebe viele von Microsoft 365 erfassten Daten mit **Power BI** oder eigener Programmierung selbst auswerten. Das Microsoft-Produkt **Delve** nutzt ähnliche Daten für personalisierte Suchergebnisse und Empfehlungen, **Clutter** für die Priorisierung von E-Mails.

5. Unterstützende Systeme für Infrastruktur und Verwaltung

Neben Software, die explizit Daten über Beschäftigte und ihre Arbeitstätigkeiten verarbeitet, sind in Unternehmen viele Systeme zu finden, die zur betrieblichen Infrastruktur gehören. Sie unterstützen Verwaltung und Arbeitsorganisation, erfassen dabei aber ebenfalls umfangreiche Daten, die potenziell auch für andere Zwecke genutzt können.

Zutrittskontrolle, Anmeldung bei Arbeitsplätzen, Geräten und Maschinen. **Zutrittssysteme** mit Schranken, Schleusen oder anderen Türsperren wie elektronische Schlösser sichern heute nicht nur den Haupteingang von Betriebsgebäuden ab, sondern oft auch den **Zutritt zu Innenräumen** (z.B. Liftanlagen, Büros, Besprechungsräume, Produktionshallen, Labors, Rechenzentren). Die Daten werden oft für die **Zeiterfassung** verwendet. Auch die **Anmeldung an Geräten** (z.B. Rechner am Arbeitsplatz, Drucker, Scanner, Kopierer, Maschinen) oder die Nutzung von **Ausgabeautomaten** (z.B. für Schutzausrüstung, Werkzeuge, Material) kann erfasst werden. Zur Prüfung der Zutrittsberechtigung werden elektronische **Magnet- und Chipkarten** genutzt, aber auch Passwörter oder **biometrische Merkmale** (z.B. Fingerabdruck, Gesicht, Iris). Aus den Protokolldaten können potenziell **Profile über Bewegungen und Arbeitstätigkeiten** abgeleitet werden, u.U. auch über die Arbeitstätigkeit hinaus (Pausen, Kantine).

Verwaltung von Gebäuden, Räumen, Fahrzeugen und anderen Betriebsmitteln. Betriebliche Gebäude und Räume werden zu digital vernetzten Umgebungen. Im Rahmen des **Facility Management** werden Vorgänge (z.B. Instandhaltung, Reinigung, Müllentsorgung, Klimatisierung) und Zustände (z.B. Temperatur, Beleuchtung) überwacht, inklusive **Gebäudesicherheit** (z.B. durch Rauch- und Feuermelder, Alarmanlagen, Bewegungsmelder, Überwachungskameras). Auch die **Zuweisung von Arbeitsplätzen, Besprechungsräumen oder Parkplätzen** sowie die **Anschaffung und Nutzung von Betriebsmitteln** wie Einrichtungsgegenständen, Büromöbeln, Maschinen, Geräten, Werkzeugen und Fahrzeugen werden u.U. überwacht (z.B. Kaffeemaschinen, Drucker, Laborutensilien, Gabelstapler, Maschinen). Systeme für die **Buchung von Besprechungsräumen und Arbeitsplätzen** oder für den Empfang **externer BesucherInnen** zeichnen ebenfalls Verhaltensdaten auf. Das **Asset Tracking** dient der Überwachung beweglicher Betriebsmittel (z.B. Reinigungsgeräte, Baumaschinen, Schuttcontainer, medizinische Geräte). Besonders invasiv ist die **Ortung von Geräten** in Innenräumen. Systeme zur **Flotten- oder Fuhrparkverwaltung** bzw. **elektronische Fahrtenbücher** zeichnen Daten über Nutzung und Standorte von Fahrzeugen auf.

Wartung der IT-Infrastruktur, Authentifizierung und Berechtigungen. Die betriebliche IT-Infrastruktur ermöglicht einen weitreichenden Zugriff auf Daten über Arbeitsalltag und Verhaltensweisen von Beschäftigten. Sie umfasst je nach Betrieb **Netzwerkinfrastruktur** und Rechenzentren, Basisdienste wie **Internetzugang, Telefonie und E-Mail**, Software auf stationären und mobilen Geräten sowie alle anderen Softwaresysteme – egal ob diese vor Ort, in der Zentrale oder in der Cloud betrieben werden. Der Zugang zum Datenverkehr ermöglicht Kontrolle von Web-Nutzung, E-Mail-Kommunikation und anderer Online-Dienste. **Endgeräte** wie PCs, Laptops, Smartphones oder Tablets und die darauf installierte Software werden via **Fernwartung** oft vollständig von der IT-Abteilung kontrolliert und ermöglichen u.a. Zugriff auf genutzte Programme/Apps, Dateien auf dem Gerät, Standort. Dies betrifft auch andere **vernetzte Geräte** (z.B. Supermarktkasse, Produktionsmaschine). Software für **Mobile Device Management** (MDM) verwaltet neben Firmengeräten auch private Laptops oder Smartphones, die betrieblich genutzt werden („Bring Your Own Device“). **Nutzeraccounts**, Logins und Berechtigungen erfüllen eine ähnliche Rolle wie Zutrittssysteme im physischen Raum. Während die **Authentifizierung** prüft, wer welche Berechtigungen hat, verknüpfen Nutzeraccounts jegliche Protokoll-, Log- und Verhaltensdaten mit der **Identität** von Beschäftigten.

Helpdesk-Systeme. Unternehmensinterne Anlaufstellen für IT-Probleme, HR-Angelegenheiten und andere Dienste ermöglichen Rückschlüsse auf Helpdesk-MitarbeiterInnen und Beschäftigte, die sich an diese Stellen wenden.

6. Systeme für Sicherheit und „Compliance"

Diverse 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 und vertraglicher Verpflichtungen sicherstellen – darunter die Sicherheit und Gesundheit der Beschäftigten. Datenverarbeitung für diese Zwecke lässt sich oft leichter rechtfertigen als für andere Zwecke – sowohl rechtlich als auch vor der Belegschaft. Gleichzeitig verarbeiten sie oft exzessive/sensible Daten, stellen ArbeitnehmerInnen unter Pauschalverdacht und können leicht für andere Zwecke missbraucht werden.

Diebstahl, Betrug, Korruption und „Compliance". Zu klassischen Überwachungs- und Kontrollmaßnahmen, die mit der Verhinderung von Diebstahl oder Vandalismus argumentiert werden, gehören **Torkontrolle und Videoüberwachung**. Überwachungskameras greifen tief in die Persönlichkeitssphäre ein und werden z.T. auch für andere Zwecke genutzt (z.B. Qualitätssicherung). Manche Systeme nutzen **Daten über Arbeitsprozesse** (z.B. Kassendaten im Handel, Daten aus Finanzbuchhaltung und ERP-Systemen wie SAP), um ungewöhnliche/auffällige Verhaltensweisen, Fehlverhalten, Betrug, Diebstahl, Korruption oder Verstöße gegen „Compliance"-Richtlinien zu entdecken, im Banken-/Finanzbereich auch zur Verhinderung von Insiderhandel und Geldwäsche. „eDiscovery"-Software ermöglicht das Durchsuchen der digitalen Archive des Betriebs nach Indizien für **Fehlverhalten von Beschäftigten**.

Arbeitssicherheit und -gesundheit. Unternehmen sind gesetzlich dazu verpflichtet, die Sicherheit und Gesundheit von ArbeitnehmerInnen zu gewährleisten. Die Verarbeitung personenbezogener Daten für diese Zwecke ist in vielen Fällen gerechtfertigt und sinnvoll. Die dabei erfassten Daten können sehr umfassend und sensibel sein, eine Nutzung für andere Zwecke muss ausgeschlossen sein. In der Industrieproduktion und auf Baustellen werden „smarte" Systeme für die Arbeitssicherheit eingesetzt, die **Körperdaten** vermessen, in der Logistik Systeme zur Verbesserung der **Fahrsicherheit**. Microsoft 365 verspricht **Ablenkung und Stress** durch zu viele parallele Tätigkeiten zu verhindern (MyAnalytics, Viva Insights). Andere Anbieter versprechen, mit tragbaren Geräten **gesundheitsschädliche Bewegungen** zu verhindern oder durch eine Analyse der Tippverhaltens **Ermüdung** zu erkennen.

IT-, Netzwerk- und Cybersicherheit. Im Gegensatz zum Beschäftigtendatenschutz haben betriebliche Systeme zum Schutz der IT-Sicherheit hauptsächlich das Ziel, das Unternehmen, dessen Infrastruktur und die geschäftlichen Werte zu schützen – nicht unbedingt die Rechte der Beschäftigten. **Verfügbarkeit, Integrität und Vertraulichkeit** der geschäftlich verarbeiteten Informationen sollen geschützt werden. Auch wenn die Informationssicherheit ein Teilbereich des Datenschutzes ist, sind ihre Ziele nicht zwingend 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**. Software zum Schutz vor Viren und Cyberangriffen überwacht oft jegliche Aktivität auf betrieblich genutzten **Endgeräten** wie PCs, Laptops, Smartphones oder Tablets (z.B. Änderungen an Dateien, Nutzung von Programmen und Zusatzgeräten wie USB-Sticks oder Druckern). **Firewalls** überwachen und filtern den Datenverkehr zwischen Betrieb und Außenwelt und können etwa den Zugriff auf bestimmte Websites blockieren. Systeme gegen **E-Mail-Spam** gehen nahtlos in eine weitreichende Auswertung von Kommunikationsinhalten über. Unter Begriffen wie **Data Loss Prevention** (DLP), **Security Information and Event Management** (SIEM), **User and Entity Behavior Analytics** (UEBA) wird Software vermarket, die umfassende Verhaltensdaten aus dem ganzen Betrieb zusammenführt, um Cyberangriffe und Datenverlust zu verhindern. Dies beinhaltet die laufende Erkennung **„ungewöhnlicher" Verhaltensweisen** von Beschäftigten, um Bedrohungen von innerhalb des Unternehmens – sogenannte **„Insider Threats"** – zu erkennen.

7. Systeme zur Datenintegration und Analyse

Daten über betriebliche Abläufe und damit auch 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 und „integriert". Damit wird potenziell eine Nutzung für Zwecke möglich, die weit von den Zwecken abweichen, für die die Daten ursprünglich erfasst wurden.

Daten zusammenführen und analysieren. Die in unterschiedlichen betrieblichen Systemen erfassten Daten werden zunehmend in zentralisierten Datenbanken zusammengeführt, um betriebliche Abläufe – und damit auch das Verhalten der Beschäftigten – zu analysieren, zu bewerten und zu steuern. Diese Datenbanken, oft unter Schlagworten wie **Data Warehouse** oder **Data Lake** beworben, werden entweder vom Unternehmen selbst, von ausgelagerten IT-Dienstleistern oder von Cloud-Anbietern betrieben. Eine wichtige Datenquelle sind **Log-, Protokoll- und Ereignisdaten** aus unterschiedlichen betrieblichen Systemen, die meist personenbezogene Daten über Arbeitstätigkeiten enthalten. Software für **Business Intelligence** – etwa von SAP, Microsoft oder Oracle – dient der Analyse und Auswertung. Kennzahlen bzw. **Key Performance Indicators (KPIs)** oder **Metrics** spielen eine große Rolle. Abläufe sollen kostengünstiger oder effizienter werden. Eine Vielfalt an **Berichtsfunktionen** stellt dar, zu welchem Grad bestimmte geschäftliche Ziele erreicht wurden und wo es Abweichungen gibt. Sogenannte **Dashboards** geben Führungskräften das Gefühl, alle wichtigen Zahlen auf einen Blick zu sehen. Auswertungen können sich auf Abläufe oder Standorte beziehen, aber auch auf Teams oder gar auf einzelne Beschäftigte – etwa zur Leistungs- und Verhaltenskontrolle. Auch Software für **Process Mining** dient der Analyse und Optimierung betrieblicher Abläufe.

Cloudbasierte Systeme, Plattformen und Apps. Die **Cloud** – das sind einerseits die gigantischen Rechenzentren von Amazon, Microsoft, Google, IBM und Oracle, in denen Speicher- und Rechenkapazitäten gemietet werden können. Andererseits werden **cloudbasierte Systeme** angeboten – also Software, die nicht vom Kundenunternehmen betrieben und gewartet wird, sondern direkt vom Anbieter der Software. Die Software wird zum Online-„Dienst", der gemietet werden kann. Dies wird als **Software-as-a-Service (SaaS)** bezeichnet. Auch Beschäftigtendaten werden damit vom Anbieter des cloudbasierten Systems verarbeitet, nicht vom Betrieb. Führende Hersteller betrieblicher Software wie Microsoft oder SAP bieten ihre Systeme vermehrt als reine Cloud-Dienste an, bei anderen wie Salesforce oder Workday war dies von Anfang an der Fall. Cloudbasierte Systeme können oft technisch unkompliziert miteinander verbunden werden. Durch **Integrationen** und Programmierschnittstellen (**APIs**) können sie miteinander „sprechen" – und etwa in Echtzeit Daten austauschen. Sie können leicht um zusätzliche Funktionen erweitert werden und werden zur **Plattform**, auf der ein Betrieb schnell eine **App** eines Drittanbieters aktivieren kann, die dann ebenfalls Datenzugriff hat. Dies kann dazu führen, dass ein System am Ende aus mehreren cloudbasierten Diensten besteht. Laufende Updates und die einfache Erweiterbarkeit dieser Systeme um mächtige Zusatzfunktionen führen dazu, dass immer schwerer nachvollziehbar ist, welche personenbezogenen Daten über Beschäftigte zu welchen Zwecken verarbeitet werden – und welcher Anbieter sie überhaupt verarbeitet.

SAP, Microsoft und andere Systeme. Eine Zusammenführung von Daten kann auch innerhalb einzelner mächtiger Systeme wie etwa Microsoft 365 oder SAP erfolgen, die in vielen Betrieben eine derart wichtige Rolle spielen, dass sie Daten für sehr unterschiedliche Zwecke verarbeiten. Ähnliches trifft auf viele branchen- und tätigkeitsspezifische Systeme zu. Aktuelle Callcenter-Software verarbeitet etwa für sich allein bereits umfassende Daten über die Arbeitstätigkeiten der Beschäftigten für sehr verschiedene Zwecke, führt sie zusammen und bietet eine Vielzahl an Berichtsfunktionen und Auswertungsmöglichkeiten. Andere Systeme führen umfassende Verhaltensdaten aus dem ganzen Betrieb im Namen der IT-Sicherheit oder Betrugsprävention zusammen.