

KEINE DIGITALISIERUNG OHNE VERTRETUNG

EINE ANALYSE POLITISCHER INITIATIVEN
FÜR MEHR MITBESTIMMUNG DER
ARBEITNEHMER*INNEN IN DER DIGITALEN
ARBEITSWELT

Justin Nogarede



Diese politische Studie wurde im November 2021 veröffentlicht von



FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES (FEPS)

Europäische Politische Stiftung (European Political Foundation) - N° 4 BE 896.230.213
Avenue des Arts 46 1000 Brüssel (Belgien)
www.feps-europe.eu
@FEPS_Europe



FRIEDRICH-EBERT-STIFTUNG

Hiroshimastrasse 28, D – 10785 Berlin, Deutschland
www.fes.de
@FES_Brussels



FONDATION JEAN-JAURÈS

12 Cité Malesherbes, 75009 Paris, Frankreich
www.jean-jaures.org
@j_jaures



FUNDACIÓN PABLO IGLESIAS

Calle Quintana 1, 28008 Madrid, Spanien
www.fpabloiglesias.es
@fpabloiglesias



FONDAZIONE PIETRO NENNI

Via Alberto Caroncini 19, 00197 Rom, Italien
www.fondazioneNenni.it
@FondazioneNenni



Diese politische Studie wurde mit finanzieller Unterstützung des Europäischen Parlaments erstellt. Sie gibt nicht die Meinung des Europäischen Parlaments wieder.

Copyright © 2021 bei der Foundation for European Progressive Studies
Foto auf der Titelseite (Quelle): shutterstock
Lektorat: Helen Johnston

ISBN: 978-2-930769-63-9

DANKSAGUNG

Diese politische Studie ist das Ergebnis mehrerer Gespräche mit folgenden Expertinnen und Experten, die in persönlicher Eigenschaft beigetragen haben:

- **Christina Colclough**, Gründerin von The Why Not Lab
- **Jean-Benoît Maisin**, Forscher an der Université Saint-Louis – Bruxelles
- **Paul Nemitz**, Mitglied des wissenschaftlichen Rates der FEPS
- **Philipp Staab**, Professor am Lehrbereich Soziologie der Zukunft der Arbeit an der Humboldt-Universität zu Berlin
- **Thorben Albrecht**, Funktionsbereichsleiter Gesellschaftspolitik, IG Metall

Der Autor und die am Projekt beteiligten Stiftungen möchten ihnen für ihre konstruktiven Beiträge und ihre Arbeit danken, ohne die diese politische Studie nicht möglich gewesen wäre. Für den Inhalt dieser Veröffentlichung ist jedoch ausschließlich die FEPS verantwortlich.

INHALT

| | |
|---|----|
| ZUSAMMENFASSUNG | 3 |
| EINLEITUNG | 5 |
| ALGORITHMEN AM ARBEITSPLATZ: TRENDS, RISIKEN, CHANCEN | 7 |
| 1. GEHT DER TREND ZUM TAYLORISMUS AUF SPEED? | 8 |
| 2. MEHR KONTROLLE, WENIGER VERANTWORTUNG: DIE RISIKEN DES ALGORITHMIC MANAGEMENTS | 11 |
| MEHR DATENSCHUTZ, MEHR MITSPRACHE: DAS POTENZIAL DER DSGVO | 14 |
| 3. SCHUTZ VON ARBEITNEHMERDATEN: MANGELNDE KENNTNISSE UND DURCHSETZUNG | 15 |
| 4. FÜR EINE AKTIVERE ROLLE DER GEWERKSCHAFTEN | 18 |
| 5. LEICHT UMZUSETZEN: WICHTIGE BESTIMMUNGEN DER DSGVO FÜR MEHR MITSPRACHE DER ARBEITNEHMER*INNEN | 19 |
| 5.1 Rechtsgrundlage für die Verarbeitung personenbezogener Daten | 19 |
| 5.2 Datenschutz-Folgenabschätzungen | 20 |
| 5.3 Profiling, automatisierte Entscheidungen und die DSGVO | 22 |
| DER DIGITALISIERTE ARBEITSPLATZ: VOM DATENSCHUTZ ZUR DATEN- GOVERNANCE | 26 |
| 6. WENN ES UM DIE DATEN VIELER GEHT, SOLLTE AUCH DIE GOVERNANCE KOLLEKTIV SEIN | 27 |

INHALT

| | |
|--|----|
| 7. KOLLEKTIVE LÖSUNGEN: INFORMATIONEN- UND MITBESTIMMUNGSRECHTE | 28 |
| 7.1 Mitarbeitervertretung im Unternehmen | 28 |
| 7.2 Die Rolle der Gewerkschaften | 30 |
| 7.3 Die Sozialpartner auf EU-Ebene: Die Rahmenvereinbarung zur Digitalisierung | 31 |
| 8. DIE GESETZGEBUNGSAGENDA DER EU – DATEN UND ALGORITHMEN REGULIEREN | 33 |
| 8.1 Das Daten-Governance-Gesetz und andere Initiativen | 33 |
| 8.2 Der regulatorische Rahmen für KI | 34 |
| 8.3 Wer konzipiert, entscheidet: Mitsprache bei der Software-Entwicklung | 36 |
| EMPFEHLUNGEN: INSTITUTIONELLE KAPAZITÄTEN AUSBAUEN | 39 |
| BIBLIOGRAPHIE, AUTOREN, ÜBER DIE FEPS UND IHRE PARTNER | 42 |
| 9. BIBLIOGRAPHIE | 43 |
| 10. ÜBER DEN AUTOR | 48 |
| 11. ÜBER DIE FEPS UND IHRE PARTNER | 49 |

ZUSAMMENFASSUNG

ZUSAMMENFASSUNG

Digitalisierung ohne ausreichende Mitbestimmung der Arbeitnehmer*innen

In der modernen Arbeitswelt wird Macht immer häufiger durch die Erfassung von Daten und ihre Nutzung in algorithmischen Systemen ausgeübt. Dieser Trend hat sich während der Coronapandemie nochmals beschleunigt. Zwar kann dieser Wandel – theoretisch – die Arbeitsqualität verbessern, zurzeit scheint er aber vor allem der besseren Überwachung und Kontrolle der Mitarbeitenden zu dienen. Damit der digitale Wandel sozial nachhaltig gelingt, müssen die Arbeitnehmer*innen und ihre Vertreter*innen die digitale Infrastruktur mitgestalten, die bestimmt, wie sie ihre Arbeit ausführen. Wenn die Arbeitnehmerseite frühzeitig an der Entwicklung bzw. Beschaffung digitaler Arbeitsmittel beteiligt wird, bietet dies den Herstellern den Anreiz, bei der Gestaltung dieser Systeme auch das Wohl der Arbeitnehmer*innen im Blick zu behalten.

Datenschutzvorschriften: Unerforschtes Potenzial

Für viele algorithmische Systeme, mit deren Hilfe Arbeitnehmer*innen überwacht und gelenkt werden oder die Produktion organisiert wird, sind personenbezogene Daten fundamental. Aus diesem Grund ist die Datenschutz-Grundverordnung (DSGVO) ein wichtiges Instrument für Arbeitnehmer*innen, um bei der Digitalisierung der Arbeitswelt stärker mitzureden. Das Potenzial der Datenschutzrechte wird bisher aber noch kaum genutzt, da es an Durchsetzung, Bewusstseinsbildung und kollektiven Maßnahmen mangelt. Datenschutzbehörden brauchen mehr Mittel, um die Vorschriften systematisch durchzusetzen und Beratungstätigkeiten auszuüben. Deshalb sollten Gewerkschaften und Betriebsräte aktiv werden und ihre Kapazitäten ausbauen, damit sie Arbeitnehmer*innen dabei unterstützen können, ihre Rechte wahrzunehmen, z. B. das Recht zu wissen, welche Daten auf welche Weise verarbeitet werden. Des Weiteren spricht vieles dafür, die Arbeitnehmerseite in die Datenschutz-Folgenabschätzungen einzubeziehen und den Anwendungsbereich der Bestimmungen zum Profiling und zur automatisierten Entscheidungsfindung zu prüfen. Schließlich sollten Betriebsräte und Gewerkschaften so weit wie möglich versuchen, die gemäß der DSGVO geltenden individuellen Rechte kollektiv zu vertreten.

Vom Datenschutz zur Daten-Governance: Kollektive Ansätze

Die DSGVO behandelt die kollektive Dimension der Datenverarbeitung und die damit verbundenen Risiken nur teilweise. Deshalb sind die bestehenden Informations-, Mitwirkungs- und Mitbestimmungsrechte für Arbeitnehmer*innen weitere wichtige Ansätze, um den Einsatz digitaler Hilfsmittel am Arbeitsplatz zu beeinflussen. Der Rechtsrahmen für die Mitbestimmung der Arbeitnehmer*innen ist in großen Teilen Europas jedoch schwach ausgeprägt und fehlt in kleinen Unternehmen oft ganz. Außerdem verfügen Gewerkschaften und Betriebsräte oft nicht über die Kapazitäten, um Software wirklich bewerten, prüfen oder gar mitgestalten zu können. Auf EU-Ebene haben die Sozialpartner auf diese Herausforderungen noch nicht wirksam reagiert.

Um die kollektiven Herausforderungen der Digitalisierung in der Wirtschaft zu lösen, hat die Europäische Kommission mehrere einschlägige Rechtsvorschriften für Arbeitnehmer*innen vorgeschlagen. Das als Entwurf vorliegende Daten-Governance-Gesetz könnte Wege zu einer verantwortungsvollen gemeinsamen Nutzung von Daten weisen, der Gesetzesentwurf für Systeme der künstlichen Intelligenz (das KI-Gesetz) muss jedoch noch verbessert werden. Ihm fehlt es an angemessenen institutionellen Strukturen für die Durchsetzung und an Möglichkeiten für einzelne Personen, ihre Rechte wahrzunehmen. Außerdem gibt es keine Bestimmungen, nach denen Arbeitnehmervertreter*innen an Entscheidungen über die Verwendung von KI am Arbeitsplatz beteiligt werden müssen. Die Verordnung könnte die Rolle der organisierten Arbeitnehmervertretung in diesem Bereich sogar schwächen.

Obwohl die DSGVO, die in Kollektivvereinbarungen geregelten Rechte und neue EU-Rechtsvorschriften wichtig sind, reichen sie alleine nicht aus, um die Mitbestimmung der Arbeitnehmer*innen bei der Gestaltung von betrieblicher Software zu gewährleisten. Beim Einsatz neuer Technologien am Arbeitsplatz erfolgt die Beteiligung der Arbeitnehmer*innen oft spät, defensiv und ohne ausreichende Informationen. Für die Mitgestaltung von Software braucht es dagegen proaktive und frühzeitige Maßnahmen und Know-how. Dies ist nur mit neuen gesamteuropäischen Institutionen und Partnerschaften zwischen Arbeitnehmerorganisationen, Wissenschaft, Zivilgesellschaft und den Behörden zu erreichen.

EINLEITUNG

EINLEITUNG

Schon 1974 sagte der US-amerikanische Arbeits-theoretiker Harry Braverman voraus, die Computerrevolution werde zur Dequalifizierung der Arbeiter*innen führen und die Überwachung der Arbeit und die Kontrolle des Personals verstärken. Seit Beginn der Coronapandemie deutet alles darauf hin, dass sich diese Dynamik weiter beschleunigt.

Eine digitale Zukunft, in der Arbeitnehmer*innen wie in einem tayloristischen Traum auf atmende Roboter reduziert werden, ist aber alles andere als unvermeidlich. Bevor das Projekt durch einen Militärputsch gestoppt wurde, rief Chiles Präsident Salvador Allende Cybersyn ins Leben, einen nationalen Plan für algorithmisches Management, ehe es den Begriff überhaupt gab, in dem Technologie mit einer zentralen Rolle autonomer Arbeiter*innen verknüpft wurde. Dieser Fall beweist die Kontingenz der technologischen Entwicklung und die zentrale Rolle sozialer Beziehungen. Ein bekannteres Beispiel ist das deutsche System von Informations-, Mitwirkungs- und Mitbestimmungsrechten der Arbeitnehmer*innen. Es zeigt, dass unter den richtigen sozialen Bedingungen sowohl die Arbeitnehmer*innen als auch die Unternehmen vom Einsatz neuer Technologien profitieren können.¹

Die Europäische Kommission ist nach eigener Aussage entschlossen, die digitale Wende „menschenzentriert“ zu gestalten. Eine auf Menschen – oder Arbeitnehmer*innen – ausgerichtete Technologiewende lässt sich aber nicht von oben verordnen: Am Arbeitsplatz lässt sie sich nur erreichen, wenn die Arbeitnehmer*innen Entscheidungen über neue Technologien, die ihre Arbeit betreffen, verstehen und an ihnen mitwirken können. Der US-amerikanische Rechtsprofessor Frank Pasquale hat darauf hingewiesen, dass algorithmische Systeme dazu verwendet werden können, die menschliche Arbeit zu ergänzen und zu verbessern.² Für Fortschritte auf diesem Weg sind die Stimmen der Arbeitnehmer*innen und die Rolle der Gewerkschaften unverzichtbar.

Nach einem kurzen Überblick über aktuelle Trends und die potenziellen Risiken datengestützter algorithmischer Systeme analysiert diese Arbeit die unterschiedlichen Politikbereiche, in denen die EU und nationale Stellen, Gewerkschaften und die Organisationen der Zivilgesellschaft die Beteiligung der Arbeitnehmer*innen aktiv stärken können. Nach einem Blick auf das Potenzial und die Grenzen der Datenschutz-Grundverordnung wird die Rolle der kollektiven Informations-, Mitwirkungs- und Mitbestimmungsrechte der organisierten Arbeitnehmerschaft untersucht. Abschließend werden die potenziellen Auswirkungen künftiger EU-Rechtsvorschriften für die digitale Wirtschaft analysiert und untersucht, was getan werden kann, um den Einfluss der Arbeitnehmer*innen auf die Gestaltung von Softwaresystemen für den Arbeitsplatz zu gewährleisten. Die Studie schließt mit einer Reihe von politischen Empfehlungen.

1 S. Holmberg, „Fighting Short-Termism with Worker Power“, Roosevelt Institute (17. Oktober 2017).

2 F. Pasquale, *New Laws of Robotics: Defending Human Expertise in the Age of AI* (Cambridge, MA: Belknap Press, 2020).

ALGORITHMEN AM ARBEITSPLATZ: TRENDS, RISIKEN, CHANCEN

ALGORITHMEN AM ARBEITSPLATZ: TRENDS, RISIKEN, CHANCEN

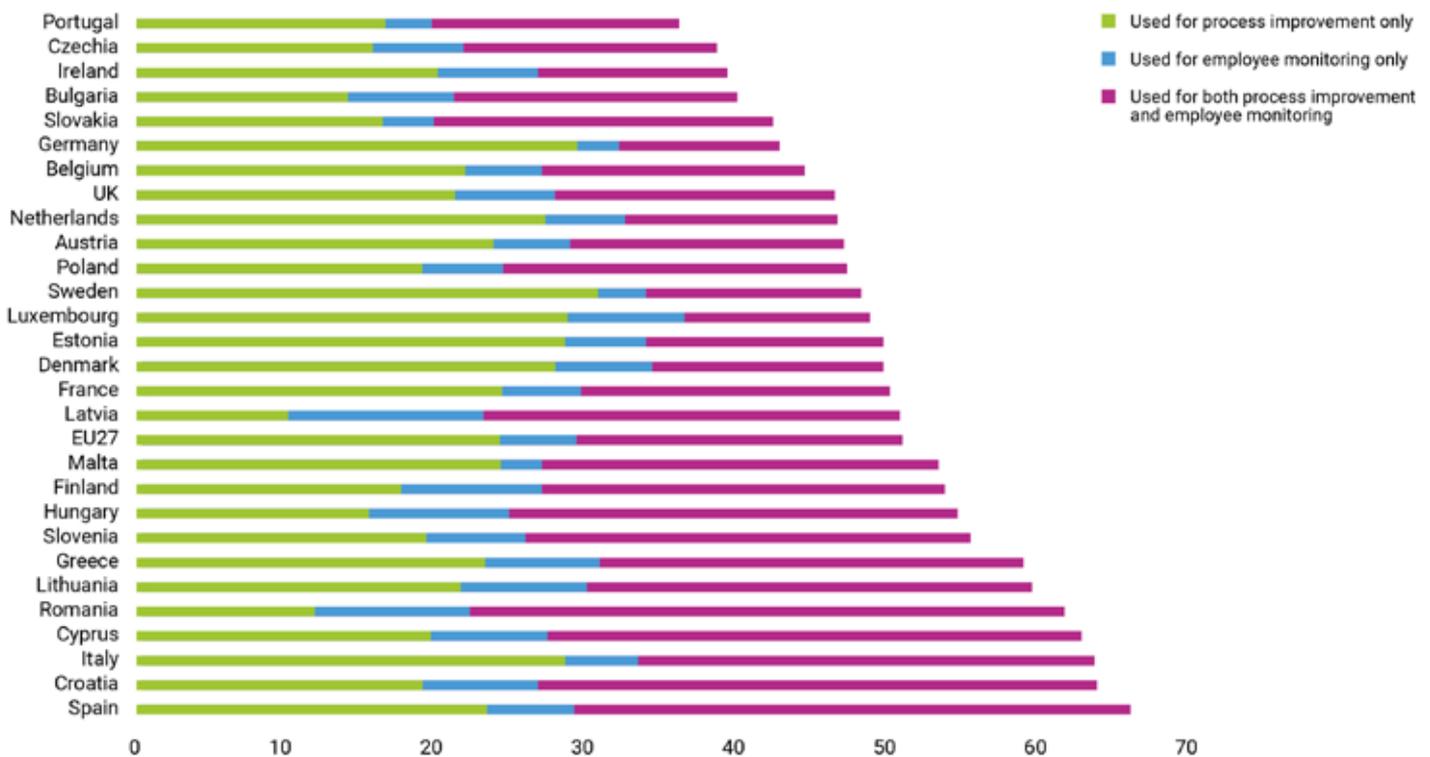
1. Geht der Trend zum Taylorismus auf Speed?

Die Digitalisierung der Arbeitswelt ist in vollem Gange: Es werden immer mehr Daten erfasst und Algorithmen eingesetzt, um Arbeitnehmer*innen zu beaufsichtigen oder um ihre Arbeit zu analysieren und sie letzten Endes zu ersetzen.³ Dieser Trend hat sich durch die Coronapandemie noch beschleunigt, weil Arbeitgeber die zunehmende Telearbeit mit

neuen digitalen Tools zur Überwachung und Leistungserfassung kombinieren. So war die Nachfrage nach Software zur Überwachung der Mitarbeitenden bei niederländischen Unternehmen laut der Softwarebewertungs-Website Capterra im ersten Quartal 2021 um 58 Prozent höher als 2020.⁴ Und laut einer aktuellen Befragung britischer Führungskräfte haben 20 Prozent von ihnen bereits Software installiert, die Mitarbeitende in Fernarbeit überwacht, oder haben dies vor.⁵

Abbildung 1: Nutzung von Datenanalytik, um Prozesse zu verbessern und/oder die Leistung von Mitarbeiter*innen zu überwachen, EU-27 und GB (%)

Quelle: ECS 2019 Fragebogen für Führungskräfte (Eurofound, 2020a)



3 P. V. Moore, M. Upchurch und X. Wittaker (Hg.), *Humans and Machines at War: Monitoring, Surveillance and Automation in Contemporary Capitalism* (London: Palgrave Macmillan, 2018).

4 NOS, „Gluurappartuur’ in trek door thuiswerken, vakbond bezorgd“, auf: <https://nos.nl/artikel/2375956-gluurappartuur-in-trek-door-thuiswerken-vakbonden-bezorgd>

5 Skillcast (2020), „Remote-working Compliance YouGov Survey“, 25. November, auf: <https://www.skillcast.com/blog/remote-working-compliance-survey-key-findings>

Bis vor kurzem galt die Nutzung von Arbeitnehmerdaten für algorithmische Systeme im Personalwesen, auch „People Analytics“ oder „algorithmisches Management“ genannt, in Europa als Randphänomen, das auf die Plattform- oder Gig-Ökonomie begrenzt war. Doch wie neue Daten zeigen, **werden digitale Managementwerkzeuge, mit denen beispielsweise Arbeitszeiten online erfasst oder die Leistung von Arbeitnehmer*innen bewertet werden, inzwischen in der gesamten Arbeitswelt eingesetzt** und sind nicht länger auf die Gig-Ökonomie beschränkt.⁶ Außerdem erweitert sich das Spektrum der Funktionen, in denen digitale Werkzeuge eingesetzt werden und kann alle Arbeitsbereiche abdecken, von der Einstellung bis zur Kündigung und alles dazwischen (siehe Infobox 1).⁷

INFOBOX 1: Automatisierte Managementaufgaben

- Auswahl von Stellenbewerbern
- Planung und Verteilung von Arbeitsaufgaben
- Überwachung der Beschäftigten
- Bewertung der Leistung von Arbeitnehmer*innen
- Einordnung in Gehaltsstufen
- Entscheidungen über Beförderungen und andere Chancen
- Start von Kündigungs- oder Disziplinarverfahren

Es ist wenig überraschend, dass Arbeitgeber vermehrt auf digitale Überwachung und Technologien zum algorithmischen Management zurückgreifen. Um die Produktivität zu steigern und Kosten zu senken, versuchen Unternehmen schon lange, die Arbeitnehmer*innen stärker zu überwachen und zu kontrollieren. Vor diesem Hintergrund wirkt die Einführung algorithmischer Systeme am Arbeitsplatz wie die Fortsetzung des wissenschaftlichen Managements des 20. Jahrhunderts mit anderen Mitteln.⁸

Aber diese anderen Mittel haben es in sich. Die Hersteller von Personal- und Unternehmenssoftware bieten Überwachungs- und Kontrollfunktionen, die viel tiefgreifender und detaillierter sind als früher. Dazu gehören die laufende Erfassung von Tastatureingaben und Browsernutzung, regelmäßige Screenshots und die Überwachung von sozialen Medien, E-Mails und Anrufen. Außerdem werden Sensoren am Arbeitsplatz immer beliebter, also z. B. am Körper zu tragende Tracker, Gesichtserkennungssoftware oder Systeme, die Augenbewegungen erfassen. Nicht zuletzt erheben die Arbeitnehmer*innen selbst mit Hilfe von Handy-Apps Gesundheits- und Fitnessdaten, die in vielen Fällen weitergegeben und mit anderen Datenquellen kombiniert werden können.⁹ Wie eine große Studie von Cracked Labs in Österreich und Deutschland zeigt, werden entsprechende Softwares und algorithmische Systeme auch in der EU angeboten – und eingesetzt.¹⁰

6 U. Huws, N. Spencer und M. Coates, „The Platformisation of Work in Europe. Highlights from Research in 13 European Countries“, FEPS, UNI Europa und die University of Hertfordshire, 2019; J. Berg, „Protecting Workers in the Digital Age: Technology, Outsourcing and the Growing Precariousness of Work“, SSRN (2019), auf: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3413740

7 J. Adams-Prassl, „What if your Boss was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work“, *Comparative Labor Law & Policy Journal* 41(1) (2019).

8 L. Nurski, „Algorithmic Management is the Past, Not the Future of Work“, Blog-Beitrag vom 6. Mai 2021, Bruegel, auf: <https://www.bruegel.org/2021/05/algorithmic-management-is-the-past-not-the-future-of-work/>

9 J. Bronowicka u.a., *‘Game that you Can’t Win’? Workplace Surveillance in Germany and Poland* (Frankfurt (Oder): Europa-Universität Viadrina, 2020), 7; A. A. Aloisi und E. Gramano, „Artificial Intelligence is Watching you at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context“, *Automation, Artificial Intelligence & Labor Law* 41(1) (2019).

10 Cracked Labs, „Digitale Überwachung und Kontrolle am Arbeitsplatz. Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management?“ (September 2021)

INFOBOX 2: Definition des Begriffs „algorithmische Systeme“

Wenn in dieser Studie der Begriff „algorithmische Systeme“ verwendet wird, sind damit hier „alle Systeme, Programme oder Prozesse“ gemeint, die „Berechnungen nutzen, um Entscheidungen oder Strategien des Managements zu unterstützen oder zu ersetzen, die sich auf Chancen, Berechtigungen, Freiheiten, Rechte und/oder Sicherheit der Arbeitnehmer*innen auswirken. Im Rahmen algorithmischer Systeme können Prognosen, Klassifizierungen, Optimierungs- oder Identifizierungsprozesse und/oder Empfehlungen eingesetzt werden.“¹¹ Anders ausgedrückt ist der Begriff weder auf voll automatisierte Systeme noch auf bestimmte technische Eigenschaften, wie „selbstlernende“ Algorithmen beschränkt, die im Bereich der künstlichen Intelligenz gerade populär sind.

So erkannten beispielsweise während der industriellen Revolution in Großbritannien Hersteller die Vorteile von Erfindungen, die dazu beitragen konnten, „handwerkliche Praktiken und Kontrollen zu umgehen und dadurch Widerstände gegen Veränderungen zu brechen.“¹⁴ Aus diesem Grund wurden Technologien für Arbeitgeber entwickelt, die anstelle von Erwachsenen Kinder beschäftigen wollten, weil Kinder billiger und leichter zu kontrollieren waren. Die äußerst detaillierten Überwachungsmöglichkeiten moderner betrieblicher Software und die sinkende Lohnquote¹⁵ deuten auf eine ähnliche Dynamik in der aktuellen digitalen Revolution hin. So kam eine große Studie über den Markt für „People Analytics“ in der EU zu dem Ergebnis, dass „die Funktionalität der Software sich oft daran orientiert, was technisch möglich ist, was oft Raum für tiefe Eingriffe in die Rechte der Arbeitnehmer*innen lässt“. Oft sind problematische Funktionen standardmäßig aktiviert und Firmen müssen sie deaktivieren, um das System rechtskonform zu nutzen.¹⁶

Technikhistoriker weisen darauf hin, dass Entwickler nicht einfach untersuchen, welche Technologie besonders effizient oder produktiv ist, und diese dann bauen. Welche Produkte entwickelt werden, hängt auch von den sozialen (hierarchischen) Beziehungen am Arbeitsplatz ab.¹² So ist die Steigerung der Produktivität nicht der einzige Grund, warum Arbeitgeber Technologie einsetzen. Es kann auch darum gehen, die Macht der Führungsebene gegenüber dem Personal auszubauen, um Arbeitskosten zu senken. Wie der US-amerikanische Professor für Arbeitsrecht Brishen Rogers festgestellt hat, ist die Steigerung der Produktivität zu begrüßen, weil sie in der Regel zu besseren Arbeitsnormen führt, wogegen eine Machtkonzentration auf der Führungsebene oft genau das Gegenteil bewirkt.¹³

11 Die Definition wurde übernommen aus: R. Richardson, „Defining and Demystifying Automated Decision Systems“, *Maryland Law Review* 81 (in Kürze erscheinend, 2022).

12 L. Winner, „Do Artifacts Have Politics?“, *Daedalus* 121 (1980).

13 B. Rogers, „The Law and Political Economy of Workplace Technological Change“, *Harvard Civil Rights-Civil Liberties Law Review* 55 (2021). Ob höhere Produktivität zu besseren Arbeitsbedingungen führt oder nicht, hängt natürlich vom Arbeitsrecht und der Verhandlungsmacht der Arbeitnehmer*innen ab.

14 J. Humphries, „The lure of aggregates and the pitfalls of the patriarchal perspective: a critique of the high wage economy interpretation of the British industrial revolution“, *Economic History Review* 66 (3) (2013), 710.

15 C. B. Frey, *The Technology Trap: Capital, Labor, and Power in the Age of Automation* (Princeton: Princeton University Press, 2019).

16 Cracked Labs, 75.

INFOBOX 3: Technologie ist nicht gleich Effizienz

In seinem Artikel „Do artifacts have politics?“ beschreibt Langdon Winner ein aufschlussreiches Beispiel, bei dem Automatisierung dazu genutzt wird, die Kontrolle durch das Management zu stärken. In den 1880er Jahren stattete der US-amerikanische Hersteller Cyrus McCormick seine Fabrik mit pneumatischen Formmaschinen im Wert von 500 000 US-Dollar aus. Die Maschinen waren jedoch weniger effizient als die Arbeiter: sie produzierten schlechtere Gussteile zu höheren Kosten. Warum hatte er sie dann gekauft? Die Maschinen machten Facharbeiter überflüssig, also genau die Arbeiter, die sich gewerkschaftlich organisiert hatten, und mit denen Cyrus McCormick Streit hatte.¹⁷ Ein aktuelles Beispiel wären Amazons Versuche, mit Hilfe von Technologien Gewerkschaften zu verhindern.

INFOBOX 4: Callcenter-Panoptikum

Das französische Unternehmen Teleperformance, das Callcenter betreibt und 380 000 Menschen beschäftigt, kündigte im Jahr 2021 an, bei den Arbeitnehmer*innen zu Hause Webcams zu installieren, die überwachen, ob diese essen, ihr Handy benutzen oder ihren Arbeitsplatz verlassen. Die Webcams sollen an ein KI-System angeschlossen werden, das nach dem Zufallsprinzip nach Verstößen sucht. Wird ein Verstoß entdeckt, macht das System automatisch ein Foto und leitet es für weitere Maßnahmen an das Management weiter.²⁰

2. Mehr Kontrolle, weniger Verantwortung: Die Risiken des algorithmischen Managements

Datenerfassung am Arbeitsplatz ist eine fundamentale Bedrohung für die Privatsphäre der Arbeitnehmer*innen. Daten könnten sich beispielsweise auf intime Aspekte einer Person beziehen, wie biometrische, genetische und affektive Daten, und sich möglicherweise auf das Privatleben der Arbeitnehmer*innen auswirken, wie z. B. die Schlafgewohnheiten.¹⁸ Die Erfassung von GPS-Daten oder Daten tragbarer Tracker enthüllt außerdem nicht nur intime Details, sondern verwischt auch schnell die

Grenze zwischen Beruf und Privatleben. **Wenn Arbeitnehmer*innen ständig überwacht werden, führt**

dies nachweislich zu Stress, Ängsten und einem Vertrauensverlust am Arbeitsplatz.¹⁹

Neben den unmittelbaren Datenschutzbedenken beziehen sich weitere Risiken bei der Erfassung und Speicherung von personenbezogenen Daten darauf, wie und von wem diese Daten genutzt werden. Durch die großflächige Erhebung von Daten aus unterschiedlichen Quellen erhalten Führungskräfte äußerst detaillierte und durchgehende Informationen über Produktivität, Verhalten und persönliche Eigenschaften von Arbeitnehmer*innen. Diese können für algorithmische Systeme eingesetzt werden, die von einfachen Entscheidungsbäumen bis zu komplexen selbstlernenden Systemen reichen, um Managementfunktionen zu automatisieren und die Kontrolle über das Personal zu verstärken.

So können Unternehmen beispielsweise automatisch Arbeitsaufgaben verteilen, die Leistung einzelner Beschäftigter verfolgen und Arbeitnehmer*innen nach einfachen Kennzahlen (gelieferte Pakete, abgeholte Bestellungen, geschriebene Wörter, versendete E-Mails) bewerten. Jede Abweichung vom

17 L. Winner, „Do Artifacts Have Politics?“, *Daedalus* 1(109) (1980), 124-5.

18 Autoriteit Persoonsgegevens (Niederländische Datenschutzbehörde), „AP. Verwerking gezondheidsgegevens wearables door werkgevers mag niet“ (8. März 2016), auf: <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet>

19 S. Sarpong und D. Rees, „Assessing the Effects of ‘Big Brother’ in a Workplace: the case of WAST“, *European Management Journal* 32(2) (2014), 216–22.

20 P. Walker, „Call Centre Staff to be Monitored via Webcam for Home-Working ‘Infractions’“, *The Guardian*, 26. März 2021, auf: <https://www.theguardian.com/business/2021/mar/26/teleperformance-call-centre-staff-monitored-via-webcam-home-working-infractions>

Durchschnitt kann festgestellt und den Arbeitnehmer*innen und Führungskräften angezeigt werden. Das kann dazu führen, dass Arbeitnehmer*innen ihre Arbeit auf diese Kennzahlen ausrichten und dabei Sicherheitsvorschriften und -verfahren ignorieren und berufliche Arbeits- und Verhaltensnormen untergraben. In den Worten einer Forschergruppe kann dies eine „datengestützte, auf Leistung ausgerichtete und stark auf die Einhaltung von Regeln konzentrierte Unternehmenskultur schaffen, in der für Autonomie und Integrität wenig Raum ist.“²¹

Während die Kontrolle des Arbeitgebers verstärkt wird, verschwimmen traditionelle Verantwortungs- und Rechenschaftsstrukturen. Durch die Gestaltung von Bewertungssystemen und den Einsatz von Spielen und unterschiedlichen Anreizen können Arbeitgeber das Verhalten der Arbeitnehmer*innen auf eine Weise steuern, die ebenso wirksam ist wie herkömmliche und direkte Formen der Kontrolle, jedoch weitaus weniger sichtbar. Wenn das Management teilweise oder vollständig automatisiert ist, ist es für Arbeitnehmer*innen schwieriger, Gründe für Entscheidungen nachzuvollziehen und anzufechten. Das macht viele automatisierte Entscheidungssysteme zur berühmten-berühmten „Black Box“.²²

Wenn mit algorithmischen Systemen etwas schief läuft, lässt sich die Ursache oft nur schwer ermitteln: waren es inkorrekte Daten, Konstruktionsfehler im System, ein Anwendungsfehler oder die Entscheidung eines Vorgesetzten auf der Grundlage von Berechnungsergebnissen? Viele analytische Systeme werden von großen Softwarekonzernen hergestellt, die in Bezug auf die Funktion des Algorithmus Eigentumsrechte geltend machen. Das bedeutet, dass weder der Arbeitgeber noch die Beschäftigten die getroffenen Entscheidungen im Detail untersuchen und prüfen können, ob das System Datenschutz und Arbeitsrecht respektiert. Das ist wichtig, weil viele vorgeblich neutrale Systeme nicht wie gewünscht funktionieren und zu diskriminierenden Ergebnissen führen.²³

Automatische und algorithmische Systeme werden am Arbeitsplatz häufig zu dem ausdrücklichen Zweck eingeführt, die Effizienz zu steigern. Wie allgemein bekannt ist, kann Technologie jedoch mehreren Zwecken gleichzeitig dienen. Neben der willkommenen Erhöhung der Produktivität können Arbeitgeber Technologie auch dazu nutzen, um ihre Macht über die Beschäftigten zu erhöhen und dadurch ganz schlicht die Arbeitskosten zu senken. Geeignete Mittel sind die Vereinfachung und Homogenisierung von Arbeitsaufgaben, der bewusste Austausch hoch qualifizierter Arbeitskräfte und eine Verstärkung der Informationsasymmetrie zwischen Arbeitnehmer*innen und Management (Überwachung). Tatsächlich zeigen einige Forschungsarbeiten, dass die Digitalisierung der Arbeit tatsächlich die Arbeitskosten senkt und die Arbeitsbedingungen verschlechtert. So nutzt Amazon Technologie ganz offen, um Versuche der Beschäftigten, sich gewerkschaftlich zu organisieren, zu erkennen und zu unterbinden. Und Zalandos subtileres algorithmisches Leistungsbewertungssystem verhindert gute Bewertungen durch Kunden und die damit verbundenen Chancen auf Beförderung und Gehaltserhöhung.²⁴

Natürlich müssen diese Risiken nicht unbedingt eintreten und die überlegte Nutzung digitaler Technologien am Arbeitsplatz kann echte Vorteile bieten. Ganz allgemein kann People-Analytics-Software Arbeitnehmer*innen dabei helfen, sich zu konzentrieren, ihre Arbeit besser zu strukturieren und so ihre Produktivität zu erhöhen. Softwaregestützte Entscheidungsprozesse können zudem Verzerrungen bei der Einstellung, Beförderung und Kündigung von Beschäftigten mindern. Tragbare Tracker können auf Risikoverhalten und Stress hinweisen und Maßnahmen für Gesundheit und Sicherheit am Arbeitsplatz unterstützen. Wenn Arbeitnehmer*innen überwacht werden, kann sie dies vor unbegründeten Beschwerden von Kunden oder Vorgesetzten schützen. Nicht zuletzt können Arbeitgeber Überwachungswerkzeuge auch aus legitimen Gründen einsetzen, z. B. um Betrug und andere Straftaten zu

21 U. Leicht-Deobald et al., „The Challenges of Algorithm-Based HR Decision-Making for Personal Integrity“, *Journal of Business Ethics* 160 (2021), 386.

22 F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (London: Harvard University Press, 2021).

23 Eine keineswegs erschöpfende Liste finden Sie unter: <https://github.com/daviddao/awful-ai>

24 Siehe P. Staab und S. Geschke, „Ratings als arbeitspolitisches Konfliktfeld. Das Beispiel Zalando“, Studie 429, Hans-Böckler-Stiftung (2020).

verhindern oder um ihre Beschäftigten vor Belästigung zu schützen.

Das positive Potenzial von Überwachungswerkzeugen und algorithmischem Management kann jedoch nur genutzt werden, wenn die Rechte der Arbeitnehmer*innen respektiert werden und sie mitbestimmen können, welche Technologien entwickelt und unter welchen Umständen sie eingesetzt werden. Daher ist es wichtig, Wege zu finden, die es den Arbeitnehmer*innen ermöglichen „über den Algorithmus zu verhandeln“, wie es der Arbeitsrechtswissenschaftler De Valerio formuliert hat.²⁵

25 V. De Stefano, „Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection“, *Comparative Labour Law & Policy* 41(1) (2019).

MEHR DATENSCHUTZ, MEHR MITSPRACHE: DAS POTENZIAL DER DSGVO

MEHR DATENSCHUTZ, MEHR MITSPRACHE: DAS POTENZIAL DER DSGVO

Seit 2018 regelt die Datenschutz-Grundverordnung die Verarbeitung personenbezogener Daten am Arbeitsplatz und in allen anderen Bereichen. Die Verordnung ist wichtig, weil viele der algorithmischen Systeme, mit deren Hilfe Arbeitnehmer*innen kontrolliert werden, personenbezogene Daten der Arbeitnehmer*innen erfassen und verarbeiten. Die DSGVO bietet also einen gesetzlichen Rahmen für die Erfassung und Nutzung personenbezogener Daten von Arbeitnehmer*innen und ist daher ein wichtiges Instrument, mit dem Arbeitnehmer*innen technologische Entwicklungen an ihrem Arbeitsplatz beeinflussen und das Kräfteverhältnis zwischen Management und Fabrikhalle zu ihren Gunsten verändern können.

Die DSGVO ist besonders wirksam, weil ihre Bestimmungen nicht nur die Privatsphäre der Arbeitnehmer*innen schützen, sondern auch eine Reihe von grundlegenden Rechten abdecken und auch für die Erstellung von Profilen und automatisierte Entscheidungsprozesse gelten. Das ist wichtig, weil die Möglichkeiten, über neue Technologien am Arbeitsplatz mitzubestimmen, innerhalb der EU sehr unterschiedlich sind und die DSGVO in manchen Ländern und Unternehmen das beste verfügbare Instrument darstellt. Doch ehe die Datenschutzvorschriften ihre volle Wirkung entfalten können, müssen sie besser erklärt und durchgesetzt werden. Hier können Arbeitnehmervertreter*innen eine entscheidende Rolle spielen.

3. Schutz von Arbeitnehmerdaten: Mangelnde Kenntnisse und Durchsetzung

Die Datenschutz-Grundverordnung ist inzwischen seit vier Jahren in Kraft, ihre Bedeutung für den Schutz und die Durchsetzung von Arbeitnehmerinteressen wird jedoch noch kaum erkannt und genutzt. Obgleich die Zahl der Verfahren, die sich direkt auf Beschäftigungsverhältnisse beziehen und zu einer Geldbuße geführt haben, langsam zunimmt und inzwischen bei über 60 Fällen liegt,²⁶ deuten die Forschungsdaten darauf hin, dass viele Arbeitnehmer*innen ihre Rechte nicht kennen, Gewerkschaften sie nicht aktiv unterstützen und Datenschutzbehörden die Vorschriften nicht umsetzen.

Erstens scheinen viele Arbeitnehmer*innen ihr Recht auf Privatsphäre und Datenschutz gar nicht zu kennen.²⁷ In einer aktuellen Umfrage des Christlich-Nationalen Gewerkschaftsbundes (CNV) in den Niederlanden gaben 13 Prozent der Befragten an, dass sie bei der Arbeit zu Hause überwacht werden, was nur in begründeten Ausnahmefällen mit Zustimmung des Betriebsrats erlaubt ist.²⁸ Auch bei der niederländischen Datenschutzbehörde gehen nur wenige Beschwerden von Arbeitnehmer*innen ein, was nach Ansicht der Behörde damit zusammenhängen könnte, dass Arbeitnehmer*innen den Umfang der Überwachung nicht kennen.²⁹ Auch der hierarchische Charakter des Arbeitgeber-Arbeitnehmer-Verhältnisses spielt dabei vermutlich eine Rolle.

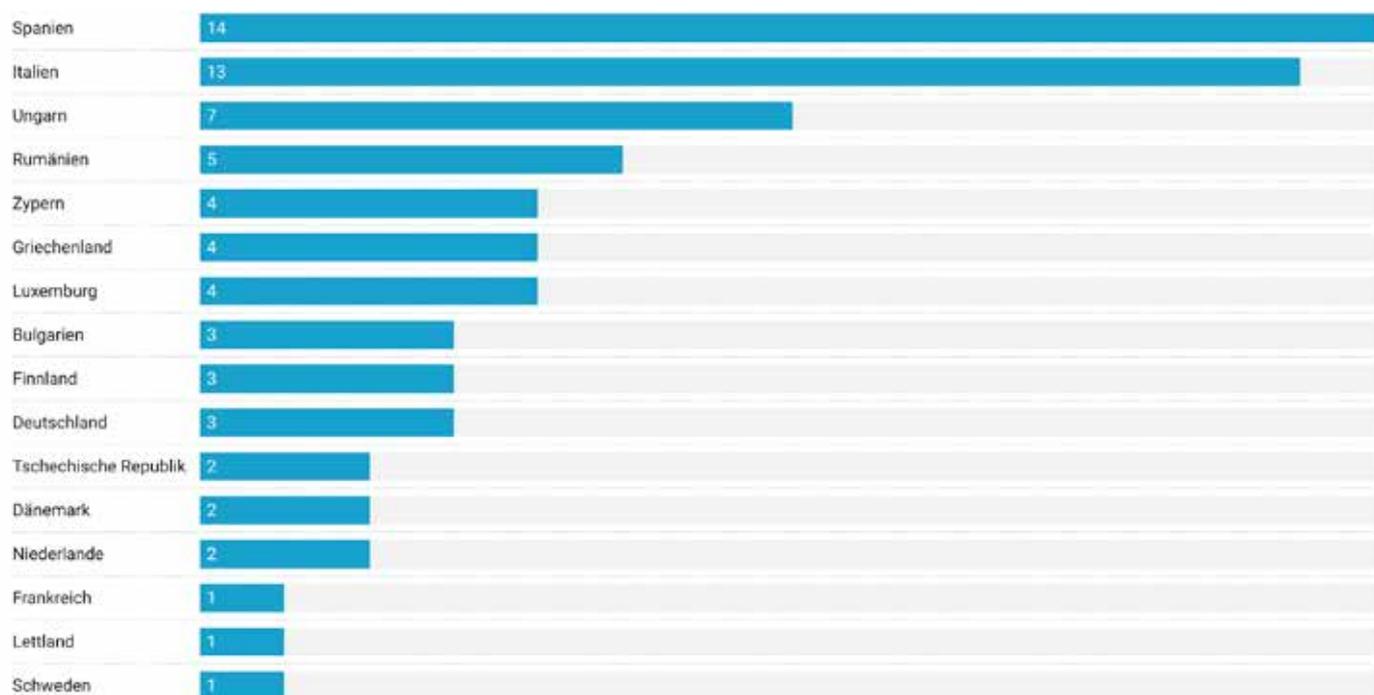
26 „GDPR Enforcement Tracker“ von CMS, auf: <https://www.enforcementtracker.com>. Die Datenbank erfasst alle öffentlich verfügbaren Bußgeldentscheidungen von Datenschutzbehörden. Sie ist nicht vollständig, bietet jedoch einen Anhaltspunkt.

27 J. Bronowicka et al., 24.

28 CNV, „Half miljoen thuiswerkers via software in de gaten gehouden“, auf: <https://www.cnv.nl/nieuws/half-miljoen-thuiswerkers-via-software-in-de-gaten-gehouden/>

29 NOS, „Gluurapparaat in trek door thuiswerken, vakbond bezorgd“, auf: <https://nos.nl/artikel/2375956-gluurapparaat-in-trek-door-thuiswerken-vakbonden-bezorgd>

Abbildung 2: Geldbußen, die von EU-Datenschutzbehörden wegen Verstößen gegen die DSGVO im Beschäftigungsbereich verhängt wurden



Die Grafik basiert auf öffentlich verfügbaren Daten, die von der Kanzlei CMS seit dem Inkrafttreten der DSGVO im Jahr 2018 im „GDPR Enforcement Tracker“ erfasst wurden. Da Datenschutzbehörden nicht verpflichtet sind, ihre Entscheidungen zu veröffentlichen, ist das Bild womöglich unvollständig. Fälle nach dem 15. November 2021 wurden nicht berücksichtigt.

Zweitens gibt es Grund zur Annahme, dass Verstöße gegen Datenschutzvorschriften bzw. deren mangelnde Durchsetzung am Arbeitsplatz besonders häufig vorkommen. Laut einer aktuellen Studie aus Polen und Deutschland kann der Umfang der Überwachung von Callcenter-Mitarbeitenden in manchen Fällen „als exzessiv bezeichnet werden“. Außerdem wird in der Studie betont, dass die DSGVO die Überwachung der Beschäftigten nicht strukturell verändert hat, zumindest soweit die Befragten wussten.³⁰ Als die britische Gewerkschaft Prospect über 7500 Arbeitnehmer*innen befragte, hatten **48 Prozent „kein Vertrauen“ oder „überhaupt kein Vertrauen“, dass sie darüber informiert waren, welche personenbezogenen Daten ihr Arbeitgeber erfasst.**³¹ Obwohl das nicht direkt beweist, dass gegen die Vorschriften verstoßen wird, lässt es doch zumindest zweifeln, ob die DSGVO für mehr Vertrauen und Transparenz bei der Verarbeitung personenbezogener Daten am Arbeitsplatz gesorgt hat.

Schon aus diesem Grund sollten Datenschutzbehörden den Datenschutz am Arbeitsplatz stärker beobachten. Es obliegt vor allem den Datenschutzbehörden zu gewährleisten, dass die Datenschutzvorschriften in der gesamten EU respektiert werden. Sie sind nach [Artikel 57](#) der DSGVO verpflichtet, die Anwendung der Datenschutzvorschriften proaktiv zu überwachen und durchzusetzen. Außerdem müssen sie allen gemeldeten Beschwerden nachgehen, sofern diese nicht offenkundig unbegründet oder exzessiv sind. Leider erfüllen die Datenschutzbehörden ihre gesetzlichen Aufgaben nicht.

Nach Berichten des europäischen Datenschutzausschusses, der Koordinierungsstelle europäischer Datenschutzbehörden, sind viele dieser Behörden nicht ausreichend finanziert. Manche Behörden melden eine Unterfinanzierung von fast 100 Prozent.³² Außerdem gibt es große Unterschiede zwischen den Budgets der einzelnen Behörden. Laut

30 J. Bronowicka at al, 21, 39.

31 Prospect, „Union Reveals that Half of Workers Don’t Know What Data their Boss Collects About Them“, 12. Februar 2020, auf: <https://prospect.org.uk/news/union-reveals-that-half-of-workers-dont-know-what-data-their-boss-collects-about-them/>

32 Europäischer Datenschutzausschuss, „First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities“, 26. Februar 2019, 7, auf: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/

einem vor kurzem veröffentlichten Bericht des Irish Council for Civil Liberties verfügen die Datenschutzbehörden in Deutschland über 32 Prozent des Gesamtbudgets aller europäischen Datenschutzbehörden. Gleichzeitig **muss die Hälfte aller Behörden immer noch mit einem Budget von 5 Millionen Euro oder (wesentlich) weniger zurechtkommen.**³³ Das führt dazu, dass die Bearbeitung von Beschwerden sehr lange dauert, Entscheidungen nicht angemessen umgesetzt und kaum Geldbußen verhängt werden. Wenn Datenschutzbehörden begründeten Beschwerden nicht nachgehen, stellt dies eine Verletzung ihrer Aufsichtspflicht dar, gegen die vor Gericht geklagt werden kann. Allerdings sollten Beschwerdeführer nicht gezwungen sein, die Behörden, die sie schützen sollen, zu verklagen, um ihre Rechte durchzusetzen.

INFOBOX 5: Datenschutzbehörden und Verletzung der Aufsichtspflicht

In ihrem Jahresbericht 2020 gibt die niederländische Datenschutzbehörde zu, dass ihr die Mittel fehlen, um ihre gesetzlichen Aufsichtspflichten zu erfüllen. Sie meldet 1500 unbearbeitete Beschwerden und 8300 Hinweise, denen sie nicht nachgehen kann. Und was besonders problematisch ist: Sie kann keine algorithmischen Systeme überprüfen, die personenbezogene Daten verarbeiten. Die niederländische Behörde ist im europäischen Vergleich noch relativ gut ausgestattet.³⁴ Trotzdem wird algorithmisches Management am Arbeitsplatz in den Niederlanden nicht kontrolliert.

Außerdem setzten viele Datenschutzbehörden ihre knappen Ressourcen nicht immer da ein, wo sie am

meisten bewirken. So konzentrieren sie sich meist nicht auf große Konzerne, die routinemäßig die Vorschriften missachten.³⁵ Außerdem zögern viele Datenschutzbehörden, die Vorschriften mittels hoher Geldbußen aggressiver durchzusetzen. Das ist besonders problematisch, wenn sie sowieso nur wenige Fälle untersuchen. Wenn die Gefahr, erwischt zu werden und dann noch eine hohe Geldbuße zahlen zu müssen, in der Praxis sehr gering ist, haben Firmen wenige Anreize, sich regeltreu zu verhalten.

INFOBOX 6: Probleme bei der Durchsetzung der DSGVO. Eine Fallstudie

Um die Leistung der Beschäftigten zu messen, nutzte Zalando ein System namens „Zonar“, das den Beschäftigten Anreize dafür bot, die Leistung ihrer Kollegen ständig zu bewerten. Diese Bewertungen wurden in individuelle Einstufungen umgerechnet, von denen Karrierechancen, Gehaltserhöhungen und möglicherweise sogar eine weitere Beschäftigung abhingen.³⁶

Nach einer jahrelangen Untersuchung kam die Berliner Datenschutzbehörde zu dem Ergebnis, dass diese Erfassung und Speicherung personenbezogener Daten gegen die DSGVO verstößt und die „360-Grad-Leistungskontrolle“ zu einem allgegenwärtigen Überwachungsdruck auf die Arbeitnehmer*innen führen kann. Dennoch verhängte sie keine Geldbuße gegen Zalando. Stattdessen gab sie Zalandos Hinweise, wie die Software DSGVO-konform gestaltet werden kann.

[COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf](#)

33 J. Ryan und A. Toner, „Europe’s Enforcement Paralysis. ICCL’s 2021 Report on the Enforcement Capacity of Data Protection Authorities“, Irish Council for Civil Liberties, 2021.

34 Autoriteit persoonsgegevens, „Jaarverslag 2020“ (2021), 11-12, auf: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2020.pdf

35 J. Nogarede, „Governing Online Gatekeepers: Taking Power Seriously“, FEPS, 2021, 29–30; Noyb, „Luxemburg’s Watchdog Refuses to Show its Teeth to US Companies“, 25. Januar, auf <https://noyb.eu/en/luxemburgs-watchdog-refuses-show-its-teeth-us-companies>.

36 Eine detaillierte Analyse von Zalandos Software Sonar findet sich bei P. Staab und S. Geschke, „Ratings als arbeitspolitisches Konfliktfeld. Das Beispiel Zalando“, Studie 429, 2020, Hans-Böckler-Stiftung.

Dieser Fall zeigt die Probleme beim Datenschutz in Beschäftigungsverhältnissen. Erstens wurde die Datenschutzbehörde erst ein Jahr nach Eingang der ersten Beschwerden über Zonar tätig. Zweitens wurden die von der Datenschutzbehörde entwickelten Leitlinien nicht öffentlich und speziell auf Zalando zugeschnitten und es wurden keine Geldbußen verhängt, obwohl Verstöße gegen die DSGVO festgestellt wurden. Das heißt, das Eingreifen der Datenschutzbehörde wirkte sich weder pädagogisch noch abschreckend auf andere Unternehmen aus. Und zuletzt waren die Betriebsräte, die es im Unternehmen gibt (und die darin vertretenen Gewerkschaften), anscheinend nicht in der Lage, Verstöße gegen die DSGVO zu erkennen.

Und schließlich gilt die Arbeitswelt bei vielen Datenschutzbehörden nicht als Tätigkeitsschwerpunkt. Wie eine Analyse der strategischen und funktionalen Prioritäten von 12 europäischen Datenschutzbehörden zeigt, enthalten nur drei davon den Bereich Beschäftigung.³⁷ Auch der **Europäische Datenschutzausschuss erwähnt den Bereich Beschäftigung in ihrem Arbeitsprogramm für 2021-2022 kein einziges Mal.** Angesichts der durch die Coronapandemie beschleunigten Digitalisierung der Arbeitswelt, die den Schutz der personenbezogenen Daten von Arbeitnehmer*innen auf der Agenda ganz nach oben hätte katapultieren sollen, ist dies beunruhigend.

4. Für eine aktivere Rolle der Gewerkschaften

Obwohl die DSGVO ausdrücklich auch für die Daten von Arbeitnehmer*innen gilt, steckt die Formulierung von Datenschutzgrundsätzen für die Arbeits-

welt noch in den Kinderschuhen. Viele Bestimmungen wurden noch nicht ausgelegt und geklärt. Die Artikel 29 Datenschutzgruppe (die Vorgängerin des Europäischen Datenschutzausschusses) hatte zwar im Jahr 2017 eine Interpretation veröffentlicht,³⁸ viele Akteure wünschen sich jedoch zusätzliche Leitlinien zum Thema Privatsphäre und Datenschutz am Arbeitsplatz.³⁹ Im Rahmen der Überprüfung der DSGVO durch die Europäische Kommission im Jahr 2020 gaben Interessenträger zu erkennen, dass sie genauere Leitlinien zum „Geltungsbereich der Rechte der betroffenen Personen (auch im Zusammenhang von Beschäftigungsverhältnissen)“ benötigen.⁴⁰ Solche Leitlinien würden Fälle verhindern, in denen die Datenschutzvorschriften der DSGVO offensichtlich missbraucht werden, z. B. als Vorwand, um Arbeitnehmer*innen und Arbeitnehmervertreter*innen Informationen vorzuenthalten.⁴¹

Gemäß [Artikel 88](#) der DSGVO können die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen. Die meisten Mitgliedstaaten haben von dieser Möglichkeit bisher noch keinen Gebrauch gemacht. Da noch kaum Entscheidungen der Aufsichtsbehörden oder Rechtsprechung vorliegen, die eine maßgebliche Auslegung datenschutzrechtlicher Grundsätze in der Arbeitswelt bieten, wäre dies aber eine sehr hilfreiche Maßnahme.

Allerdings müssen Gewerkschaften und Arbeitnehmervertreter*innen in Unternehmen nicht auf eine Klärung in Form von nationalen Rechtsvorschriften oder Kollektivvereinbarungen warten. Die DSGVO enthält bereits Artikel, die es Arbeitnehmer*innen ermöglichen, ihre speziellen Datenschutzrechte geltend zu machen und auch die Grundrechte von Arbeitnehmer*innen in einer digitalisierten Arbeitswelt voller „People Analytics“ ganz allgemein schüt-

37 C. Kress, R. Van Eijk and G. Zanfir-Fortuna, „New Decade, New Priorities: A Summary of Twelve European Data Protection Authorities’ Strategic and Operational Plans for 2020 and Beyond“, Future of Privacy Forum, 12. Mai 2020, auf: https://fpf.org/wp-content/uploads/2020/05/FPF_DPAStrategiesReport_05122020.pdf

38 Artikel 29 Datenschutzgruppe, Stellungnahme 2/2017 über Datenverarbeitung am Arbeitsplatz, 8. Juni 2017.

39 F. Hendrickx, E. Gramano und D. Mangan, „Privacy, Data Protection and the Digitalisation of Work: How Industrial Relations Can Implement a New Pillar“, Kluwer Regulating for Globalization Blog, 26. Juni 2020, auf: <http://regulatingforglobalization.com/2020/06/26/privacy-data-protection-and-the-digitalisation-of-work-how-industrial-relations-can-implement-a-new-pillar/>

40 Europäische Kommission, SWD (2020), 115.

41 S. Stolton, „Employers Accused of Abusing EU Data Privacy Rules to Hinder Trade Unions“, Euractiv, 19. März 2020.

zen. Inzwischen ist aber deutlich geworden, dass Datenschutzbehörden allein das geltende Recht nicht an allen Arbeitsplätzen in der EU durchsetzen können. Deshalb sollten Arbeitnehmerorganisationen bei der Umsetzung der DSGVO eine aktivere Rolle übernehmen, die auch als wichtiges Sprungbrett für mehr Mitsprache der Gewerkschaften bei der Digitalisierung von Arbeitsplätzen dienen könnte.

Erstens können Gewerkschaften und ihre Vertreter*innen vor Ort Aufklärungskampagnen und Schulungen am Arbeitsplatz durchführen. Außerdem sollten sie Ressourcen gezielt dafür einsetzen, gute Arbeitsbeziehungen zum Datenschutzbeauftragten (falls im Unternehmen vorhanden) und der zuständigen Datenschutzbehörde aufzubauen, die dazu beitragen, dass das geltende Recht von Anfang an und nicht erst nach dem Eingang von Beschwerden durchgesetzt wird. Gewerkschaften können aber auch selbst eine aktive Rolle bei der Durchsetzung von Datenschutzrechten spielen. So können beispielsweise Gewerkschaften und andere gemeinnützige Organisationen gemäß [Artikel 80 Absatz 1](#) der DSGVO Arbeitnehmer*innen vertreten, in ihrem Namen bei Datenschutzbehörden Beschwerde einreichen und ihr Recht auf einen wirksamen gerichtlichen Rechtsbehelf wahrnehmen. Gewerkschaften können diese Möglichkeit nutzen, um in diesem für

INFOBOX 7: Datenschutz-Vertrauensleute

1971 beauftragte die norwegische Stahl- und Metallarbeitergewerkschaft das Forschungsinstitut „Norsk Regnesentral“ mit der Untersuchung aller neuen digitalen Technologien, die am Arbeitsplatz eingeführt wurden. Dies führte zur Schaffung von „Datenschutz-Vertrauensleuten“, die neue Technologien im Auftrag der Gewerkschaft analysieren und Veränderungen vorschlagen, die die Interessen der Arbeitnehmer*innen schützen.⁴² Seitdem erlaubt das norwegische Arbeitsrecht die Einrichtung von „Datenschutz-Vertrauensleuten“ im privaten und (bis vor kurzem) im öffentlichen Sektor.

die Arbeitsbedingungen von Arbeitnehmer*innen zentralen Bereich Präsenz und Stärke zu zeigen.

Zweitens können die Mitgliedstaaten gemäß [Artikel 80 Absatz 2](#) Gewerkschaften und andere gemeinnützige Organisationen dazu berechtigen, bei Datenschutzbehörden und Datenverantwortlichen eine Beschwerde einzulegen, wenn ihres Erachtens die Rechte einer betroffenen Person verletzt worden sind. Leider haben viele Mitgliedstaaten noch nicht von dieser Möglichkeit Gebrauch gemacht, Gewerkschaften, Verbraucherverbände und andere Organisationen der Zivilgesellschaft ein entsprechendes Beschwerderecht einzuräumen.

INFOBOX 8: Kollektive Durchsetzung der DSGVO

Nach den französischen Rechtsvorschriften zur Umsetzung der DSGVO können Gewerkschaften „Datenschutz-Verbandsklagen“ einreichen, wenn die Verarbeitung personenbezogener Daten Personen betrifft, deren Interessen von der Gewerkschaft vertreten werden. Andere Mitgliedstaaten könnten diesem Modell folgen.

5. Leicht umzusetzen: wichtige Bestimmungen der DSGVO für mehr Mitsprache der Arbeitnehmer*innen

5.1 Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Laut DSGVO ist die Verarbeitung personenbezogener Daten nur erlaubt, wenn eine ausdrückliche Rechtsgrundlage besteht. In der digitalen Wirtschaft verlassen sich Firmen oft auf die Einwilligung der Nutzer. Da die Beziehung zwischen Arbeitgeber und Arbeitnehmer hierarchisch ist, stellt die Zustimmung eines Beschäftigten jedoch in der Regel keine Einwilligung im Sinne der DSGVO dar, die eine „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung“ erfordert. Nach Einschätzung der Arti-

42 D. F. Noble, „Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools“, in: D. Preece, I. McLoughlin und P. Dawson [Hg.], *Technology, Organizations and Innovation: Critical Perspectives on Business and Management. Band 1: The early debates* (London: Routledge, 2000), 395.

kel 29 Datenschutzgruppe sind „Beschäftigte aufgrund des in der Beziehung zwischen Arbeitgeber und Arbeitnehmer begründeten Abhängigkeitsverhältnisses fast nie in der Position, ihre Einwilligung frei zu erteilen, zu verweigern oder zu widerrufen. Aufgrund der ungleichen Machtverhältnisse können Beschäftigte ihre freiwillige Einwilligung nur in Ausnahmefällen erteilen.“⁴³ Außerdem muss die Einwilligung eine für einen bestimmten Fall und in informierter Weise gegebene Willensbekundung darstellen. Diese Bedingung kann demnach durch standardmäßige Einstellungen auf Geräten oder in installierten Programmen gar nicht erfüllt sein.

Alternativ könnten Arbeitgeber die Verarbeitung personenbezogener Daten von Arbeitnehmer*innen damit rechtfertigen, dass dies zur Wahrung berechtigter Interessen erforderlich ist. Darunter könnten z. B. die Überwachung von Beschäftigten zu dem Zweck fallen, die Sicherheit der Beschäftigten oder Anlagen des Unternehmens zu schützen oder die Produktivität am Arbeitsplatz zu kontrollieren. Diese Interessen müssen jedoch immer gegen die Grundrechte der Beschäftigten abgewogen werden: Müssen sie vernünftigerweise erwarten, dass sie beobachtet werden? Im Fall einer heimlich installierten Software, die Tastatureingaben erfasst, lautet die Antwort der deutschen Justiz: Nein.⁴⁴

Selbst wenn Arbeitgeber Beschäftigtendaten zur Wahrung berechtigter Interessen verarbeiten wollen, müssen sie in jedem Fall allgemeine Grundsätze wie etwa Datenminimierung, Verhältnismäßigkeit und Transparenz beachten. Besonders letztere wird oft vernachlässigt: Arbeitgeber sollten die Arbeitnehmer*innen immer über Art, Umfang und Zwecke der Verarbeitung ihrer personenbezogenen Daten informieren.

Die Tatsache, dass sich betriebliche Softwares, die personenbezogene Daten verarbeiten, rasant verbreiten, die Einwilligung der Arbeitnehmer*innen allein für deren rechtmäßige Verwendung jedoch nicht ausreicht, eröffnet Arbeitnehmer*innen und insbesondere deren Vertreter*innen ganz neue Möglich-

INFOBOX 9: Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten

Arbeitgeber können sich bei der Einführung von Überwachungssystemen in der Regel nicht auf die Einwilligung der Arbeitnehmer*innen berufen. Die naheliegende Rechtsgrundlage ist ein berechtigtes Interesse des Arbeitgebers. Dieses muss jedoch sorgfältig gegen die Grundrechte der Arbeitnehmer*innen abgewogen werden und erforderlich, verhältnismäßig und transparent sein. Demnach verstößt die willkürliche Überwachung der Beschäftigten immer gegen die DSGVO.⁴⁵

keiten. Sie können diese Praktiken in Frage stellen und mit dem Management über die Ziele, die Verhältnismäßigkeit und die Modalitäten von Systemen diskutieren, für die personenbezogene Daten der Arbeitnehmer*innen verarbeitet werden müssen.

5.2 Datenschutz-Folgenabschätzungen

Nach [Artikel 35](#) der DSGVO sollten Arbeitgeber eine Abschätzung der Folgen für den Datenschutz durchführen, bevor sie digitale Technologien verwenden, die eine Verarbeitung personenbezogener Daten beinhalten und voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Beschäftigten zur Folge haben.⁴⁶ Was als hohes Risiko gilt, wurde von der Artikel 29 Datenschutzgruppe geklärt, und auch einzelne Datenschutzbehörden führen Listen der Fälle, in denen eine Folgenabschätzung Pflicht ist. Dazu gehören „Bewertung oder Rangordnung“, die Beteiligung besonders gefährdeter Betroffener – zu denen Beschäftigte gehören sollten – und die systematische Überwachung. Zusammen genommen bedeutet dies, dass kaum ein System, das die Leistung der Arbeitnehmer*innen überwacht und/oder bewertet, von der Pflicht ausgenommen sein sollte,

43 Artikel 29 Datenschutzgruppe (2017); siehe auch Erwägungsgrund 41 der DSGVO

44 Bundesarbeitsgericht, 27. Juli 2017, 2 AZR 681/16.

45 Die anderen Ausnahmen, beispielsweise zur Erfüllung rechtlicher Verpflichtungen (Sozialbeiträge) oder zur Erfüllung eines Vertrags (Berechnung des Gehalts) sind eng gefasst und im Regelfall unstrittig.

46 Außerdem sollten Datenschutz-Folgenabschätzungen regelmäßig wiederholt werden, insbesondere bei selbstlernenden Programmen, deren Funktionsweise sich mit der Zeit verändern kann. Siehe Artikel 29 Datenschutzgruppe (2017) WP 248, 4. April 2017, 19, auf: <https://ec.europa.eu/newsroom/article29/items/611236/en>.

Tabelle 1: Artikel 35 DSGVO: Fälle, bei denen laut Datenschutzbehörden immer eine Datenschutz-Folgenabschätzung erforderlich ist

| Land | Maßnahme | Beispiel |
|------|--------------------|---|
| NL | Leistungsbewertung | Systematische und umfassende Bewertung Einzelner, z. B. die Arbeitsleistung von Beschäftigten |
| IT | Fernüberwachung | Verarbeitung im Rahmen eines Beschäftigungsverhältnisses über technologische Systeme (Videoüberwachung, Geolokalisierung), durch die die Aktivitäten der Beschäftigten aus der Ferne überwacht werden |
| FR | Personalverwaltung | Erstellung von Profilen zum Zweck der Personalverwaltung |

insbesondere wenn das System auch zu automatisierten Entscheidungen führt.

Wenn feststeht, dass eine Folgenabschätzung erforderlich ist, muss gemäß der DSGVO ein „Datenverantwortlicher“ (der Arbeitgeber) *gegebenenfalls* den Standpunkt der betroffenen Personen oder ihrer Vertreter*innen einholen. Wenn man bedenkt, dass die DSGVO die Datenverarbeitung in Beschäftigungsverhältnissen besonders streng reguliert, ist anzunehmen, dass auch [Artikel 35](#) streng ausgelegt werden sollte. Das bedeutet, dass Arbeitgeber verpflichtet sind, bei der Folgenabschätzung für Datenverarbeitungsvorgänge, die die Beschäftigten betreffen, diese auch zu konsultieren.

Auch nach Einschätzung des Datenschutzbeauftragten des Vereinigten Königreichs (UK Information Commissioner’s Office) sollten Datenverantwortliche den Standpunkt betroffener Personen (oder deren Vertreter*innen) einholen und dokumentieren, sofern kein guter Grund dagegen spricht (der dann dokumentiert und erläutert werden sollte).⁴⁷ In Deutschland und anderen Mitgliedstaaten sind Arbeitgeber bereits durch das Arbeitsrecht verpflichtet, bei Datenschutz-Folgenabschätzungen

Arbeitnehmervertreter*innen zu konsultieren, das gilt jedoch nicht überall in der EU.

Die Beteiligung der Beschäftigten oder deren Vertreter*innen macht Folgenabschätzungen auch relevanter. Wie Studien zeigen, werden Datenschutz-Folgenabschätzungen leicht zu abstrakten Compliance-Übungen, die nicht die Risiken für die Betroffenen (Arbeitnehmer*innen) mindern oder Produkte datenschutzfreundlicher machen, sondern lediglich das Unternehmen vor Haftung schützen.⁴⁸ Wenn auch die Arbeitnehmer*innen ihre Standpunkte vertreten können, werden die negativen Auswirkungen auf ihre Grundrechte (nicht nur auf ihre Privatsphäre) eher berücksichtigt.

47 Information Commissioner’s Office, „How Do We Do a DPIA?“, auf: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how7>

48 F. Ferra, I. Wagner, E. Boiten et al., „Challenges in Assessing Privacy Impact: Tales from the Front Lines“, *Security and Privacy* 3(2) (2020).

INFOBOX 10: Datenschutz-Folgenabschätzungen

Das Management sollte die Belegschaft bei einer Datenschutz-Folgenabschätzung konsultieren. Dies ist nicht nur gesetzlich vorgeschrieben, sondern gewährleistet auch, dass die Abschätzung relevant ist und sich auf den Schutz der Arbeitnehmerrechte konzentriert.

5.3 Profiling, automatisierte Entscheidungen und die DSGVO

Wenn die personenbezogenen Daten der Arbeitnehmer*innen dazu genutzt werden, Verhalten, Interessen oder Arbeitsleistung zu analysieren oder vorherzusagen, nennt man das „Profiling“. Algorithmische Systeme können auf der Grundlage solcher Profile Entscheidungen hinsichtlich der Arbeitnehmer*innen treffen, beispielsweise zu Arbeitszeiten, Gehalt oder Beförderung. Die DSGVO schützt vor solchen Praktiken, indem sie beispielsweise für mehr Transparenz sorgt und es Arbeitnehmer*innen ermöglicht, anstelle einer automatisierten Bewertung eine menschliche Bewertung zu verlangen.

Der gemäß der DSGVO (und der davor geltenden Richtlinie) geltende Schutz vor Profiling und automatisierten Entscheidungsprozessen wurde bisher kaum genutzt und hat die Entwicklung von Informationssystemen bisher praktisch nicht beeinflusst. Manche meinen, das liege daran, dass die Bestimmungen so komplex sind.⁴⁹ Dies mag zwar stimmen, trotzdem zeigt ein sorgfältiges Studium der einschlägigen Bestimmungen, dass Arbeitnehmer*innen und ihre Vertreter*innen die DSGVO nutzen können, um Informationen über algorithmische Entscheidungen, die sie betreffen, anzufordern und deren Verwendung zu begrenzen.

Die wichtigste Bestimmung in Bezug auf automatisierte Entscheidungen ist [Artikel 22](#), nach dem

Arbeitnehmer*innen das Recht haben, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die sie erheblich beeinträchtigt. Obwohl die Bestimmung von einem Recht spricht, ist sie eigentlich als Verbot zu verstehen, was mit dem Gesamtziel der DSGVO (besserer Schutz personenbezogener Daten) übereinstimmt. Diese Lesart entspricht auch dem [Erwägungsgrund 71](#), nach dem eine „automatisierte Entscheidungsfindung, einschließlich des Profilings, erlaubt sein sollte, wenn dies gesetzlich ausdrücklich zulässig oder für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist oder wenn die betroffene Person ihre ausdrückliche Einwilligung hierzu erteilt hat.“ Wenn diese Voraussetzungen nicht erfüllt sind, sollten sie mit anderen Worten verboten sein. Dies stimmt auch mit den Leitlinien der Artikel 29 Datenschutzgruppe überein.⁵⁰

INFOBOX 11: Artikel 22 (1) DSGVO über automatisierte Entscheidungen

„Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.“

Die Ausnahmeregelung, die automatisierte Entscheidungen für die Erfüllung eines Vertrags erlaubt, gilt nur unter der Voraussetzung, dass sie „erforderlich“ ist. In der Praxis bedeutet dies, dass es keine andere Möglichkeit geben darf, den Vertrag zu erfüllen. Das lässt sich so auslegen, dass Entscheidungen über Beförderungen, Boni und insbesondere Kündigungen in keinem Fall automatisiert erfolgen dürfen, weil diese Entscheidungen nie so komplex sind, dass ein Mensch sie nicht treffen kann.⁵¹ Diese Einschätzung entspricht auch dem

49 L. A. Bygrave, „Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making“, University of Oslo Faculty of Law Legal Studies Research Paper Series Nr. 2019-01, 2019, 3-4.

50 Artikel 29 Datenschutzgruppe, „Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679“, 2017, 19.

51 A. Todolí-Signes, „Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection“, ETUI, 2019, 7-8.

allgemeinen Standpunkt der EU in Bezug auf künstliche Intelligenz, nach dem die letztliche Kontrolle immer von Menschen ausgeübt werden muss.

Zugegebenermaßen sind manche Beobachter der Ansicht, dass [Artikel 22](#) nur für vollständig automatisierte Systeme gilt. Diese Lesart würde alle Systeme ausschließen, die „Entscheidungshilfen“ liefern oder bei denen irgendwo noch ein Mensch in irgendeiner Scheinfunktion beteiligt ist.⁵² Das hätte absurde Konsequenzen, denn es würde die Arbeitnehmer*innen einigen der am meisten automatisierten Systeme zur Leistungssteuerung von Be-

schäftigten, wie dem ADAPT-System von Amazon, schutzlos ausliefern. Dieses System führt dazu, dass Arbeitnehmer nach einer Reihe automatisch erzeugter Warnungen quasi-automatisch entlassen werden. Tatsächlich sprechen sich viele Rechtswissenschaftler gegen diese enge und wörtliche Auslegung aus.⁵³

Abbildung 3: Das Leistungserfassungsprogramm ADAPT von Amazon⁵⁴

„Es wird erwartet, dass sie 100 % des vorgegebenen Produktivitätswerts erreichen. Bitte beachten Sie: Erhält ein Mitarbeiter innerhalb von 12 fortlaufenden Monaten einen zweiten letzten Beratungsbericht oder 6 dokumentierte Beratungsberichte, dann endet sein Beschäftigungsverhältnis.“

Leistungstrend. Nachstehend wird Ihre bisherige Produktivitätsleistung zusammengefasst

| Beginn | Einheiten | Arbeitsstunden | E/h | % des Gesamtwerts | % der Kurve | Ausgenommen |
|--------------------------|-----------|----------------|-----|-------------------|-------------|-------------|
| Mai 01, 2019, 5:00 Uhr | 5038 | 16 | 324 | 82,23 | 82,23 | N |
| April 24, 2019, 5:00 Uhr | 1759 | 5 | 348 | 87,9 | 87,9 | J |
| April 17, 2019, 5:00 Uhr | 0 | 0 | 0 | 0 | 0 | J |
| April 10, 2019, 5:00 Uhr | 1856 | 6 | 317 | 80,47 | 80,47 | J |
| April 03, 2019, 5:00 Uhr | 4272 | 12 | 347 | 88,28 | 88,28 | J |
| März 27, 2019, 5:00 Uhr | 0 | 0 | 0 | 0 | 0 | J |

52 S. Wachter, B. Mittelstadt und L. Floridi, „Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation“, *International Data Privacy Law* 7(2) (2017).

53 M. Veale und L. Edwards, „Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling“, *Computer Law & Security Review* 34(2) (2018); A. D. Selbst und J. Powles, „Meaningful Information and the Right to Explanation“, *International Data Privacy Law* 7(4) (2017).

54 Das Leistungserfassungssystem ADAPT von Amazon, Bewertung des Mitarbeiters Parker Knight, abgerufen auf <https://www.revealnews.org/wp-content/uploads/2019/11/Parker-Knight-productivity-report.pdf>. Siehe auch: Will Evans, „Ruthless Quotas at Amazon Are Maiming Employees“, *The Atlantic*, 5. Dezember (2019). <https://www.theatlantic.com/technology/archive/2019/11/amazon-warehouse-reports-show-worker-injuries/602530/>.

Wie Todolí-Signes überzeugend darlegt, gilt der Schutz nach [Artikel 22](#) auch dann, wenn ein Algorithmus eine „Entscheidung trifft“ und ein menschlicher Mitarbeiter diese nur *umsetzt*. Ganz allgemein argumentiert er, dass es keine vollständig automatisierten Entscheidungen gibt. Algorithmen haben keinen Willen, Entscheidungen werden immer von Menschen getroffen, entweder wenn sie den Algorithmus programmieren oder wenn sie seine Ergebnisse anwenden. Da immer eine menschliche Intervention erforderlich ist, kann die nicht bedeuten, dass solch eine Intervention Arbeitnehmer*innen daran hindern würde, sich auf die Einwände von [Artikel 22](#) zu berufen, da diese dann nie anwendbar wären.⁵⁵ Diese Lesart wird auch von Expert*innen für KI und Computer unterstützt.⁵⁶

Was die Transparenz angeht, haben Arbeitnehmer*innen das Recht zu erfahren, dass ihre Arbeit (vollständig oder teilweise) von automatisierten Entscheidungsprozessen beeinflusst wird, das Recht auf aussagekräftige Informationen über die Funktionsweise der betreffenden Algorithmen (Parameter, Gewichtung) und das Recht, etwas über die Konsequenzen dieses Prozesses zu erfahren. Dies ergibt sich aus [Artikel 22\(3\)](#), [Artikel 13\(2\)\(f\)](#) und [Artikel 14\(2\)\(g\)](#) sowie dem allgemeinen Grundsatz der Transparenz der Verarbeitung.

Zwar wird in Wachter et al. bestritten, dass es nach Erfassung der entsprechenden Informationen auch das Recht auf eine konkrete Erklärung gibt, warum die jeweilige Entscheidung getroffen wurde.⁵⁷ Doch in [Erwägungsgrund 71](#) wird daran erinnert, dass Profiling und automatisierte Entscheidungen „mit angemessenen Garantien verbunden sein sollten, einschließlich der *spezifischen* Unterrichtung der

betroffenen Personen und des Anspruchs [...], auf Darlegung des eigenen Standpunkts, auf *Erläuterung der nach einer* entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung.“ Dies spricht dafür, dass das Recht auf eine spezifische Erläuterung nach einer Entscheidung besteht.

Diese Lesart stimmt auch mit dem Zweck der Bestimmung überein, nämlich Betroffenen dabei zu helfen, für sie nachteilige unfaire und diskriminierende Entscheidungen zu erkennen und gegen diese Entscheidungen vorzugehen. Das wäre kaum möglich, wenn Arbeitgeber die Funktionsweise eines Algorithmus nur ganz allgemein erklären müssten. Dann hätten Arbeitnehmer*innen keine Möglichkeit, die Ablehnung eines Antrags oder die Gründe für eine Kündigung zu verstehen, was den Leitlinien der Artikel 29 Datenschutzgruppe widerspricht, nach denen die Erläuterung automatisierter Entscheidungen verständlich sein sollte.⁵⁸ Grundsätzlich unterstützen viele Forschende den Standpunkt, dass es ein Recht auf Erklärung gibt.⁵⁹

55 A. Todolí-Signes, „Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection“, ETUI, 2019, 7-8.

56 J. Bryson, „The Past Decade and Future of AI's Impact on Society“, in *Towards a New Enlightenment? A Transcendent Decade* (Madrid, BBVA, 2018).

57 Wachter, Mittelstadt und Floridi, „Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation“, 92.

58 Artikel 29 Datenschutzgruppe, „Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679“, 2017, 25.

59 A.D. Selbst und J. Powles, „Meaningful Information and the Right to Explanation“, *International Data Privacy Law* 7(4) (2017); Lee A. Bygrave, „Article 22“, in C. Kuner, L. A. Bygrave und C. Docksey [Hg.], *Commentary on the EU General Data Protection Regulation* (Oxford: Oxford University Press, 2019); I. Mendoza und L. A. Bygrave, „The Right Not to be Subject to Automated Decisions Based On Profiling“, in: T. Synodinou, P. Jougoux, C. Markou und T. Prastitou [Hg.], *EU Internet Law: Regulation and Enforcement* (Springer: 2017), 77–98.

INFOBOX 12: DSGVO und das Recht auf Erklärung

In einem vor kurzem zu Ende gegangenen Rechtsstreit zwischen Arbeitnehmer*innen und dem Fahrdienst-Vermittler Ola hat das Amsterdamer Regionalgericht entschieden, dass Arbeitnehmer*innen ein Anrecht darauf haben, dass das Unternehmen ihnen erläutert, auf welcher Logik und welchen Kriterien das automatisierte Entscheidungssystem beruht, das Fahrer*innen mit Geldbußen belegen kann. Außerdem entschied das Gericht, dass Arbeitnehmer*innen das Recht haben, anstelle einer voll automatisierten Entscheidung die Beurteilung durch einen Menschen zu verlangen. Obwohl das Urteil noch nicht rechtskräftig ist, deutet es darauf hin, dass sich Arbeitnehmer*innen nicht nur bei Datenschutzproblemen auf die DSGVO berufen können und dass die DSGVO tatsächlich das Recht auf eine Erklärung „voll“ automatisierter Entscheidungen begründet.⁶⁰

Die DSGVO begrenzt die Erfassung personenbezogener Daten und sieht ein Informations- und Konsultationsrecht für Arbeitnehmer*innen vor, das auch dann gilt, wenn personenbezogene Daten analysiert und für Entscheidungsprozesse verwendet werden. Dadurch bietet sie umfassende Möglichkeiten, um zu gewährleisten, dass Arbeitnehmer*innen bei der Umsetzung digitaler Technologien am Arbeitsplatz gehört und konsultiert werden.

60 Rechtbank Amsterdam, Uitspraak 11-3-2021, c/13/689705.

DER DIGITALISIERTE ARBEITSPLATZ: VOM DATENSCHUTZ ZUR DATEN-GOVERNANCE

DER DIGITALISIERTE ARBEITSPLATZ: VOM DATENSCHUTZ ZUR DATEN- GOVERNANCE

6. Wenn es um die Daten vieler geht, sollte auch die Governance kollektiv sein

Die Datenschutz-Grundverordnung konzentriert sich vor allem auf den Schutz der Rechte des Einzelnen. Immer mehr Forschende betonen jedoch, dass der Schwerpunkt auf Einzelpersonen im Zeitalter von Big Data aus den folgenden logischen, wirtschaftlichen und praktischen Gründen nicht ausreicht.

Erstens betreffen Daten rein logisch selten nur eine einzige Person. Wenn jemand Informationen über seine DNS zur Verfügung stellt, sagt dies auch etwas über seine Blutsverwandten aus, auch wenn sie gar nicht gefragt wurden. Und die Daten, die ein einzelner Mitarbeitender erzeugt (E-Mails, Standortdaten, Audioaufnahmen, Leistungserfassung) betreffen häufig auch seine Kolleg*innen.

Deshalb reicht es nicht aus, Daten-Governance ausschließlich aus der Perspektive des Individuums und der vertikalen Beziehungen zwischen der Person, deren Daten verarbeitet werden, und der (juristischen) Person, die sie verarbeitet, zu betrachten. Wie S. Viljoen darlegt, hat die Erzeugung von Daten oft mit „horizontalen Beziehungen“ zu tun, bei denen Informationen über persönliche Merkmale oder den Standort einer Person möglicherweise viele andere Personen mit ähnlichen Merkmalen betreffen.⁶¹ Deshalb sind kollektive Formen der Daten-Governance notwendig, um einerseits die Risiken zu minimieren und andererseits das Potenzial der Erfassung und Analyse (personenbezogener) Daten voll auszuschöpfen.

Zweitens liegen auch die wirtschaftlichen Gründe für die Datenproduktion nicht im Individuellen, sondern in der Masse. Der wichtigste Anreiz für die Erfassung personenbezogener Daten besteht darin, Verbindungen zwischen einzelnen Personen zu erkennen und daraus Profile zu erzeugen, mit denen sich das Verhalten von Gruppen voraussagen und beeinflussen lässt. Diese Techniken wurden zuerst in der Werbebranche entwickelt (nutzerbasierte Werbung), verbreiten sich aber inzwischen überall in Wirtschaft und Gesellschaft. Auf der Grundlage großer Mengen personenbezogener Daten bilden Firmen Profile bestimmter Verbrauchergruppen. Diese Profile berücksichtigen zwar oft bekannte Merkmale, die durch das Antidiskriminierungsrecht geschützt sind, wie Alter, Geschlecht und ethnische Herkunft, können aber hunderte von Variablen enthalten, die nicht unter das Antidiskriminierungsrecht fallen, nicht intuitiv sind und daher von den Betroffenen nur schwer erkannt und verstanden werden.⁶²

Drittens lässt sich die Erzeugung von Gruppenprofilen anhand von Daten nur schwer zu den personenbezogenen Daten zurückverfolgen, auf denen sie beruhen, weil dabei große anonymisierte Datenmengen verwendet werden. Dies erschwert es den Betroffenen, sich auf die DSGVO zu berufen.⁶³ Außerdem begründet die DSGVO zwar das Recht auf eine Erklärung algorithmischer Entscheidungen mit wesentlichen Auswirkungen, nicht jedoch das „Recht auf vernünftige Schlussfolgerungen“. Personen, die von algorithmischen Entscheidungen betroffen sind, haben keine praktische Handhabe, um zu gewährleisten, dass diese Entscheidungen auf vernünftigen Schlussfolgerungen basieren.⁶⁴

61 S. Viljoen (im Erscheinen), „Democratic Data: A Relational Theory For Data Governance“, *Yale Law Journal*.

62 Die Europäische Kommission hat Vorschläge für Rechtsvorschriften vorgebracht, um diese Probleme zu lösen, siehe: „Gesetz über digitale Märkte“, COM/2020/842 final und „Gesetz über digitale Dienste“, COM/2020/825 final.

63 A. Mantelero, „Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection“, *Computer Law & Security Review* 32 (2017), 238-55.

64 S. Wachter und B. Mittelstadt, „A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI“, *Columbia Business Law Review* 2 (2019), 12.

Das Informations- und Machtgefälle, das die digitale Wirtschaft von heute kennzeichnet, ist natürlich nicht neu und in der hierarchischen Beziehung zwischen Management und Arbeitnehmer*innen noch wesentlich stärker ausgeprägt. Um dieses Gefälle abzubauen, haben die Länder Europas schon lange ein ausgefeiltes System kollektiver Regelungsmechanismen aufgebaut, in dem Gewerkschaften, Betriebsräte und andere Institutionen dafür sorgen, dass Arbeitnehmer*innen kollektiv vertreten werden, über Entscheidungen des Managements informiert werden und diese Entscheidungen aktiv beeinflussen können.

Es gibt durchaus Versuche, diese kollektiven Systeme aus der Arbeitswelt auf den Verbraucherschutz in der digitalen Wirtschaft zu übertragen, beispielsweise durch die Gründung von „Datengewerkschaften“ für Verhandlungen mit Facebook und Konsorten⁶⁵. Ob diese Ansätze auch die Digitalisierung der Arbeitswelt erfolgreich beeinflussen können, ist jedoch eine offene Frage. Die DSGVO ermöglicht es Gewerkschaften und Arbeitnehmervertreter*innen, sich für den Datenschutz einzusetzen. Dies geht zum einen ausdrücklich aus Artikel 88 hervor, nach dem durch Kollektivvereinbarungen spezifische Datenschutzmaßnahmen eingeführt werden können. Es ergibt sich aber auch implizit aus der Bestimmung, dass die individuelle Einwilligung grundsätzlich nicht als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten angeführt werden kann, weil diese Einwilligung in einem hierarchischen Beschäftigungsverhältnis nicht freiwillig ist.

7. Kollektive Lösungen: Informations- und Mitbestimmungsrechte

Das Arbeitsrecht sichert den Arbeitnehmer*innen gewisse Informations- und Mitbestimmungsrechte und stellt auf europäischer Ebene bis hinunter zu einzelnen Unternehmen genau die kollektiven

Mechanismen bereit, die Arbeitnehmer*innen den Einfluss auf die technologische Entwicklung geben, der im Datenschutzrecht derzeit nicht vorgesehen ist. Sie können am besten gewährleisten, dass die Digitalisierung zu mehr Produktivität und zu besseren Arbeitsbedingungen führt. Allerdings ist der praktische Schutz und der kollektive Einfluss der Arbeitnehmer*innen innerhalb Europas aus mehreren Gründen sehr unterschiedlich ausgeprägt.

7.1 Mitarbeitervertretung im Unternehmen

Erstens ist die Vertretung der Beschäftigten auf Firmenebene durch Betriebsräte in Ländern wie Deutschland hoch entwickelt, wo die Betriebsräte jeder neuen Technologie am Arbeitsplatz zustimmen müssen. In vielen Ländern Süd- und Osteuropas sind Betriebsräte dagegen weniger verbreitet und haben da, wo es sie gibt, nur das Recht, nach einer Entscheidung informiert zu werden. Während die Beschäftigten in Ländern wie Deutschland, Frankreich und der Tschechischen Republik in den Vorständen großer Unternehmen vertreten sein müssen, kommt das z. B. in den baltischen Ländern gar nicht und in Italien, Spanien, Portugal und den meisten anderen europäischen Ländern nicht in der Privatwirtschaft vor.⁶⁶

Allerdings fehlen selbst in Deutschland in vielen Unternehmen Strukturen zur Teilhabe und Mitbestimmung. **So waren in Deutschland, dem EU-Land, in dem Rechtsrahmen und Praxis mit am weitesten entwickelt sind, 2019 weniger als 40 Prozent aller Arbeitnehmer*innen in Unternehmen mit einem Betriebsrat beschäftigt.**⁶⁷ Besonders in kleinen Unternehmen fehlen oft Strukturen für die Mitwirkung der Arbeitnehmer*innen. Das ist ein Problem, weil KMU besonders häufig standardisierte Personalsoftware ohne die notwendigen Sicherheitsvorkehrungen nutzen. Dies stellt das offizielle politische Ziel der EU in Frage, die schnelle Digitalisierung der KMU in ganz Europa zu gewährleisten.⁶⁸

65 Siehe z. B. die niederländische Initiative zur Gründung einer Datengewerkschaft, die kollektiv mit Facebook und Google über deren Umgang mit Nutzerdaten verhandeln soll, auf: <https://thedataunion.eu>

66 Siehe die Datenbank des Europäischen Gewerkschaftsinstituts zur Mitbestimmung von Arbeitnehmer*innen in Europa, auf: <https://www.worker-participation.eu>

67 Im ehemaligen Westdeutschland arbeiteten nur 41 Prozent der Beschäftigten in Unternehmen mit einem Betriebsrat (von den Unternehmen mit 5 oder mehr Beschäftigten). In der ehemaligen DDR war der Anteil mit 36 Prozent der Beschäftigten noch geringer. Siehe P. Ellguth, „Ost- und Westdeutschland nähern sich bei der Reichweite der betrieblichen Mitbestimmung an“, IAB-FORUM, 13. Mai 2020, auf: <https://www.iab-forum.de/ost-und-westdeutschland-naehern-sich-bei-der-reichweite-der-betrieblichen-mitbestimmung-an/>

68 Siehe Europäische Kommission, „Digitaler Kompass 2030“ (2021), COM/2021/118 final.

INFOBOX 13: Betriebsräte in Deutschland

Selbst in Deutschland, das bei der Mitarbeiterbeteiligung eine Führungsrolle einnimmt, gibt es nur in 40 Prozent aller Firmen mit über 5 Beschäftigten einen Betriebsrat mit unterschiedlicher Kapazität. Das heißt, dass in Deutschland die Arbeitnehmer*innen in den meisten Unternehmen keinen konkreten Einfluss auf die Einführung neuer Technologien haben. In vielen anderen europäischen Ländern ist die Lage noch schlechter.

Außerdem werden die Entscheidungen in großen Unternehmen, auch zu Gestaltung und Funktionsweise technischer Systeme, immer mehr zentralisiert und in der Hierarchie nach oben verlagert. So gaben in einer von der IG Metall durchgeführten Befragung von Betriebsräten und Vertrauensleuten aus fast 2000 Unternehmen **87 Prozent der Betriebsräte an, dass über wichtige Veränderung auf Unternehmens- und Konzernebene entschieden wird.**⁶⁹ Aber auch die Unternehmen und einzelnen Branchen werden immer stärker konzentriert.⁷⁰ Auf technischer Ebene führen die „agile Revolution“ und der Umstieg auf cloudbasierte Softwarelösungen dazu, dass mehr und mehr Systeme regelmäßig von großen Cloud-Anbietern überarbeitet werden.⁷¹ Diese oft weltweit tätigen Firmen schützen ihre Software mit Rechten des geistigen Eigentums und den Verweis auf Betriebsgeheimnisse und verhindern damit eine Überprüfung durch externe Stellen.⁷²

Laut einer umfassenden Untersuchung des europäischen Markts für Programme zur Mitarbeiterüber-

wachung und Managementsoftware durch Cracked Labs hat die Umstellung auf Cloud-Dienste Dritter dazu geführt, dass die Unternehmen die von ihnen genutzte Soft- und Hardware nicht mehr direkt kontrollieren. Der Autor stellt fest, dass die Funktionsweise der Software und die Datenverarbeitungsprozesse stark standardisiert sind und sogar interne IT-Abteilungen kaum noch verstehen, was genau in der Cloud passiert.⁷³

Vor diesem Hintergrund ist es nicht überraschend, dass Arbeitnehmervertreter*innen in der Praxis nicht alle Software-Updates wirksam überprüfen (oder gar mitgestalten) können, obwohl dies gesetzlich vorgeschrieben ist. So ergab beispielsweise die Befragung von Betriebsratsmitgliedern in Österreich, dass sehr viele algorithmische Prozesse von Betriebsräten nicht wirklich geprüft werden, was vermutlich einen Gesetzesverstoß darstellt.⁷⁴

Dass Betriebsräte Probleme haben, mit der technischen Entwicklung Schritt zu halten, bestätigen auch die – zugegebenermaßen begrenzten – Daten und Studien, die zu diesem Thema zu finden sind. Eine Analyse von über 1100 Tarifverträgen, die in italienischen Unternehmen zwischen 2015 und 2018 geschlossen wurden, betont beispielsweise, dass Gewerkschaften und Arbeitnehmervertreter*innen grundsätzlich einen defensiven Ansatz verfolgen und vor allem versuchen, Arbeitnehmer*innen vor invasiven Überwachungs- und Kontrollmechanismen zu schützen. Laut den Autoren „sind nur gelegentlich erste Anzeichen für eine stärker proaktive Rolle der Arbeitnehmervertreter*innen zu erkennen, die so weit reicht, dass auch die Zwecke und Abläufe der Datenverarbeitung mitbestimmt werden und versucht wird, in die Digitalisierung eine soziale und kollektive Perspektive zu integrieren.“⁷⁵

69 K. Schäfers und J. Schroth, „Industrie 4.0 im Sinne der Beschäftigten. Das Projekt „Arbeit+Innovation“ der IG Metall“, Reihe „Gewerkschaften im Wandel 4.0“, Friedrich-Ebert-Stiftung, September 2021, 11.

70 Siehe z. B. J. De Loecker und J. Eeckhout, „Global Market Power“, NBER Working Paper 24768 (2018).

71 S. Gürses und J. van Hoboken, „Privacy After the Agile Turn“, in: Evan Selinger et al. [Hg.], *Cambridge Handbook of Consumer Privacy* (Cambridge: Cambridge University Press, 2018).

72 Siehe O. Lobel, „The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property“, *Texas Law Review* 93(789) (2015), und J. Cohen, *Between Truth and Power. The Legal Constructions of Informational Capitalism* (New York, Oxford University Press, 2019).

73 Cracked Labs, 75-6.

74 Cracked Labs, 137-43.

75 E. Dagnino und I. Armaroli, „A Seat at the Table: Negotiating Data Processing in the Workplace“, *Comparative Labor Law & Policy Journal* (2020), 173-95.

Weil KI-Systeme dynamisch sind und als selbstlernende System auch nach der Inbetriebnahme ihre Merkmale ändern können, müssten Betriebsräte ihre Verwendung außerdem laufend überwachen. Anstatt einfach der Verwendung eines Programms zuzustimmen, müssen Betriebsräte regelmäßige Gespräche mit dem Management und Mechanismen zur Konfliktlösung fordern, die Anpassungen erlauben, wenn sich das System ändert.⁷⁶

Gewerkschaften müssen aber auch praktische Instrumente bereitstellen, mit denen Betriebsräte neue Technologien überprüfen und die Prozesse beeinflussen können. Eines dieser Instrumente ist der „Kompass Digitalisierung“, den die IG Metall gemeinsam mit Forschenden entwickelt hat.⁷⁸

7.2 Die Rolle der Gewerkschaften

Wenn Betriebsräten die nötigen Kapazitäten fehlen, müssen die Gewerkschaften aktiv werden und die Arbeitnehmer*innen und ihre Vertreter*innen im Unternehmen praktisch und mit Know-how unterstützen. In Deutschland ist die IG Metall sehr aktiv am (digitalen) Umbau der Arbeitswelt beteiligt und stellt Arbeitnehmervertreter*innen vor Ort Schulungen, technisches Wissen und Ressourcen zur Verfügung (siehe Infobox 14).

Der gewerkschaftliche Organisationsgrad und die Kapazität der Gewerkschaften sind jedoch je nach Branche und Land sehr unterschiedlich. Während in Schweden, Dänemark, Finnland und den anderen skandinavischen Ländern die Gewerkschaftsdichte mit einem Durchschnitt von 64,7 Prozent sehr hoch ist, liegt sie in anderen Teilen der EU weit darunter (siehe Tabelle 2 auf der nächsten Seite).

INFOBOX 14: IG Metall und die Industrie 4.0

Mit ihrer Projektreihe „Arbeit+Innovation“ unterstützt die IG Metall Betriebsräte und Vertrauensleute dabei, ihre Informations- und Mitbestimmungsrechte im Unternehmen wahrzunehmen und dadurch den technologischen Wandel der Arbeitswelt mitzugestalten. Die Reihe konzentriert sich auf Schulungen, Hilfe bei der praktischen Umsetzung von Prozessen am Arbeitsplatz und Unterstützung durch ein Netzwerk externer Expert*innen (Wissenschaftler*innen, Beratungsfirmen).⁷⁷

76 T. Albrecht und C. Kellermann, „Artificial Intelligence and the Future of the Digital Work-Oriented Society“, Friedrich-Ebert-Stiftung, Oktober 2020, auf: <https://socialdialogue.fes.de/news-list/e/artificial-intelligence-and-the-future-of-the-digital-work-oriented-society>

77 K. Schäfers und J. Schroth, „Industrie 4.0 im Sinne der Beschäftigten. Das Projekt „Arbeit+Innovation“ der IG Metall“.

78 T. Albrecht und D. Gerst, „Designing Work in a Digitalising World“, *Social Europe Journal* 18. Mai 2021, auf: <https://socialeurope.eu/designing-work-in-a-digitalising-world>

Tabelle 2: Gewerkschaftsdichte in Europa (2018)

| | Nord | Mittel/West | Süd | West | Mittel/Ost |
|--------------------------|-------------|---------------------------|--------------------|----------------|--|
| Gewerkschafts- dichte | 64,7 % | 29,1 % | 19,1 % | 37,8 % | 27,1 % |
| Länder | DK, FI, SE | AT, BE, DE, LU, NL, SI | ES, FR, GR, IT, PT | CY, IE, MT, UK | BG, CZ, EE, HR, HU, LT, LV, PL, RO, SK |

Quelle: Torsten Müller, „Tarifverhandlungssysteme in Europa. Ein paar stilisierte Fakten“, ETUI, 2020; auf Grundlage der OECD-AIAS ICTWSS Datenbank (2021).

Außerdem erreichen Gewerkschaften nicht alle Arbeitnehmer*innen. In der Plattformwirtschaft werden Arbeitnehmer*innen z. B. oft wie Selbständige behandelt, obwohl sie ausgeklügelten Formen der algorithmischen Überwachung und Kontrolle unterliegen. Deshalb fehlen ihnen die kollektiven Verhandlungs- und Schutzmechanismen, die Beschäftigte – zumindest theoretisch – genießen und damit Informations-, Beteiligungs- und Mitbestimmungsrechte in Bezug auf neue Technologien. Damit Plattformbeschäftigte verstehen können, wie sie kontrolliert und ob sie fair behandelt oder diskriminiert werden, reicht es nicht, individuelle Daten anzufordern, was inzwischen dank der DSGVO möglich, wenn auch weiterhin unpraktisch ist.

Auch wenn einzelne Uber-Fahrer mit Hilfe der DSGVO Informationen über die personenbezogenen Daten anfordern können, die über sie am Arbeitsplatz erfasst werden, ist die Aussagekraft dieser Informationen beschränkt. Nur wenn sie ihre Daten mit denen anderer Uber-Fahrer kombinieren, können sie aus den Daten verwertbare Informationen ableiten.

Aber auch für (noch nicht) Beschäftigte reicht der Geltungsbereich des Arbeitsrechts womöglich nicht aus. So suchen Arbeitgeber inzwischen oft in sozialen Medien nach Informationen über Stellenbewerber und bewerten anhand dieser Informationen deren Beschäftigungsfähigkeit und künftige Leistung, bevor überhaupt ein Beschäftigungsvertrag zustande kommt. Oder sie erfassen, welchen Browser Stellenbewerber für Online-Tests verwenden, um ihre künftige Leistung zu bewerten.⁷⁹

7.3 Die Sozialpartner auf EU-Ebene: Die Rahmenvereinbarung zur Digitalisierung

Angesichts der rasanten Digitalisierung der Arbeitswelt, die oft von weltweit agierenden Konzernen vorangetrieben wird, könnte man erwarten, dass sich die Sozialpartner auf europäischer Ebene der Sache annehmen und strukturelle Schutzmaßnahmen entwickeln, die für Arbeitnehmer*innen auf betrieblicher Ebene nur schwer erreichbar wären. Tatsächlich haben die Sozialpartner auf europäischer Ebene im Juni 2020 eine Rahmenvereinbarung zur Digitalisierung verabschiedet.⁸⁰

79 D. Peck, „They’re Watching You at Work“, *The Atlantic*, Dezember (2013), auf: <https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/>

80 BusinessEurope, SMEunited, CEEP und der ETUC, „European Social Partners Framework Agreement on Digitalisation“, Juni 2020, auf: https://www.etuc.org/system/files/document/file2020-06/Final%2022%2006%2020_Agreement%20on%20Digitalisation%202020.pdf.

Das Dokument erkennt an, dass die Digitalisierung von Arbeitsplätzen zu Problemen bei der Arbeitsorganisation, den Arbeitsbedingungen und der Qualifikationen führen kann und spricht sich für einen „partnerschaftlichen Ansatz zwischen Arbeitgebern, Arbeitnehmer*innen und ihren Vertreter*innen“ und die „Entwicklung eines am Menschen orientierten Ansatzes zur Integration digitaler Technologien in die Arbeitswelt“ aus. Allerdings enthält die Vereinbarung weder eine verbindliche Interpretation der DSGVO und ähnlicher Rechtsvorschriften noch eine klare Leitlinie, wie ihre Bestimmungen in der Arbeitswelt umgesetzt werden sollen. Stattdessen setzt sie voraus, dass die konkreten Probleme der Digitalisierung kontextabhängig sind und daher nicht auf EU-Ebene kollektiv gelöst werden können.

Die Vereinbarung behandelt vier Bereiche: digitale Kompetenzen und der Schutz von Arbeitsplätzen, Modalitäten für die Verbindung und Trennung, künstliche Intelligenz und der Grundsatz, dass die Kontrolle immer von Menschen ausgeübt werden muss sowie Überwachung und der Respekt der Menschenwürde. Unter diesen Überschriften **zählt die Vereinbarung allgemeine Grundsätze und freiwillige Maßnahmen auf, die aber nicht detailliert ausgeführt oder nach ihrer Priorität geordnet sind.**⁸¹ Deshalb bieten sie Arbeitnehmervertreter*innen auf nachfolgenden Ebenen vermutlich nur wenig praktische Hilfestellung.

Die Vereinbarung konzentriert sich auf Verfahren und überlässt die Inhalte dezentralen Verhandlungen am Arbeitsplatz oder in geringerem Umfang in Kollektivverhandlungen. Da die Vereinbarung an vielen Stellen auf nationale Verfahren und Praktiken verweist, hängt in der Praxis viel davon ab, ob die Beteiligung und Mitbestimmung der Arbeitneh-

mer*innen im jeweiligen Mitgliedstaat gesetzlich garantiert ist und ob Betriebsräte und Gewerkschaften genug Macht und Kapazitäten haben, um ein Mitspracherecht einzufordern. Wie bereits erläutert, sind sowohl die Gesetze in den einzelnen Mitgliedstaaten als auch die Kapazitäten der Gewerkschaften und Betriebsräte zwischen den unterschiedlichen Mitgliedstaaten der EU und innerhalb von ihnen sehr unterschiedlich.

INFOBOX 15: Werkzeugkasten für Betriebsräte

2017 veröffentlichte die UNI Global Union 10 Grundsätze für den Schutz von Beschäftigten. Zusammen bilden sie einen Rahmen für Daten-Governance am Arbeitsplatz und können Gewerkschaften und Betriebsräten in ganz Europa als Leitlinie dienen.⁸² Daneben hat das Why Not Lab die einzelnen Phasen des Datenlebenszyklus und deren Bedeutung für Arbeitnehmervertreter*innen beschrieben.⁸³

2021 veröffentlichte AlgorithmWatch einen Leitfaden, der Betriebsräte dabei unterstützt, KI-gestützte Systeme zu prüfen, die am Arbeitsplatz eingeführt werden. Der Leitfaden enthält detaillierte Fragen zur Funktionsweise der Software, Verfahren zur Qualitätssicherung und die Art und Weise, wie das neue System in das Unternehmen integriert wird.⁸⁴

81 Siehe auch I. Senatori (2020) „The European Framework Agreement on Digitalisation: a Whiter Shade of Pale?“, *Italian Labour Law e-Journal* 13 (2) 2020.

82 UNI Global Union, „10 Principles for Workers’ Data Rights and Privacy“ (2017).

83 Christina Colclough, „Workers’ Rights: Negotiating and Co-governing Digital Systems at Work“, *Social Europe* September (2020).

84 S. Stiller, J. Jäger und S. Gießler, „Automatisierte Entscheidungen und Künstliche Intelligenz im Personalmanagement: Ein Leitfaden zur Überprüfung essenzieller Eigenschaften KI-basierter Systeme für Betriebsräte und andere Personalvertretungen“, 2. März 2020, AlgorithmWatch, auf: https://algorithmwatch.org/de/wp-content/uploads/2020/03/AlgorithmWatch_AutoHR_Leitfaden_2020.pdf.

8. Die Gesetzgebungsagenda der EU – Daten und Algorithmen regulieren

Die Europäische Kommission hat erkannt, dass die rechtliche Regulierung zum Thema Daten fundamentale Schwächen aufweist. Zurzeit saugen sich große Tech-Unternehmen mit Daten voll, während nützlichere Formen des Datenaustauschs nur langsam in Gang kommen, weil geeignete rechtliche Strukturen fehlen. Der Europäischen Kommission ist auch bewusst, dass bestimmte Probleme mit algorithmischen Systemen, insbesondere Sicherheitslücken sowie mangelnde Transparenz und menschliche Überwachung, Maßnahmen erfordern, die über die Rechte und Pflichten im Rahmen der DSGVO hinaus gehen. Aus diesem Grund hat sie eine Reihe von Legislativvorschlägen veröffentlicht, um den Zugang zu Daten zu erleichtern, das Daten-Governance-Ökosystem zu verbessern und die Sicherheit algorithmischer Systeme auf dem Binnenmarkt zu gewährleisten.

Diese Vorschläge zeigen zwar vielversprechende Ansätze, um den Schutz von Bürger*innen und Arbeitnehmer*innen zu verbessern, sie werden ihren Zweck aber vermutlich nicht erreichen, weil keine funktionierenden Institutionen für ihre Um- und Durchsetzung vorgesehen sind.

8.1 Das Daten-Governance-Gesetz und andere Initiativen

Während große Tech-Unternehmen die Daten von Millionen Bürger*innen aggregieren und dabei kaum Transparenz bieten, haben diese Bürger*innen kaum Möglichkeiten, ihre Interessen kollektiv zu vertreten. Datenschutzgesetze bieten tatkräftigen Menschen die Möglichkeit, Zugang zu ihren personenbezogenen Daten zu erhalten. Sie bieten aber keine kollektiven Regelungsmechanismen, die vorteilhaftere Formen des Datenaustauschs und Gegengewichte bieten können. Arbeitnehmer*innen, von denen viele

nach dem Arbeitsrecht nicht einmal echte Teilhabe- und Informationsrechte genießen, stehen vor einem ähnlichen Problem.

Das gilt z. B. für Plattformbeschäftigte, die für einen echten Erkenntnisgewinn aggregierte Daten bräuchten, an die sie aber nicht kommen. Auch wenn einzelne Uber-Fahrer mit Hilfe der DSGVO Informationen über die personenbezogenen Daten anfordern können, die über sie am Arbeitsplatz erfasst werden, ist die Aussagekraft dieser Informationen beschränkt. Nur wenn sie ihre Daten mit denen anderer Uber-Fahrer kombinieren, können sie verwertbare Informationen ableiten. Außerdem verwenden Uber und andere Gig-Plattformen die Daten der Arbeitnehmer*innen, um ihre Algorithmen zu trainieren und zu verbessern, die sie dann über das Urheberrecht und Rechtsvorschriften zum Schutz von Betriebsgeheimnissen schützen.⁸⁵ In den Worten von Professor Brishen Rogers: „Uber hat das stillschweigende Wissen und Handwerkszeug einzelner Fahrer gekapert oder repliziert und vermietet es jetzt an die Fahrer zurück.“⁸⁶

Dieses Problem ließe sich nur mit einer Art „Daten-Treuhandenschaft“ lösen. Laut Mozillas Data Futures Lab ist ein Daten-Treuhänder ein Mittler, „der Daten(-rechte) im Auftrag von Begünstigten mit deren Einwilligung und für einen definierten Zweck verwaltet“.⁸⁷ Mit dem vorgeschlagenen Daten-Governance-Gesetz von 2020 will die Europäische Kommission die Einführung solcher Datenmittler erleichtern.⁸⁸

INFOBOX 16: Beispiele für Daten-Treuhandschaften, Mozillas Data Futures Lab

Datengenossenschaften: die Zusammenlegung von Daten durch Einzelne oder Organisationen zum Nutzen der Gruppe. Ein gutes Beispiel ist „Driver’s Seat“, eine Genossenschaft privater

85 O. Lobel, „The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property“, *Texas Law Review* 93(789) (2015).

86 B. Rogers, „The Law and Political Economy of Workplace Technological Change“, *Harvard Civil Rights-Civil Liberties Law Review* 55 (2021), S. 562.

87 Mozilla Insights, „Data Futures Lab Glossary“, auf <https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/data-futures-lab-glossary/>.

88 Europäische Kommission, „Vorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz)“, COM/2020/767 final.

89 J. van Geuns und A. Brandescu, „Shifting Power Through Data Governance“, September 2020, Mozilla Insights.

Autobesitzer, die sich gegenseitig Zugang zu ihren Daten gewähren und so Wissen generieren können, dass sonst nur Fahrdienst-Anbieter wie Uber, Lyft und Ola besitzen.

Daten-Trusts: ein Rechtskonstrukt, bei dem ein Treuhänder Daten im Interesse mehrerer Treuehmer verwaltet. Obwohl das Konzept aus Ländern mit britischer Rechtstradition (USA, Großbritannien) kommt, möchte die EU auf europäischer Ebene mit dem Vorschlag für ein Daten-Governance-Gesetz ähnliche Konzepte einführen.

Obwohl die Verhandlungen über das Daten-Governance-Gesetz noch nicht abgeschlossen sind, wird es vermutlich wertvolle Begriffe einführen, z. B. Dienste für die gemeinsame Datennutzung, die treuhänderischer Pflichten erfüllen müssen. Das bedeutet, diese neuen Daten-Treuhänder müssen im besten Interesse der Personen handeln, deren Daten sie verwalten. Dies könnte zu neuen und besseren Geschäftsmodellen für die gemeinsame Datennutzung führen. Der Vorschlag deckt die gemeinsame Nutzung personenbezogener Daten ab, sieht aber derzeit nicht die Möglichkeit vor, in der DSGVO garantierte Rechte auf Datengenossenschaften zu übertragen oder zu delegieren. Dies würde vermutlich die Wirksamkeit der Verordnung mindern, weil Datengenossenschaften ihre Mitglieder nicht wirksam vertreten können, mit Ausnahme der begrenzten Möglichkeiten, die die DSGVO schon bietet.⁹⁰

Dennoch löst der Vorschlag nicht die Regelungsprobleme, die zu erwarten sind, wann immer mehr Daten gemeinsam genutzt werden. Wie Sean McDonald dargelegt hat, enthält das Gesetz zwar Bedingungen für EU-weit tätige Marktteilnehmer, die Dienste für die gemeinsame Datennutzung anbieten, die Aufgabe, die Einhaltung dieser Vorschriften zu überwachen und potenzielle politische Konflikte zu lösen, wird jedoch nationalen Institutionen überlassen.⁹¹ Vermutlich gehören dazu die Datenschutzbehörden, die schon ihren bisherigen gesetzlichen Aufgaben nicht gerecht werden.

Das Daten-Governance-Gesetz sieht das Recht vor, Beschwerde gegen einen Anbieter von Diensten für

die gemeinsame Datennutzung einzulegen, und das Recht auf einen wirksamen gerichtlichen Rechtsbehelf. Diese Rechte müssen aber letztlich von Behörden geschützt werden, die schon jetzt überlastet sind. Als einzige Stelle auf europäischer Ebene ist der „Europäische Dateninnovationsrat“ vorgesehen. Diese Expertengruppe hat keine rechtlichen Befugnisse und muss sich auf Überredung und informellen Druck verlassen, um in der EU gewisse Mindeststandards durchzusetzen. Wenn man die Erfahrungen mit der DSGVO zugrunde legt, die über einen stärkeren Koordinationsmechanismus auf EU-Ebene verfügt, dürfte dies kaum ausreichen.

Alles in allem hat das Daten-Government-Gesetz das Potenzial, verantwortungsbewusstere Geschäftsmodelle für die gemeinsame Nutzung von Daten zu schaffen und könnte insbesondere Arbeitnehmer*innen in der Gig-Ökonomie dabei helfen, ihre Verhandlungsmacht mit Hilfe aggregierter Daten zu stärken. Andererseits fehlen ergänzende Institutionen sowie Kontroll- und Rechtsmechanismen, was die wirksame Umsetzung des Gesetzes komplizieren dürfte.

Die vorgeschlagenen Gesetze über digitale Dienstleistungen und digitale Märkte vernachlässigen generell Probleme in Beschäftigungsverhältnissen, könnten aber wie das Daten-Government-Gesetz dazu beitragen, zumindest zuständigen Behörden und in bestimmten Fällen zugelassenen Forschenden und gewerblichen Nutzern einen vereinfachten Zugang zu den Daten der größten Plattformen zu gewähren. Außerdem werden Online-Plattformen zu Transparenz in Bezug auf die Nutzungsbedingungen und auf die Algorithmen und Empfehlungssysteme verpflichtet, die sie verwenden. Die Pflichten hinsichtlich des Datenzugangs und einer Prüfung durch externe Stellen gelten jedoch nur für die ganz großen Plattformen, was die meisten, wenn nicht alle Plattformen der Gig-Ökonomie ausschließt. Deshalb werden diese Gesetzesvorschläge nicht dazu beitragen, Formen von systematischer Diskriminierung, von denen Plattformbeschäftigte möglicherweise betroffen sind, aufzudecken und zu bekämpfen.

8.2 Der regulatorische Rahmen für KI

Die DSGVO hat (noch) nicht zur Schaffung und Entwicklung von Programmen geführt, die die Rechte

90 Europäische Kommission, „Vorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz)“, COM/2020/767 final, Erwägungsgrund 24.

91 S. McDonald, „A Novel, European Act of Data Governance“, Centre for International Governance Innovation, 2020.

der Arbeitnehmer*innen an ihren Daten sowie ihre Autonomie und ihre Teilhabe an einem digitalisierten Arbeitsumfeld schützen. Auch die Systeme der Mitbestimmung und Teilhabe von Arbeitnehmer*innen konnten anscheinend noch nicht erfolgreich in digitale Systeme überführt werden. Dafür gibt es viele Gründe, angefangen von schwachen Rechten und Durchsetzungslücken, über die fehlende technische Kapazität der Gewerkschaften bis zu den algorithmischen Systemen selbst, die oft cloudbasiert sind, sehr oft geändert werden und (absichtlich) schwer zu verstehen sind. Deshalb verschärft die digitale Transformation die Informationsasymmetrie zwischen Arbeitnehmer*innen und Management.

Vor diesem Hintergrund ist der von der Europäischen Kommission vorgeschlagene Rechtsrahmen für KI eine vielversprechende Initiative.⁹² Mit dem Vorschlag will die Kommission die Sicherheit algorithmischer Systeme verbessern, sie leichter verständlich machen und Entwickler und Nutzer zu mehr Transparenz und Rechenschaftspflicht in Bezug auf Nutzung und Auswirkungen dieser Systeme zwingen. Als Verordnung würde die künftige Rechtsvorschrift direkte rechtliche Verpflichtungen für alle Akteure schaffen, die KI-Systeme mit hohem Risiko betreiben, einsetzen oder nutzen. In Bezug auf Beschäftigungsverhältnisse entspricht die vorgeschlagene Verordnung jedoch nicht den Erwartungen. Sie berücksichtigt nur Entwickler und „Nutzer“, also in der Regel Unternehmen und Arbeitgeber, berücksichtigt aber weder Arbeitnehmer*innen noch Verbraucher*innen.

Der Rechtsrahmen stuft KI-Systeme, die zur Verwaltung von Arbeitnehmer*innen und als Arbeitszugang für Selbständige genutzt werden, als Systeme mit hohem Risiko ein. Darunter fallen z. B. die Verwendung algorithmischer und automatisierter Systeme für die Einstellung und Entlassung von Arbeitnehmer*innen, die Verteilung von Arbeitsaufgaben und die Leistungsüberwachung. Laut dem Entwurf bedeutet die Klassifizierung von KI-Systemen am Arbeitsplatz als Hochrisiko-KI-System, dass die Eingabedaten für das System relevant und re-

präsentativ sein müssen. Außerdem müssen diese Systeme einer angemessenen menschlichen Aufsicht unterliegen, die durch ihre Struktur erleichtert werden muss.⁹³ Der Schwerpunkt auf der Konzeption der Systeme erinnert an den Ansatz der DSGVO, die ebenfalls zu einem eingebauten Datenschutz verpflichtet.

Allerdings ist überhaupt nicht klar, wie solche abstrakten Grundsätze konkret umgesetzt werden sollen.⁹⁴ So müssen Hochrisiko-KI-Systeme gemäß dem Verordnungsentwurf so konzipiert werden, dass sie von Menschen wirksam beaufsichtigt werden können. Außerdem müssen die für Hochrisiko-KI-Systeme verwendeten Daten repräsentativ und relevant sein. Wer aber entscheidet, was ein angemessenes Konzept ist und wann Daten repräsentativ sind? Dafür braucht es eine enge Zusammenarbeit zwischen Interessenträgern wie der Zivilgesellschaft, Arbeitnehmervertreter*innen, der Softwarebranche, der Wissenschaft und den Behörden. Dies wird in der Verordnung aber nicht thematisiert. Solange Normen, Regeln und Institutionen fehlen, werden diese Fragen wahrscheinlich von Arbeitgebern und der Softwarebranche beantwortet. Schließlich könnte man auch fragen, ob so wichtige Fragen wie Entlassungen wirklich nur als hoch riskant eingestuft oder nicht eher ganz von automatischen Entscheidungsprozessen ausgenommen werden sollten.

Weil das vorgeschlagene „KI-Gesetz“ keine konkreten Beteiligungs-, Konsultations- und Beschwerderechte für Arbeitnehmer*innen und ihre Vertreter*innen vorsieht (für andere Bürger*innen übrigens ebenso wenig), liegt die ganze Verantwortung auf Softwareentwicklern und einzelnen Arbeitgebern, die KI-Systeme am Arbeitsplatz verwenden. Sie müssen selbst prüfen und gewährleisten, dass die Verordnung eingehalten wird. In Bezug auf die DSGVO haben Untersuchungen jedoch gezeigt, dass die darin vorgesehenen Instrumente zur Minderung von Datenschutz-Risiken, wie etwa Datenschutz-Folgenabschätzungen, die ebenfalls eine Form der Selbstbewertung darstellen, Lücken aufweisen. Sie führen zwar zu einer Reihe von Compliance-Maß-

92 Europäische Kommission, „Vorschlag für ein Gesetz über künstliche Intelligenz“, COM/2021/206 final.

93 Europäische Kommission, „Vorschlag für ein Gesetz über künstliche Intelligenz“, COM/14/206 final, Artikel 10 und 14, 2021.

94 Siehe z. B. M. Coeckelbergh, *AI Ethics* (London: MIT Press, 2020), 165.

nahmen, mindern aber weder die Risiken für die Betroffenen, noch sorgen sie für die Entwicklung von datenschutzfreundlicher Software.⁹⁵ Entsprechend ist zu erwarten, dass sich eine Selbstbewertung gemäß den künftigen KI-Vorschriften darauf konzentriert, die Haftungsrisiken der Firmen zu mindern, aber nicht inhaltlich mit den Bedürfnissen der Arbeitnehmer*innen auseinandersetzt.

Wie bereits dargelegt, bietet das geltende Arbeitsrecht in Europa natürlich bereits einen gewissen Schutz gegen einige Risiken algorithmischer Systeme am Arbeitsplatz – wenn auch keinen flächendeckenden und perfekten Schutz. Allerdings werden die als Entwurf vorliegenden neuen KI-Vorschriften in Form einer direkt anwendbaren Verordnung und ohne Verweise auf die Sozialpartner und bereits bestehende nationale Schutzmaßnahmen im Bereich algorithmisches Management eingeführt. Deshalb befürchten manche Beobachter, sie könnten bereits vorhandene und strengere nationale Vorschriften und arbeitsrechtliche Praktiken untergraben.⁹⁶ In bestimmten Ländern wäre die Einführung zudringlicher neuer Überwachungs- und Kontrolltechnologien nur nach detaillierten Vereinbarungen mit Arbeitnehmervertreter*innen möglich. Dennoch scheint das KI-Gesetz in seiner aktuellen Form derartigen Systemen nach einer unverbindlichen Selbstbewertung Tür und Tor zu öffnen.

Das heißt nicht, dass die EU keine verbindlichen Vorschriften für Systeme zur automatisierten Entscheidungsfindung einführen sollte – im Gegenteil. Schon die Tatsache, dass Kollektivabkommen in großen Teilen Europas schwach sind oder ganz fehlen, macht Mindestbedingungen für die Verwendung von Systemen, die mit Arbeitnehmer*innen interagieren, notwendig. Als rechtliche Grundlage dient jedoch bisher eindeutig die Marktintegration. Die EU sollte aber keine Situation schaffen, in der die EU-weite Marktintegration und Anreize für die Nutzung von KI in Kombination mit einem schwachen System der Selbstbewertung kollektive Maßnahmen vor Ort verdrängen und bestimmen, wie die Vorschriften am Arbeitsplatz interpretiert werden.

95 F. Ferra, I. Wagner, E. Boiten et al., „Challenges in Assessing Privacy Impact“.

96 V. De Stefano, „The EU Proposed Regulation on AI: A Threat to Labour Protection?“ *Regulating for Globalization*, Wolters Kluwer, 16. April 2021 auf: <http://regulatingforglobalization.com/2021/04/16/the-eu-proposed-regulation-on-ai-a-threat-to-labour-protection/>.

97 M. Veale und F. Zuiderveen Borgesius, „Demystifying the Draft EU Artificial Intelligence Act“, *Computer Law Review International* 22(4) (2021).

98 L. Lessig, *Code and Other Laws of Cyberspace* (New York, Basic Books, 1999).

Dies gilt umso mehr, wenn die neuen KI-Vorschriften weder starke Durchsetzungsmechanismen noch ein EU-weites Organ für gemeinsames Handeln und Koordinierungsmaßnahmen vorsehen. Der geplante Europäische Ausschuss für künstliche Intelligenz ist eine reine Expertengruppe ohne Entscheidungsbefugnis oder ausreichende personelle Ausstattung sodass, wie M. Veale und F. Borgesius feststellen „die wirklichen Regeln vermutlich von obskuren Normungsgremien für Elektronik ohne Erfahrung in Grundrechtsfragen geschrieben werden“.⁹⁷ Ferner merken sie an, dass die Organe für Marktüberwachung, die die Vorschriften durchsetzen sollen, für die gewaltige Aufgabe, nicht nur KI-Entwickler, sondern auch die Nutzer in ganz unterschiedlichen Situationen zu kontrollieren, unzureichend ausgestattet sind. Die Chance, dass die Behörden diese komplexen neuen Aufgaben bewältigen, ist verschwindend gering.

Deshalb muss der künftige Vorschlag zur künstlichen Intelligenz auch institutionelle Mechanismen enthalten, die die Kluft zwischen denjenigen, die Systeme konstruieren, und den Gruppen überbrücken, die mit den Folgen leben müssen, nicht zuletzt an ihrem Arbeitsplatz.

8.3 Wer konzipiert, entscheidet: Mitsprache bei der Software-Entwicklung

Vor inzwischen 20 Jahren hat der US-amerikanische Juraprofessor Lawrence Lessig vorhergesagt, dass der Code Gesetz sein wird und Bürger*innen und kollektive Institutionen über die Form der digitalen Infrastruktur entscheiden sollten.⁹⁸ Seit die Beziehungen in der Arbeitswelt immer mehr durch von Algorithmen bestimmten Systeme in Codes gefasst – und verschleiert – werden, gilt diese Maxime für die Arbeitswelt besonders.

Während Arbeitnehmer*innen noch versuchen, Datenschutzrechte eher defensiv zu nutzen, bergen moderne algorithmische Systeme ganz andere Risiken und Chancen. Heute haben Unternehmen die Möglichkeit, gewaltige Datenmengen zu erfassen,

zu speichern und zu analysieren, die ihnen ein Bild der Produktionsprozesse in Echtzeit, einen „digitalen Zwilling“ zeigen, mit dessen Hilfe sie Abläufe steuern und optimieren und die Ergebnisse fast sofort überprüfen können. In Europa verspricht dies unter anderem das Unternehmen Celonis.⁹⁹

Die Frage ist, wozu diese Daten genutzt werden. Zurzeit geht der Trend hin zu einer Fortsetzung der tayloristischen Revolution – mit neuen Mitteln. Arbeitnehmer*innen werden immer stärker überwacht und kontrolliert, was ihre Autonomie und Verhandlungsmacht untergräbt. Es gibt aber Alternativen. Schon Anfang der 1970er Jahre entwickelte Stafford Beer, ein visionärer Kybernetiker und Unternehmensforscher, für die chilenische Regierung ein technologisches System zur Erfassung und Verwaltung der Produktion: das Projekt Cybersyn. Das war algorithmisches Management auf nationaler Ebene.

INFOBOX 17: Projekt Cybersyn

Das Projekt Cybersyn „entsprang der Fähigkeit, sich vorzustellen, wie Computerisierung in einer Fabrik etwas anderes bewirken könnte, als Beschleunigung und Herabstufung von Arbeitsplätzen [...]“. Der Staat schuf die Möglichkeit, bei der Konzipierung in neue Richtungen zu denken, indem er der sozialen Gerechtigkeit Vorrang einräumte und die nötigen finanziellen und personellen Ressourcen bereitstellte, um die technologische Innovation in diese Richtung zu verschieben. Das zeigt, dass der Staat Techniker dazu zwingen (und inspirieren) kann, darüber nachzudenken, wie Systeme dem Wohl der Bürger dienen können, das nicht immer mit Gewinn, Marktchancen, Effizienz, technischer Eleganz oder einem coolen Systemkonzept gleichgesetzt werden kann.¹⁰¹

Allerdings war es nicht als System geplant, das die technokratische Kontrolle erleichtern sollte. Wie die Wissenschaftlerin Eden Medina darlegt, empfahl Stafford Beer, dass „die Regierung die Modelle für staatliche Fabriken von Arbeiter*innen entwickeln lässt, und nicht von Ingenieuren, weil diese die Prozesse vor Ort am besten kennen. Das heißt, die Arbeiter*innen würden an der Entwicklung des Systems mitwirken, das sie dann auch betreiben und nutzen. Wenn die Arbeiter*innen sowohl mit dem Kopf als auch mit der Hand arbeiten können, fühlen sie sich weniger von ihrer Arbeit entfremdet.“¹⁰⁰

Um den Einfluss der Arbeitnehmer*innen auf die Konzipierung der Software zu stärken, sind heute mehrere Ansätze nötig. Zum einen müssten die Interessen und offiziellen Beteiligungsfunktionen der Arbeitnehmer*innen direkt in die algorithmischen Systeme integriert werden. Zum anderen müssten Funktionen eingeführt werden, über die Betriebsräte und Vertrauensleute automatisch auf einschlägige Informationen zugreifen und dadurch direkt gewährleisten können, dass das Arbeitsrecht und die Rechte der Arbeitnehmer*innen z. B. in Bezug auf Überstunden oder den Schutz vor Diskriminierung gewahrt werden. Wenn Gewerkschaften schon heute um den Zugang zu digitalen Kommunikationsnetzen kämpfen, könnten sie doch auch gleich noch Zugang zu digitalen Managementsystemen und „digitalen Zwillingen“ fordern. Bei der ökologischen Nachhaltigkeit hat sich diese Denkweise bereits durchgesetzt. So hat der Software-Anbieter SAP seine Absicht angekündigt, den vollständigen ökologischen Fußabdruck aller Ressourcen, die durch sein Ressourcenplanungssystem (ERP) laufen, zu integrieren. Das heißt, die Software wird ausdrücklich dazu konzipiert, Nachhaltigkeit zu fördern. Für die sozio-ökologische Wende sollte mit sozialen Anforderungen etwas Ähnliches passieren. Dies entspricht auch dem offiziellen politischen Ziel der EU, ihre soziale und ihre umweltpolitische Agenda zu kombinieren.¹⁰²

99 Cracked Labs, 95.

100 E. Medina, „Rethinking Algorithmic Regulation“, *Kybernetes* 44(6-7) (2015), 1010.

101 Ebd., 1010.

102 Siehe z. B. Europäische Kommission, „Mitteilung über ein starkes soziales Europa für einen gerechten Übergang“, COM (2020), 14.

Es ist allerdings unwahrscheinlich, dass große Softwarefirmen aus eigenem Antrieb Systeme für soziale Nachhaltigkeit und mehr Mitsprache der Arbeitnehmer*innen entwickeln. Es ist ganz klar, dass die grüne Wende in diesem Bereich nur deshalb – langsam – vorankommt, weil die Anbieter nach der gesellschaftlichen Mobilisierung der letzten Jahre verbindliche Rechtsvorschriften erwarten und Umweltfreundlichkeit inzwischen zu einem vielversprechenden Geschäftsmodell geworden ist.

Es gab bereits Experimente und Programme, bei denen Arbeitnehmer*innen an der Konzipierung von Technologie beteiligt wurden, vor allem in den skandinavischen Ländern. Sehr erfolgreich war das TCO-Prüfsiegel für Computer-Hardware, das die schwedische Angestelltengewerkschaft TCO schon 1992 eingeführt hat.¹⁰³ Für den Software-Bereich startete der schwedische Gewerkschaftsdachverband (LO) gemeinsam mit der TCO 1998 das Projekt „UsersAwards“. Zum Projekt gehörten Benutzerumfragen in einzelnen Branchen, Konferenzen, Entwicklungsprojekte, IT-Wettbewerbe und die Einführung eines Zertifizierungssystems für betriebliche Software.¹⁰⁴

Trotz der Zertifizierung von zwei Software-Paketen im Jahr 2002 konnte sich das System aufgrund der Reaktivität und mangelnden Zusammenarbeit mit Software-Firmen nie durchsetzen.¹⁰⁵ Heute dürfte die Beteiligung der Software-Hersteller angesichts der Marktkonzentration in vielen Segmenten für Unternehmenssoftware noch schwieriger sein. Ein Großteil der betrieblichen Software-Systeme wird heute von großen Unternehmen entwickelt, die den gesamten europäischen oder sogar internationalen Markt bedienen. Deshalb kann der soziale Wettstreit über ihre Konzipierung nicht ausschließlich in einzelnen Unternehmen oder auch nur in einzelnen Ländern stattfinden. Er muss von einer Institution geführt werden, die in der gesamten EU tätig ist

und das Fachwissen und die Netzwerke von Gewerkschaften, Organisationen der Zivilgesellschaft, Wissenschaft (Datenschutz und Arbeitsrecht, Interaktion zwischen Menschen und Computer, Software-Entwicklung) und der zuständigen Behörden bündelt.

Eine solche Institution sollte über genug Fachwissen und Kapazitäten verfügen, um Software-Pakete und deren Updates zertifizieren zu können. Es ließe sich z. B. ein Zertifizierungssystem denken, das Software vorab testet und als DSGVO- und arbeitsrechtskonform kennzeichnet. Dafür ist jetzt genau der richtige Zeitpunkt, weil es in vielen Bereichen, wie der Umsetzung der DSGVO in der Arbeitswelt oder den künftigen Regeln für eine auf den Menschen ausgerichtete Gestaltung von KI-Systemen, noch keine Zertifizierungen oder Normen gibt. Bestehenden Normungsgremien fehlen oft die Legitimität und Mechanismen, die der Zivilgesellschaft und den Sozialpartnern eine echte Mitbestimmung ermöglichen würden.¹⁰⁶ Dies würde Arbeitnehmer*innen und Betriebsräte schützen, weil sie dann von ihren Arbeitgebern einfach ein entsprechendes Zertifikat fordern könnten. Aber auch Unternehmen, die Software entwickeln und nutzen, würden von diesem System profitieren, weil sie damit sicher sein können, dass ihre Systeme mindestens gesetzlich zulässig und im Idealfall sogar nutzerfreundlich sind. Diese Institution könnte sogar Software überprüfen, die bereits auf dem Markt ist, wenn die künftigen Gesetze über digitale Märkte und digitale Dienstleistungen entsprechende Bestimmungen enthalten.

103 A. Walldius et al., „User Certification of Workplace Software: Assessing both Artefact and Usage“ *Behaviour & Information Technology* 2(28) (2019), 101–20.

104 A. Walldius, J. Gulliksen und Y. Sundblad, „Revisiting the UsersAward Programme from a Value Sensitive Design Perspective“, 5th Decennial Aarhus Conference on Critical Alternatives, 2017.

105 J. Larner und A. Walldius, „The Platform Review Alliance Board: Designing an Organizational Model to Bring Together Producers and Consumers in the Review and Commissioning of Platform Software“ *Journal of Organization Design* 14(8) (2019).

106 J. Cohen, *Between Truth and Power. The Legal Constructions of Informational Capitalism* (New York, Oxford University Press, 2019), 202-237.

EMPFEHLUNGEN: INSTITUTIONELLE KAPAZITÄTEN AUSBAUEN

EMPFEHLUNGEN: INSTITUTIONELLE KAPAZITÄTEN AUSBAUEN

Die DSGVO gibt Arbeitnehmer*innen und ihren Vertreter*innen starke Instrumente in die Hand, mit denen sie Einblicke in die Erfassung und Verwendung ihrer personenbezogenen Daten gewinnen können, und gewisse Instrumente, um die Analysen und Entscheidungen zu prüfen, die auf deren Grundlage erfolgen. Die geltenden Informations- und Mitbestimmungsrechte bieten Arbeitnehmer*innen sogar noch mehr Ansätze, um Informationen – und Mitbestimmung – in Bezug auf die Nutzung neuer Technologien am Arbeitsplatz einzufordern. Damit diese Rechte zu greifbaren Ergebnissen führen, muss aber noch viel getan werden, um die bestehenden Aufsichtsbehörden sowie die Kapazität der kollektiven Organe zu stärken, die die Arbeitnehmer*innen auf nationaler Ebene und in den Unternehmen vertreten.

EU-Organe und Mitgliedstaaten:

- Datenschutzbehörden sollten mit angemessenen personellen und finanziellen Ressourcen ausgestattet und in der Umsetzung der DSGVO in der Arbeitswelt geschult werden. In der digitalen Wirtschaft ist der Schutz personenbezogener Daten nicht länger ein Randthema, sondern eine wichtige Frage an jedem Arbeitsplatz. Die Kapazitäten der Regulierungsbehörden sollten das widerspiegeln.
- Mitgliedstaaten, die dies bisher noch nicht getan haben, sollten das nach [Artikel 80\(2\)](#) der DSGVO mögliche kollektive Beschwerderecht einführen, um einzelne Betroffene und die Datenschutzbehörden zu entlasten und es Gewerkschaften und Organisationen der Zivilgesellschaft zu ermöglichen, die Datenschutzrechte vieler Einzelner kollektiv durchzusetzen.
- Die Organe der EU sollte in Legislativvorschlägen wie dem Daten-Governance-Gesetz und insbesondere dem KI-Gesetz die Interessen der Arbeitnehmer*innen in den Vordergrund stellen und in beiden Gesetzen eine Infrastruktur für gründliche Überprüfungen vorsehen. Das KI-Gesetz vertraut

zu stark darauf, dass die Unternehmen selbst die Rechtskonformität prüfen. Es sollte Betriebsräte und Gewerkschaften ausdrücklich dazu berechtigen, bei der Einführung algorithmischer Systeme am Arbeitsplatz an der Überprüfung dieser Systeme mitzuwirken.

- Der von der Europäischen Kommission angekündigte Legislativvorschlag zur Verbesserung der Arbeitsbedingungen von Plattformbeschäftigten sollte diesen ein Recht auf Kollektivverhandlungen einräumen.

Datenschutzbehörden:

- Datenschutzbehörden sollten die Beschäftigung zu einem Schwerpunktbereich machen, vor allem angesichts des Digitalisierungsschubs durch die Coronapandemie. Dies ist ein Bereich, in dem ein frühzeitiges Eingreifen noch immer möglich ist und die Regulierungsbehörden Erwartungen formulieren und Praktiken gestalten können, anstatt erst dann einzugreifen, wenn sich ein komplettes Geschäftsmodell um nicht nachhaltige Praktiken herum ausgebildet hat (wie dies bei verbraucherorientierten Online-Plattformdiensten der Fall war).
- Datenschutzbehörden brauchen mehr Mittel, um systematische Aufklärungs-, Beratungs- und Durchsetzungskampagnen zum Datenschutz am Arbeitsplatz durchführen zu können. Vor allem angesichts der rasanten Veränderungen während der Coronapandemie sind Durchsetzungsmaßnahmen und Leitlinien der Behörden dringend notwendig und erfolgsversprechend.
- Da die Ressourcen zur Durchsetzung der Vorschriften knapp sind, sollten die wenigen Entscheidungen, die Datenschutzbehörden im Bereich Beschäftigung treffen, pädagogisch und abschreckend wirken. Das bedeutet weniger informelle Verhandlungen hinter verschlossenen Türen und mehr offiziell veröffentlichte Entscheidungen mit wirksamen Geldbußen.

- Die Entscheidungen von Datenschutzbehörden im Bereich Beschäftigung und dazugehörige Gerichtsurteile sollten in einer speziellen, öffentlich zugänglichen Datenbank erfasst werden. Dies würde allen beteiligten Akteuren, d. h. Gewerkschaften, Betriebsräten, Arbeitgebern und Herstellern von Datensystemen für die Arbeitswelt, den Zugang zu Informationen und bewährten Verfahren erleichtern. Mittelfristig würde eine solche Datenbank die Arbeitsbelastung der Datenschutzbehörden in diesem Bereich stark mindern, weil sich Konflikte und Beschwerden vermeiden lassen, wenn die Praxis der Behörden und Gerichte öffentlich einsehbar ist und dafür sorgt, dass Interpretation und Erwartungen stabiler und vorhersehbarer werden.

Gewerkschaften, Vertrauensleute und Betriebsräte

- Einiges deutet darauf hin, dass Beschäftigtendaten häufig rechtswidrig genutzt werden. Deshalb sollten Vertrauensleute und Betriebsräte Wissenslücken der Arbeitnehmer*innen in Bezug auf ihre Datenschutzrechte schließen, die Interessen der Arbeitnehmer*innen im Bereich Datenschutz gegenüber dem Management aktiv vertreten und Arbeitnehmer*innen bei Beschwerden unterstützen. Datenschutzbehörden müssen Beschwerden wegen mutmaßlicher Verstöße gegen die DSGVO nachgehen.
- Betriebsräte, Gewerkschaften und Vertrauensleute sollten eine Kooperation mit dem für den Arbeitsplatz zuständigen Datenschutzbeauftragten anstreben. Gemeinsam sollten sie an allen wichtigen Schritten bei der Einführung technologischer Systeme beteiligt sein, in denen personenbezogene Daten verarbeitet werden. Auch Datenschutzbehörden sind wichtige Partner, wenn es darum geht, die Bedeutung der DSGVO für die Arbeitswelt zu klären.
- Jede Gewerkschaft sollte intern oder in ihrem Netzwerk über einen Datenanalysten verfügen. Ohne Fachwissen über Daten und algorithmisches Management – sowohl rechtlich als auch notwendigerweise technisch – werden die Gewerkschaften in diesem Bereich nur mit Mühe relevant bleiben. Umgekehrt können Gewerkschaften viel dazu beitragen, die Arbeitsplätze von morgen zu verbessern, wenn sie jetzt die Gelegenheit nutzen und die Datenschutzforderungen von Betriebsräten, Vertrauensleuten und einzelnen Arbeitnehmer*innen aktiv unterstützen.
- Für zentrale Bestimmungen der DSGVO fehlt bisher eine Interpretation für die Arbeitswelt. Deshalb sollten Gewerkschaften versuchen, diese in den nach [Artikel 88](#) der DSGVO möglichen Kollektivvereinbarungen bereitzustellen. Außerdem sollten sie Musterklagen einreichen, um die Auslegung der DSGVO zu beschleunigen und Wissenschaftler*innen ermutigen, die nötige Interpretationsarbeit zu leisten. Moderne Arbeitsplätze brauchen eine enge Kooperation von Arbeitsrechts- und Datenschutzanwälten, und die Gewerkschaften sollten die Zusammenarbeit dieser beiden Bereiche vorantreiben.
- Auf europäischer Ebene sollten Gewerkschaften eine Methodologie entwickeln, mit deren Hilfe Gewerkschaften und Betriebsräte prüfen können, wie gut sie die Rechte ihrer Mitglieder in Fragen digitaler Technologien vertreten können. Das könnte es ihnen erleichtern, Kompetenz- und Kapazitätslücken zu erkennen. Die Institutionen für den sozialen Dialog sollten dafür den systematischen Austausch mit dem Europäischen Datenschutzausschuss suchen.
- Die Konzipierung von Software ist äußerst wichtig, lässt sich aber nur schwer beeinflussen, weil die Entwickler oft weltweit tätig sind und durch Rechte des geistigen Eigentums und den Verweis auf Betriebsgeheimnisse eine externe Überprüfung ihrer Software verhindern. Deshalb sollten Gewerkschaften und die Zivilgesellschaft in Zusammenarbeit mit Universitäten und Behörden eine neue Institution schaffen, die in der gesamten EU tätig ist und eine Zertifizierung und Überprüfung von Software-Systemen für den Arbeitsplatz aus Perspektive der Arbeitnehmer*innen ermöglicht.

**BIBLIOGRAPHIE,
AUTOREN,
ÜBER DIE FEPS UND
IHRE PARTNER**

BIBLIOGRAPHIE

Adams-Prassl, J. 'What if your Boss was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work', *Comparative Labor Law & Policy Journal* 41(1) (2019).

Albrecht, T., and C. Kellermann, 'Artificial Intelligence and the Future of the Digital Work-Oriented Society', Friedrich-Ebert-Stiftung, October 2020, at: <https://socialdialogue.fes.de/news-list/e/artificial-intelligence-and-the-future-of-the-digital-work-oriented-society>.

Albrecht, T., and D. Gerst, 'Designing Work in a Digitalising World', *Social Europe Journal* 18 May (2021), at: <https://socialeurope.eu/designing-work-in-a-digitalising-world>.

Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, 8 June 2017.

Article 29 Working Party (2017) WP 248, 4 April 2017, at: https://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', 2017.

Aloisi, A., and E. Gramano, 'Artificial Intelligence is Watching you at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context', *Automation, Artificial Intelligence & Labor Law* 41(1) (2019).

Autoriteit Persoonsgegevens (Dutch Data Protection Authority), 'AP. Verwerking gezondheidsgegevens wearables door werkgevers mag niet' (8 March 2016), at: <https://autoriteitpersoonsgegevens.nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet>.

Autoriteit persoonsgegevens, 'Jaarverslag 2020' (2021), at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2020.pdf.

[nl/sites/default/files/atoms/files/ap_jaarverslag_2020.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2020.pdf).

Berg, J. 'Protecting Workers in the Digital Age: Technology, Outsourcing and the Growing Precariousness of Work', SSRN (2019), at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3413740.

Bronowicka, J. et al, 'Game that you Can't Win? Workplace Surveillance in Germany and Poland (Frankfurt (Oder): European University Viadrina, 2020).

Bundesarbeitsgericht, 27 July 2017, 2 AZR 681/16.

BusinessEurope, SMEunited, CEEP and the ETUC, 'European Social Partners Framework Agreement on Digitalisation', June 2020, at: https://www.etuc.org/system/files/document/file2020-06/Final%2022%2006%2020_Agreement%20on%20Digitalisation%202020.pdf.

Bygrave, L. A., 'Article 22', in eds C. Kuner, L. A. Bygrave and C. Docksey, *Commentary on the EU General Data Protection Regulation* (Oxford: Oxford University Press, 2019).

Bygrave, L. A., 'Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making', University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2019-01, 2019.

CMS, 'GDPR Enforcement Tracker', at: <https://www.enforcementtracker.com>.

CNV, 'Half miljoen thuiswerkers via software in de gaten gehouden', at: <https://www.cnv.nl/nieuws/half-miljoen-thuiswerkers-via-software-in-de-gaten-gehouden/>.

Coeckelbergh, M., *AI Ethics* (London: MIT Press, 2020), 165.

Cohen, J., *Between Truth and Power. The Legal Constructions of Informational Capitalism* (New York, Oxford University Press, 2019).

Colclough, C., 'Workers' Rights: Negotiating and Co-governing Digital Systems at Work', *Social Europe* September (2020).

Cracked Labs, 'Digital Überwachung und Kontrolle am Arbeitsplatz. Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management?' (September 2021).

Dagnino, E., and I. Armaroli, 'A Seat at the Table: Negotiating Data Processing in the Workplace', *Comparative Labor Law & Policy Journal* (2020), 173–95.

De Loecker, J., and J. Eeckhout, 'Global Market Power', NBER Working Paper 24768 (2018).

De Stefano, V., 'Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection', *Comparative Labour Law & Policy* 41(1) (2019).

De Stefano, V., 'The EU Proposed Regulation on AI: A Threat to Labour Protection?'. *Regulating for Globalization*, Wolters Kluwer, 16 April, 2021 at: <http://regulatingforglobalization.com/2021/04/16/the-eu-proposed-regulation-on-ai-a-threat-to-labour-protection/>.

Ellguth, P., 'Ost- und Westdeutschland nähern sich bei der Reichweite der betrieblichen Mitbestimmung an', IAB-FORUM, 13 May 2020, at: <https://www.iab-forum.de/ost-und-westdeutschland-naehern-sich-bei-der-reichweite-der-betrieblichen-mitbestimmung-an/>.

European Commission, SWD (2020), 115.

European Commission, 'Digital Compass 2030' (2021), COM/2021/118 final.

European Data Protection Board, 'First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities', 26 February, 2019, 7, at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf.

Ferra, F., I. Wagner, E. Boiten et al, 'Challenges in Assessing Privacy Impact: Tales from the Front Lines', *Security and Privacy* 3(2) (2020).

Frey, C. B., *The Technology Trap: Capital, Labor, and Power in the Age of Automation* (Princeton: Princeton University Press, 2019).

Gürses, S., and J. van Hoboken, 'Privacy After the Agile Turn', in eds Evan Selinger et al, *Cambridge Handbook of Consumer Privacy* (Cambridge: Cambridge University Press, 2018).

Hendrickx, F., E. Gramano and D. Mangan, 'Privacy, Data Protection and the Digitalisation of Work: How Industrial Relations Can Implement a New Pillar', *Kluwer Regulating for Globalization Blog*, 26 June 2020, at: <http://regulatingforglobalization.com/2020/06/26/privacy-data-protection-and-the-digitalisation-of-work-how-industrial-relations-can-implement-a-new-pillar/>.

Holmberg, S. 'Fighting Short-Termism with Worker Power', Roosevelt Institute (17 October 2017).

Humphries, J., 'The lure of aggregates and the pitfalls of the patriarchal perspective: a critique of the high wage economy interpretation of the British industrial revolution', *Economic History Review* 66 (3) (2013).

Huws, U., N. Spencer and M. Coates, 'The Platformisation of Work in Europe. Highlights from Research in 13 European Countries', FEPS, UNI Europa and the University of Hertfordshire, 2019.

Information Commissioner's Office, 'How Do We Do a DPIA?', at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how7>.

Kress, C., R. Van Eijk and G. Zanfir-Fortuna, 'New Decade, New Priorities: A Summary of Twelve European Data Protection Authorities' Strategic and Operational Plans for 2020 and Beyond', Future of Privacy Forum, 12 May 2020, at: https://fpf.org/wp-content/uploads/2020/05/FPF_DPAStrategiesReport_05122020.pdf.

Larner, J., and A. Walldius, 'The Platform Review Alliance Board: Designing an Organizational Model to Bring Together Producers and Consumers in the Review and Commissioning of Platform Software', *Journal of Organization Design* 14(8) (2019).

Leicht-Deobald, U., et al, 'The Challenges of Algorithm-Based HR Decision-Making for Personal Integrity', *Journal of Business Ethics* 160 (2021).

Lessig, L., *Code and Other Laws of Cyberspace* (New York, Basic Books, 1999).

Lobel, O., 'The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property', *Texas Law Review* 93(789) (2015).

Mantelero, A., 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection', *Computer Law & Security Review* 32 (2017), 238–55.

McDonald, S., 'A Novel, European Act of Data Governance', Centre for International Governance Innovation, 2020.

Medina, E., 'Rethinking Algorithmic Regulation', *Kybernetes* 44(6–7) (2015).

Mendoza, I., and L. A. Bygrave, 'The Right Not to be Subject to Automated Decisions Based On Profiling', in eds T. Synodinou, P. Jougoux, C. Markou and T. Prastitou, *EU Internet Law: Regulation and Enforcement* (Springer: 2017), 77–98.

Moore, P. V., M. Upchurch and X. Wittaker (eds), *Humans and Machines at War: Monitoring, Surveillance and Automation in Contemporary Capitalism* (London: Palgrave Macmillan, 2018).

Noble, D. F., 'Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools', in eds D. Preece, I. McLoughlin and P. Dawson, *Technology, Organizations and Innovation: Critical Perspectives on Business and Management. Volume 1: The early debates* (London: Routledge, 2000)..

Nogarede, J., 'Governing Online Gatekeepers: Taking Power Seriously', FEPS, 2021.

NOS, "Gluurappartuur" in trek door thuiswerken, vakbond bezorgd', at: <https://nos.nl/artikel/2375956-gluurapparatuur-in-trek-door-thuiswerken-vakbonden-bezorgd>.

Noyb, 'Luxemburg's Watchdog Refuses to Show its Teeth to US Companies', 25 January, at <https://noyb.eu/en/luxemburgs-watchdog-refuses-show-its-teeth-us-companies>.

Nurski, L. 'Algorithmic Management is the Past, Not the Future of Work', blog post 6 May 2021, Bruegel, at: <https://www.bruegel.org/2021/05/algorithmic-management-is-the-past-not-the-future-of-work/>.

Pasquale, P., *New Laws of Robotics: Defending Human Expertise in the Age of AI* (Cambridge, MA: Belknap Press, 2020).

Pasquale, F., *The Black Box Society: The Secret Algorithms That Control Money and Information* (London: Harvard University Press, 2016)

Peck, D., 'They're Watching You at Work', *The Atlantic*, December (2013), at: <https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/>.

Prospect, 'Union Reveals that Half of Workers Don't Know What Data their Boss Collects About Them', 12 February, 2020, at: <https://prospect.org.uk/news/union-reveals-that-half-of-workers-dont-know-what-data-their-boss-collects-about-them/>.

Rechtbank Amsterdam, Uitspraak 11-3-2021, c/13/689705.

Richardson, R. 'Defining and Demystifying Automated Decision Systems', *Maryland Law Review* 81 (forthcoming 2022).

Rogers, B., 'The Law and Political Economy of Workplace Technological Change', *Harvard Civil Rights-Civil Liberties Law Review* 55 (2021).

Ryan, J., and A. Toner, 'Europe's Enforcement Paralysis. ICCL's 2021 Report on the Enforcement Capacity of Data Protection Authorities', Irish Council for Civil Liberties (2021).

Sarpong, S., and D. Rees, 'Assessing the Effects of 'Big Brother' in a Workplace: the case of WAST', *European Management Journal* 32(2) (2014).

Schäfers, K., and J. Schroth, 'Shaping Industry 4.0 on Workers' Terms. IG Metall's Work_Innovation Project', Trade Unions in Transformation 4.0 series, Friedrich-Ebert-Stiftung, September 2021.

Selbst, A. D., and J. Powles, 'Meaningful Information and the Right to Explanation', *International Data Privacy Law* 7(4) (2018).

Senatori, I., (2020) 'The European Framework Agreement on Digitalisation: a Whiter Shade of Pale?', *Italian Labour Law e-Journal* 13 (2) (2020).

Skillcast (2020), 'Remote-working Compliance YouGov Survey', 25 November, at: <https://www.skillcast.com/blog/remote-working-compliance-survey-key-findings>.

Staab, P., and S. Geschke, 'Ratings als arbeitspolitisches Konfliktfeld. Das Beispiel Zalando', Study 429, Hans Böckler Stiftung (2020).

Stiller, S., J. Jäger and S. Gießler, 'Automated Decisions and Artificial Intelligence in Human Resource Management: Guideline for Reviewing Essential Features of AI-based Systems for Works Councils and Other Staff Representatives', 18 May 2021, AlgorithmWatch, at: https://algorithmwatch.org/en/wp-content/uploads/2021/05/AlgorithmWatch_AutoHR_Guideline_2021.pdf.

Stolton, S., 'Employers Accused of Abusing EU Data Privacy Rules to Hinder Trade Unions', Euractiv, 19 March (2020).

Todolí-Signes, A., 'Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection', ETUI, 2019.

UNI Global Union, '10 Principles for Workers' Data Rights and Privacy' (2017).

Van Geuns, J., and A. Brandescu, 'Shifting Power Through Data Governance', September 2020, Mozilla Insights.

Veale, M., and L. Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling', *Computer Law & Security Review* 34(2) (2018).

Veale, M., and F. Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act', *Computer Law Review International* 22(4) (2021).

Viljoen, S., (forthcoming), 'Democratic Data: A Relational Theory For Data Governance', *Yale Law Journal*.

Walker, P., 'Call Centre Staff to be Monitored via Webcam for Home-Working "Infractions"', *The Guardian*, 26 March, 2021, at: <https://www.theguardian.com/business/2021/mar/26/teleperformance-call-centre-staff-monitored-via-webcam-home-working-infractions>.

Wachter, S., and B. Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI', *Columbia Business Law Review* 2 (2019).

Wachter, S., B. Mittelstadt and L. Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law* 7(2) (2017).

Walldius, A., et al, 'User Certification of Workplace Software: Assessing both Artefact and Usage', *Behaviour & Information Technology* 2(28) (2019), 101–20.

Walldius, A., J. Gulliksen and Y. Sundblad, 'Revisiting the UsersAward Programme from a Value Sensitive Design Perspective', 5th Decennial Aarhus Conference on Critical Alternatives, 2017.

Winner, L., 'Do Artifacts Have Politics?', *Daedalus* 121 (1980).

ÜBER DEN AUTOR



JUSTIN NOGAREDE

Justin Nogarede ist Analyst für Digitalpolitik bei der Foundation for European Progressive Studies (FEPS). Davor war er im Generalsekretariat der Europäischen Kommission unter anderem für politische Strategien im Bereich digitale Märkte und Binnenmarkt zuständig. In der Europäischen Kommission war er an der Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt und an der Entwicklung politischer Initiativen zu standardessentiellen Patenten, audio-visuellen Medien, Internet-Governance und Produkthaftung beteiligt.

ÜBER DIE FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES (FEPS)

Die Foundation for European Progressive Studies (FEPS) ist eine Denkfabrik, die den progressiven politischen Strömungen innerhalb der EU zuzuordnen ist. Ihre Mission besteht darin, mittels innovativer Studien, Politikberatung, Weiterbildung und Diskussionen progressive politische Maßnahmen und Strategien in ganz Europa anzuregen und mit Fakten zu unterfüttern.

Die FEPS arbeitet eng mit ihren 68 Mitgliedern und anderen Partnern zusammen, zu denen renommierte Universitäten, Wissenschaftler*innen, Politiker*innen und Aktivist*innen gehören und trägt so dazu bei, auf lokaler, regionaler, nationaler, europäischer und globaler Ebene Brücken zwischen vielen unterschiedlichen Interessenträgern aus Politik, Wissenschaft und Zivilgesellschaft zu bauen.



Avenue des Arts 46, B-1000 Brüssel, Belgien +32 2 234 69 00
info@feeps-europe.eu
www.feeps-europe.eu
@FEPS_Europe

In der modernen Arbeitswelt wird Macht immer häufiger durch die Erfassung von Daten und ihre Nutzung in algorithmischen Systemen ausgeübt. Dieser Trend hat sich während der Coronapandemie nochmals beschleunigt. Zwar kann dieser Wandel – theoretisch – die Arbeitsqualität verbessern, zurzeit scheint er aber vor allem der besseren Überwachung und Kontrolle der Mitarbeitenden zu dienen. Damit der digitale Wandel sozial nachhaltig gelingt, müssen die Arbeitnehmer*innen und ihre Vertreter*innen die digitale Infrastruktur mitgestalten, die bestimmt, wie sie ihre Arbeit ausführen. Wenn die Arbeitnehmerseite frühzeitig an der Entwicklung bzw. Beschaffung digitaler Arbeitsmittel beteiligt wird, bietet dies den Herstellern den Anreiz, bei der Gestaltung dieser Systeme auch das Wohl der Arbeitnehmer*innen im Blick zu behalten.

Nach einem kurzen Überblick über aktuelle Trends und die potenziellen Risiken datengestützter algorithmischer Systeme analysiert diese Arbeit die unterschiedlichen Politikbereiche, in denen die EU und nationale Stellen, Gewerkschaften und die Organisationen der Zivilgesellschaft die Beteiligung der Arbeitnehmer*innen aktiv stärken können. Nach einem Blick auf das Potenzial und die Grenzen der Datenschutz-Grundverordnung wird die Rolle der kollektiven Informations-, Mitwirkungs- und Mitbestimmungsrechte der organisierten Arbeitnehmerschaft untersucht. Abschließend werden die potenziellen Auswirkungen künftiger EU-Rechtsvorschriften für die digitale Wirtschaft analysiert und untersucht, was getan werden kann, um den Einfluss der Arbeitnehmer*innen auf die Gestaltung von Softwaresystemen für den Arbeitsplatz zu gewährleisten.

Die Studie schließt mit einer Reihe von politischen Empfehlungen an die EU-Institutionen und -Mitgliedstaaten, die Datenschutzbehörden und die Arbeiterbewegung, die vor allem darauf ausgerichtet sind, wie das Potenzial der Datenschutz-Grundverordnung (DSGVO) zur Stärkung der Stimmen von Arbeitnehmer*innen beim digitalen Wandel der Arbeitswelt verwirklicht werden kann.

**DIESE POLITISCHE STUDIE WURDE IM NOVEMBER 2021
VERÖFFENTLICHT VON:**

FEPS
FOUNDATION FOR EUROPEAN
PROGRESSIVE STUDIES



**FRIEDRICH
EBERT
STIFTUNG**

Fondation
Jean Jaurès

FUNDACIÓN
PABLO IGLESIAS

**FONDAZIONE
PIETRO NENNI**

Copyright © 2021 der FEPS