Big Boss is watching you.

Die prekäre Situation der gläsernen Lohnabhängigen.

Mit diesem Beitrag soll auf ein Set von Problemlagen aufmerksam gemacht werden, das sehr viele Menschen und unser aller gesellschaftliche Beziehungen berührt, für das bislang aber kein Problembewusstsein zu finden ist. Die Problematik ist der Tragweite zum Trotz weitgehend unerforscht, in ihrem Wesen, ihren Bedingungen und Auswirkungen. Es geht, wie Titel und Untertitel andeuten, um die prekäre Situation Lohnabhängiger in Bezug auf eine spezifische Form des Ausgeliefertseins. Bei dieser spezifischen Form des Ausgeliefertseins Lohnabhängiger geht es nicht einfach um Überwachung oder *nur* um Überwachung. Es geht im Kern nicht um die durch den technologischen Wandel bedingt mannigfaltigeren, einfacheren und billigeren Optionen Lohnabhängige zu überwachen. Es geht nicht um Privatsphäre am Arbeitsplatz. Es geht, daher der an Orwell gemahnende Titel, um viel viel mehr.

Worauf gründet sich die angesprochene spezifische Form des Ausgeliefertseins, was ist das Spezifische der Form? Geht es allein darum, dass es sich um Lohnabhängige handelt oder ist da mehr zu beachten? Inwiefern verdienen Abhängigkeiten und Interessenlagen mehr Problembewusstsein? Plus, wie sieht es mit Möglichkeiten aus, wie ist es um Ansätze bestellt, gesellschaftlich unerwünschte Auswirkungen einzudämmen bzw. mittels proaktiver Eingriffe in die bedingende Struktur auszuschließen?

Mit diesen Fragen beschäftigt sich folgender Aufriss. In mehreren systematischen Bildern versuche ich in die prekäre Situation der gläsernen Lohnabhängigen einzuführen und das Spezifische dieser Form des Ausgeliefertseins herauszuarbeiten. Meine Einblicke in die Problemlage verdanken sich dabei der langjährigen Zusammenarbeit mit Betriebsrät_innen, dem Austausch mit Hauptamtlichen der GPA-djp und dem Kontakt mit Datenschutz- und Netzaktivist_innen.

Bild 1: Arbeiten in der MitM-Umgebung

Beginnen wir mit einer der vier grundlegenden Bedingungen und Einflussgrößen unserer spezifischen Form des Ausgeliefertseins, der „*digitalen Revolution*“. Wir finden

uns heute in einer weitgehendst digitalisierten Arbeitswelt wieder. Folglich sind die basalen Eigenschaften und Probleme digitaler Kommunikation zu bestimmenden Strukturbedingungen auch der Arbeitswelt geworden. Diese Vorbedingungen sollen hier folgendermaßen – in ein Bild – zusammengefasst werden:

Gehen wir von der Zeichnung des simplen Sender-Empfänger-Modell aus. Wir senden, speichern, empfangen heute kaum mehr analog sondern digital. Wir senden „*digits*“, Ziffern, unsere Informationen nicht etwa als Buchstaben sondern als binäre Zahlen, Nuller und Einser, *bits*. Diese *bits*, die Einzelteile aus denen die Daten zusammengesetzt sind, sind zwischen Senderin S /E und Empfängerin E /S (a) simpel, (b) schnell, (c) billig und einfach zu (d) automatisieren (1) kopier-, (2) speicher- und (3) veränderbar. Das was S/E und E /S an Information austauschen sind also Nuller und Einser, die als exakte Datenpaketskopien sowohl bei S /E und E /S zu finden sind. Sowie auch an allen Schittstellen entlang ihrer Datenübertragung.

Diese digitale Ordnung bringt unzählige Vorteile mit sich. Unter anderem liegen die in der erleichterten Vervielfältigung, schnelleren Übertragung, flexiblen Bearbeitung, billigen Ablage oder weiteren Reichweite von Infos beziehungsweise Daten. Die *bits* sind heute bereits überall und sind überall hin übertrag- und kopierbar. Denken wir an Datenkabel oder kabellose Übertragungen, an Netzwerke oder unsere einzelnen „d*evices*“, seien das Smartphones, klassische PCs, Pads oder Kameras, Herzfrequenzmesser, Uhren, Busstation-Infotafeln, Navigationsgeräte.

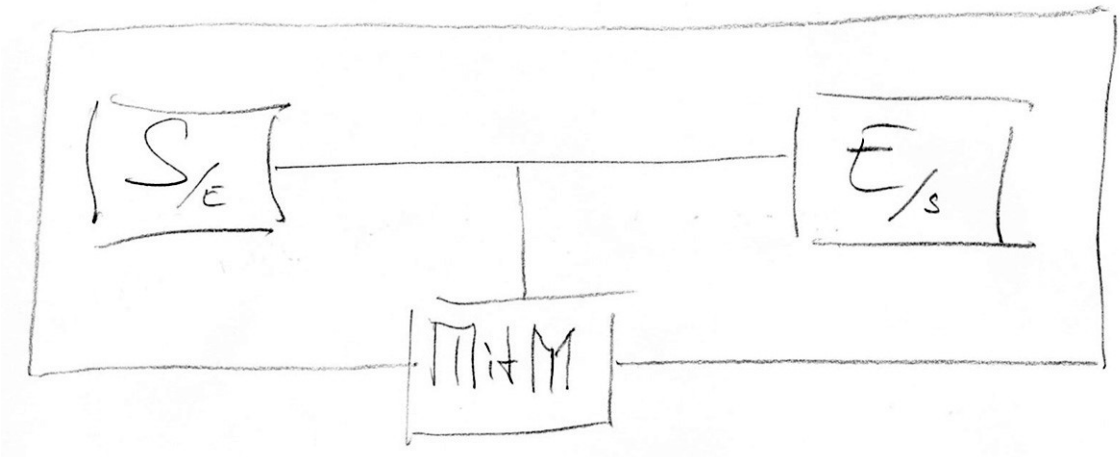

Bild 1: simples Sender_in-Empfänger_in-Modell mit Man in the Middle

Ein Problem, das mit dieser digitalen Ordnung einher geht, hat mit all den oben genannten Vorteilen zu tun und damit, dass sie von Dritten missbraucht werden können, die sich in die Datenübertragung zwischen S /E und E/S einschalten. Für diese Dritten, die

in der Regel unbemerkt bleiben, hat sich seit langem der Begriff „ *Man in the Middle* “ (MitM) etabliert. Überall wo sich Dritte in Datenübertragung einschalten, können sie unsere *bits'n'bytes* potentiell mitkopieren, für sich speichern, aber auch löschen oder an den Datenpaketen etwas verändern. Sie könnten außerdem Nuller und Einser an E/S oder S/E schicken, die S/E oder E/S als Quelle ausgeben, aber Fälschungen sind. Wir sprechen dann von „*Man in the Middle-Attacken*“. (Hier wäre nicht nur an menschliche Kommunikation etwa per E-Mail, Chat, Messaging-Systemen oder per Telefonate zu denken sondern an jede Datenübertragung zwischen Geräten, Speicherorten, Programmen.)

Diese MitM-Problematik ist für sich genommen kein Spezifikum der Arbeitswelt. Alle sind betroffen, jede Datenübertragung davon berührt. Schauen wir uns die Schutz- und Gegenmaßnahmen an, sieht das Bild jedoch etwas verändert aus. Wie sehen die aus? Die Gegenmaßnahmen sind im Prinzip banal, in der Umsetzung leider nicht. Verschlüsselte Datenübertragung verhindert, dass Angreifer in der MitM-Position mit den Nullern und Einsern etwas anfangen können, die wir übertragen. Das System des Signierens von Zertifikaten schafft Überprüfbarkeit, dass Datenpakete wirklich von S/E und E/S kommen und über die gesamte Strecke der Datenübertragung nicht ein bit verändert wurde. Diese beiden Gegenmaßnahmen schließen, wie das Bild schon zeigt, die Möglichkeit von MitM nicht aus, schlicht weil das keinen Sinn macht. Sie unterbinden aber, dass aus der MitM-Position heraus Attacken erfolgreich sind, dass unsere Daten verwendet oder gefälschte Informationen eingespeist werden.

Das alles setzt voraus, dass wir uns an die goldene Regel halten, wie sie uns von allen Datenschützern immer als vorrangigstes Prinzip genannt werden wird: nie die Kontrolle über die eigenen Geräte abgeben. Haben wir die einmal verloren, können wir nicht mehr sicher sagen, dass wir die Regeln bestimmen, nach denen unsere Geräte das machen, was wir auf ihnen und mit ihnen tun wollen. Ein Computer, zu dem wir den Zugang abgegeben haben, gilt als unsicher, es ist potentiell fremdbestimmt.

Ist ein Gerät einmal unsicher, können wir noch soviel und kompetent verschlüsseln, wir dürfen dem Gerät selbst nicht mehr vertrauen. Überall kann eine versteckte Hintertür eingebaut sein. Wir können noch soviel überprüfen, ob S/E und E/S wirklich gesichert die Sender- und Empfänger-Personen, -Accounts, -Programme, -Speicherorte sind, als die sie sich identifizieren. Den Systemen der Identifikation ist nicht mehr zu trauen. Deswegen sind Datenschutzprofis radikal, wenn wir sie fragen, was da dann noch zu machen ist. Nichts. Ist die Kontrolle über die eigenen Geräte einmal abgegeben, ist sie für immer verloren.

Genau das ist nun freilich die spezifische Ausgangsbedingung der Arbeitswelt. Lohnabhängige arbeiten auf Geräten, über die sie nie Kontrolle hatten. Sie sind unsicher. Die Regeln, die auf Arbeitsgeräten, in den Netzwerken, auf den Servern im Betrieb gelten, werden von der Unternehmensführung bestimmt. Das Unternehmen ist der omnipotente und omnipräsente Man in the Middle jeder digitalen Operation im Betrieb.

Damit wäre das erste Bild vorgestellt. Es ist grundlegend, beschreibt die prekäre Situation der Lohnabhängigen aber noch nicht. Es bezeichnet lediglich eine Ausgangslage: Lohnabhängige arbeiten heute in einem digitalen Umfeld, das dem MitM=Unternehmen volle Kontrolle über alle *bits'n'bytes* zulässt. Wie eingangs dieses Abschnitts angedeutet, würde ich diese Ausgangslage als eine der vier Bedingungen der spezifischen Form des ausgeliefert seins Lohnabhängiger ansehen. Es handelt sich um die relativ neueste, also am wenigsten analysierte Einflussgröße. Die anderen sind dagegen bekannt: das durch den Kapitalismus bedingte Verhältnis der Lohnabhängigkeit selber, das die Arbeitenden zum Verkauf ihrer Arbeitskraft an das Kapital zwingt, dann die rechtlichen Rahmenbedingungen, von denen hier noch zu sprechen sein wird, und schließlich die Frage der politischen Macht der organisierten Arbeitenden, im Betrieb, der Branche, dem Staat beziehungsweise weltweit.

Bild 2: Bits kontrollieren, Daten aggregieren

Es dringt Mitte des zweiten Jahrzehnts des 21. Jahrhunderts immer mehr ins breite Bewusstsein vor, dass wir nicht kontrollieren können, wer wo Daten über uns hat und was mit diesen Daten geschieht. Es lässt sich nicht mehr verhindern, dass Staat und Behörden, dass Infrastrukturanbieter und Sozialversicherungen, dass Unternehmen und Vereine detaillierte Daten über uns besitzen, gespeichert in *bits'n'bytes* … und mithin allzu einfach kopier-, verlier- und verknüpfbar. Die Daten, was sie über uns aussagen, wie sehr sie in die Tiefe gehen, was sich mit ihnen anstellen lässt, all das ist verschiedener Natur. Es macht einen Unterschied, dass der Handelskonzern aus unseren Einkäufe einiges über einen ganzen Haushalt errechnen kann, was ein AMS aus „Kundendaten“ über uns weiß, oder ob Vorgesetzte wissen, wo wann auf welcher Straße Mitarbeiter_innen wie schnell und mit welchem Verbrauch gefahren sind.

Der erste große Unterschied liegt im Abhängigkeitsverhältnis unabhängig irgendwelcher Datenlagen, also bevor wir davon ausgehen, dass eine Behörde, ein Unternehmen oder unser Arbeitgeber Daten über uns sammelt. Unsere Position gegenüber dem Staat ist die der Bürger_in. Den Unternehmen stehen wir als Nutzer_innen, Kund_innen, Konsu-

ment_innen gegenüber. Und in der Arbeit sind wir Arbeiter_innen, Angestellte oder Dienstnehmer_innen gegenüber Vorgesetzten. Für jede dieser Dimensionen gibt es nun eigene spezifische Rechtsverhältnisse, unterschiedliche Möglichkeiten der Kontrolle bzw des Einspruchs, der Rechtsdurchsetzung im Fall des Falles.

Ein weiterer großer Unterschied zwischen den Verhältnissen (1) Staat-Bürger_innen, (2) Unternehmen/Kund_in, (3) Betrieb/Lohnabhängige liegt in den verschiedenen Interessensstrukturen und in weiterer Folge den Praktiken, Kulturen. Diese Differenz bleibt auch eingedenk dessen relevant, dass die Praktiken der Kontrollgesellschaft und des Neoliberalsmus da wie dort auf dem Vormarsch sind. Umgekehrt bestehen innerhalb der oben unterschiedenen Verhältnisse Differenzen; also etwa in den Interessen der Geheimdienste oder Krankenkassen, zwischen den Praktiken lokaler Buchhändler und dem weltweiten Versandhandelskonzern, bezüglich der Managementkultur beispielweise im Call-Center oder am Bau.

Die Interessen, gängige Praktiken und Kulturen bestimmen weitgehend, wo welche Daten erfasst werden und wie mit ihnen umgegangen wird. Bei all der daraus entstehenden Bandbreite bleiben die Unterschiede relevant, bleibt der strukturelle Interessenskonflikt zwischen Kapital und Lohnabhängigen grundlegend.

Der dritte Unterschied liegt in der Dichte, Konzentration und Verfügbarkeit der Informationen. Im Betrieb fallen pro Mitarbeiter_in laufend jede Menge exakter Daten auf vielen Ebenen an und sie liegen, mehr oder weniger, in einer Hand. Laufend heißt über die gesamte Arbeitszeit hinweg, stundenlang, täglich, über Jahre hinweg. Jede Menge heißt, dass neben Personal- und Lohnverrechnungsdaten viele andere hinzukommen wie etwa aus der Zeiterfassung, Produktion, betriebsinternen Kommunikation, Zutritts- und Leistungskontrolle etc. Exakt heißt, dass diese Daten auf und mit den Systemen des Unternehmens unter eindeutiger Identifikation der einzelnen Mitarbeiter_in bit für bit erfasst werden können. Das erledigt schon jeder Tastenanschlag und Klick eingeloggter Mitarbeiter_innen auf den „ *devices*“ oder die Zutrittsmagnetkarte, das Telefonsystem, der im Qualitätsmanagment festgelegte Arbeitsablauf usw.

Dort wo rechtliche Rahmen der Datenerfassung Grenzen setzen und organisierte Lohnabhängige auf Einhaltung dieser Grenzen drängen, wirken digitale Logik und Kapitalismus diametral Richtung Entgrenzung. Daten zu erfassen und zu speichern geht fast mühelos und ist kostengünstig. Daten auszuwerten und mit wiederum anderen Daten zu verknüpfen, verspricht in der digitalen Welt Mehrwert. Was sich mit in Nullern und Einsern gesicherten Informationen machen lässt, steht in keinem Verhältnis zu den Kosten.

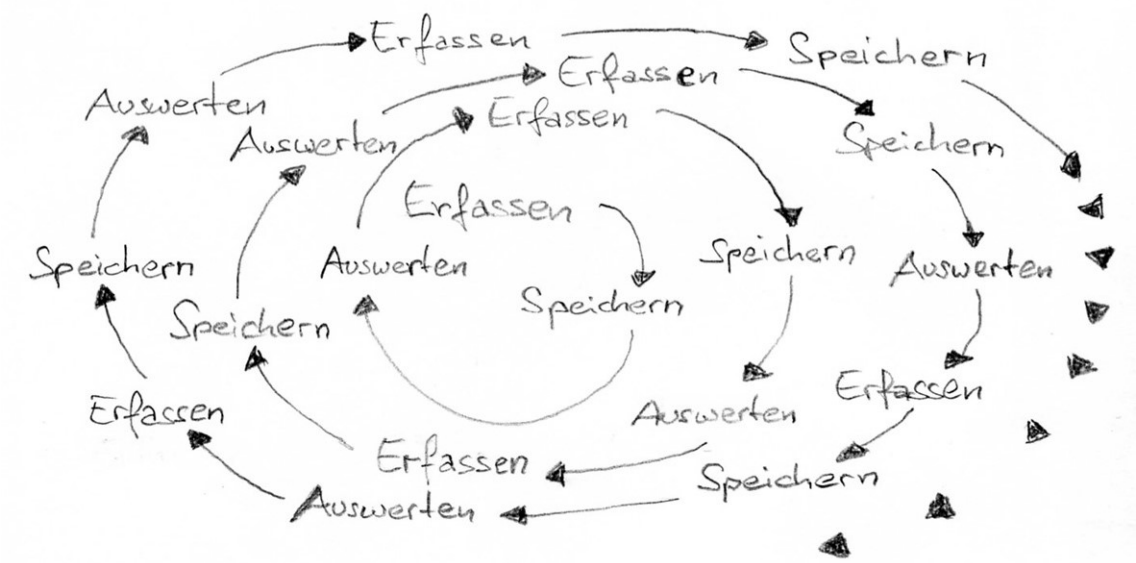

Bild 2: Die Mehrwert versprechende Spirale aus Daten Erfassen, Sichern, Auswerten usw.

Aus dem analogen Informationen Besorgen wird im pathologischen Extrem digitaler „*Datensammelwahn*“. Aus dem Bedürfnis, Wissen archiviert und zugänglich zu halten, wird das krankhafte Speichern jedweder *bit's'bytes* auf Vorrat, wird anlasslose „*Vorratsdatenspeicherung*“. Aus dem Bedürfnis die Welt besser zu erkennen und zu beherrschen, wird der triebhafte Zug zur „*Rasterfahndung*“. Freilich sind diesen Schritten in der digitalen Welt immer noch Schranken gesetzt, sie werden aber weiterhin kleiner.

Der technologische Fortschritt in Bezug auf Sammeln, Speichern, Auswerten wird vorangetrieben, angetrieben durch die Erwartungshaltungen des Kapitals. Das notwendige Know-how verbreitet sich und wird abgesenkt, dh., dass für Kund_innen spezielle und bedienungsfreundliche Anwendungen produziert werden (wie zB. Hard- und Software, die dem Management bessere Überwachung der Mitarbeiter_innen und Kontrolle der Belegschaft bieten). Rechtliche Schranken und Einschränkungen werden – mit großem Druck von Seiten des Kapitals – abgebaut.

Bild 3: Verstärkung asymmetrischer Machtverhältnisse

„*Daten sind das Öl des 21. Jahrhunderts*“, heißt es, und als solches wollen sie gefördert, verarbeitet und ausgewertet werden. Sie können zweifellos kapitalisiert werden. Dadurch werden jedoch nicht so sehr asymmetrische Machtverhältnisse geschaffen, als dass bereits vorhandene, abgesicherte Asymmetrien Voraussetzung dazu sind, Daten in Kapital umwandeln zu können. Die Möglichkeit dazu setzt in der Regel eine privilegierte Position voraus und liegt nicht in den *bit's'bytes* selbst begründet.

Daten könn(t)en schließlich genauso offen und frei zugänglich sein. Sie können Mittel zum Abbau von Asymmetrien sein, sind das manchmal auch. Viel wahrscheinlicher sind sie aber Mittel zur Absicherung eines Machtungleichgewichts. Weniger abstrakt ausgedrückt, es liegt nicht in an Daten, die z.B. Unternehmen über uns als Lohnabhängige haben, dass wir einfacher zu beherrschen sind. Vielmehr liegt es an den Möglichkeiten des Unternehmens, ungeahnt detaillierte personenbezogene Informationen über uns zu besitzen sowie weitgehendst sanktionsfrei gegen uns und unsere Interessen zu nutzen.

Dass bestehende asymmetrische Machtverhältnisse vor diesem Hintergrund weiter verstärkt werden, hängt also wesentlich mit der Frage von Besitz und Eigentum von Daten zusammen, mit der Verteilung von Rechten an Information und ihrer Verwendung. Klar, das galt schon vor der digitalen Revolution. Wer Informationen anhäufen und den Zugang beschränken oder die Nutzung durch andere sogar ausschließen kann, hat eine privilegierte Position und kann sich weitere Vorteile verschaffen.

Die technischen Grundlagen der digitalen Welt legen dagegen eher nahe, dass Beschränkung und Ausschluss von Information schwieriger geworden sein müsste. Daten sind in ihrer Natur als *bits'n'bytes* leichter denn je allen zugänglich. Es sind also nicht die eingangs geschilderten technischen Bedingungen, die Asymmetrien fordern und fördern, jedenfalls nicht alleine. Es sind Fragen der Rechte, der Ressourcen, des Eigentums (an Produktionsmitteln) und von Kontrolle, Mitbestimmung, Sanktionen.

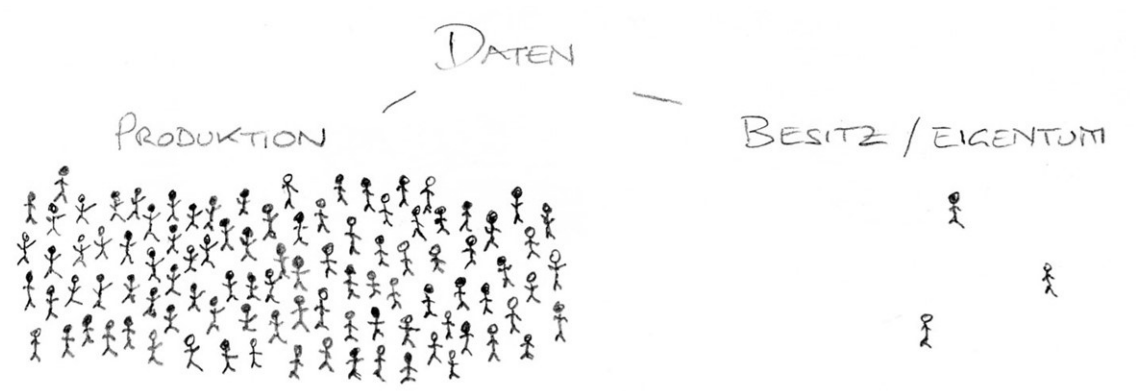

Bild 3: Ein bekanntes Bild, der Gegensatz von Produktion und Eigentum, hier für Daten.

Der Blick auf Produktion versus Besitz bzw. Eigentum von Daten wird an dieser Stelle Viele an die vordergründigen Produkte von Unternehmen denken lassen, an Werke, an Dienstleistungen, die angeboten und verkauft werden. Für die prekäre Situation der gläsernen Lohnabhängigen sind diese Daten weniger relevant, als die „Metadaten“ der Arbeitsprozesse. Produktion, das Arbeiten mit den (und auf den) Produktionsmitteln des Unternehmens, könnte auch ohne Erfassung personenbezogener Daten über die Lohnab-

hängigen funktionieren. Gläsern werden die Arbeitenden erst dadurch, dass auf den Produktionsmitteln erfasste *bits* konkret einer einzelnen der vielen im Betrieb arbeitenden Lohnabhängigen zuordenbar sind.

Wir sind somit wieder beim Bild des MitM-Unternehmens angelangt. Durch die Auswahl und Konfiguration der eingesetzten technischen Systeme und *devices* steuert das Unternehmen, welche *bits'n'bytes* von Lohnabhängigen produziert werden und welche dabei anfallenden Informationen einzelnen Personen zugerechnet werden können. Die zur Kontrolle der Arbeitenden geeigneten Daten fallen nicht einfach automatisch im auf die Produktion ausgerichteten Arbeitsverlauf an. Es braucht eine Unternehmensleitung, die zielgerichtet die Art, die Quantität und die Qualität der ihr zur Verfügung stehenden Daten festlegt, in dem sie eine gewisse digitale Arbeitsumgebung und -abläufe vorschreibt. Dabei wird naheliegender Weise nicht allein an die Notwendigkeiten der Produktion gedacht, sondern – je nach Interessen, gängige Praktiken und Managmentkulturen – an die Bedürfnisse der H&R-Abteilung, des Controlling, der Compliance, der IT usw.

Pointierter gesagt: Arbeitsorganisation wird so vorgeschrieben, dass die Lohnabhängigen mir jeder Operation selbst die Informationen zu ihrer Kontrollierbarkeit liefern, für die Reproduktion der herrschenden Reproduktionsverhältnisse.

Bild 4: Like Puppets on a String, die Dystopie

Fassen wir zusammen, was wir bis hierhin wissen, und stellen wir die Frage, was das im worst-case bedeuten könnte: Erstens bedeuten zugewiesene Arbeitsplätze und -geräte im digitalen Zeitalter, rundum in eine intransparente *Man-in-the-Middle*-Umgebung eingebettet zu sein.

Zweitens wissen wir, dass die digitalen Arbeitsumgebungen ständig Informationen über die in ihnen Tätigen sammeln. Die Arbeitenden produzieren einen Gutteil der exakten personenbezogener Daten sogar selbst. Die Summe der durch Messgeräte, Sensoren und die Aktionen der Arbeitenden anfallenden Daten sind darüber hinaus unmittelbar im Besitz des Unternehmens.

Aus diesen ersten Punkten folgt drittens, dass Daten jederzeit verknüpft und personenbezogen ausgewertet werden könn(t)en, ohne dass die Betroffenen etwas davon mitbekommen.

Viertens verstehen wir, dass Unternehmensleitungen die von ihnen beherrschte digitale

Arbeitsumgebung gezielt so einrichten, dass Lohnabhängige nicht nur die für die Produktion von Waren und Dienstleistungen notwendigen Daten produzieren. Immer mer technische Systeme und Arbeitsabläufe haben nicht unmittelbar mit der Produktion zu tun sondern dienen der Überwachung, Kontrolle und Beherrschung der Arbeitenden.

Betrachten wir das alles fünftens im Angesicht jüngerer Entwicklungen wie *data mining* und *big data*. Was mit Datenbeständen, wie sie in modernen Unternehmen über Lohnabhängige anfallen, alles gemacht werden kann, ist schlechterdings nicht absehbar. Die vage Formulierung ist bewusst gewählt. Wir bekommen gesellschaftlich eben gerade erst eine Ahnung, welche Möglichkeiten *data mining* in riesigen Datenmengen bringen wird. Wir wissen, dass sie immens sein werden. Bereits jetzt finden stochastische Modelle Anwendung, auf Basis derer Wahlverhalten progostiziert werden, genauso wie deviantes Verhalten, psychologische Eigenheiten, Leistung- und Krankheitserwartungen je nach Veränderung der Arbeitsumgebung, … oder sehr früh die Schwangerschaft einer Lohnabhängigen, die von ihrem Glück selbst noch gar nichts weiß. Alles was es dazu braucht, ist nicht einmal *big data* sondern lediglich ein personenbezogen erfassendes Zutrittssystem mit Sensoren zwischen Arbeitsplatz und Toilettanlagen und die Software, die Veränderungen in der Frequenz und Dauer des Aufs-Klo-Gehens mit dem Muster bei eintretenden Schwangerschaften abgleicht. Das ist nun nicht die Zukunft sondern seit zwei Jahrzehnten Realität.

Sechstens müssen wir uns vor Augen halten, dass detaillierte personenbezogene Daten Geld wert sind und dass Datensätze zu Personen weltweit gehandelt werden. Da z.B. Kundendaten regelmäßig verkauft werden, müssen wir im worst-case davon ausgehen, dass selbiges für die detaillierten Daten aus dem Arbeitsprozess gilt. Außerdem ist bekannt, dass Datenbestände mitunter verloren gehen können. Unternehmen tauschen untereinander Informationen über Lohnabhängige aus. Der Staat kann an die aussagekräftigen Daten kommen. Die Frage ist also nicht, ob das passiert, sondern in welchem Ausmaß das die Regel wird: *data mining* unter Einbeziehung von „Arbeitswelt-Daten“ verknüpft mit Datenbeständen aus anderen Quellen. Besitzer_innen derart umfassender Datenbanken werden mehr über uns modellieren können, als wir über uns selbst wissen.

Siebentens sollten uns bewusst sein, dass all diese Möglichkeiten der Überwachung und Kontrolle das Geschäftsmodell boomender Branchen und Industrien sind. Eine Unternehmensleitung muss sich nicht selbst einfallen lassen, wie sie die digitale MitM-Umgebung eines Betriebs zur Kontrolle der Lohnabhängigen effizienter ausbauen könnte. Den Unternehmen werden von konkurrierenden Spezialist_innen immer ausge-

arbeitetere technische Systeme angeboten, Hardware ebenso wie Software. Parallel zu den neu entwicklten Überwachungs- und Kontrollwerkzeugen verändern sich Management kulturen, verbreiten sich neue Philosophien der „*workforce*“-Überwachung, die auf z.B. auf die ständig fühlbar gemachte Präsenz des *big boss is watching you* setzen. Ein Zugang zu Management hat sich etabliert, der mittels Auswertung personenbezogener Daten zu einem *ranking* darauf setzt, pro Quartal die Mitarbeiter_innen in der unteren Dreierperzentile zu kündigen, um über den Weg die *human ressources* zu optimieren.

Schließlich ist achtens zu beobachten, dass rechtliche Rahmenbedingungen national, auf EU-Ebene und global (bzw transnational) Schritt für Schritt unvorteilhafter werden, sei es für Bürger_innen oder Lohnabhängige. Im internationalen Vergleich haben die Beschäftigten in Österreich noch dazu am meisten zu verlieren. Sie haben bei Anpassungen an neue EU- oder globale Rechtsordnungen am meisten zu verlieren.

Es ist mit fortschreitender Aufzählung absehbar, was vom *worst-case* zu erwarten ist. Die Daten, die Arbeiter_innen weltweit selbst für ihre Kontrolle mitproduzieren, zementieren das asymmetrische Machtverhältnis zwischen Kapital und Arbeit weiter ein. Die gläserne Lohnabhängigen sind im großen Stil und bis zur einzelnen Person runtergebrochen ausrechenbar. Im Angesicht neuer mächtiger Überwachungs- und Kontrolltechniken bei im worst-case als beseitigt anzunehmenden rechtlichen Einschränkungen, gilt das von der Ebene der einzelnen Betriebsabteilung über die Größenordnung des transnational agierenden Konzerns bis hin zur gesamtgesellschaftlichen Dimension.

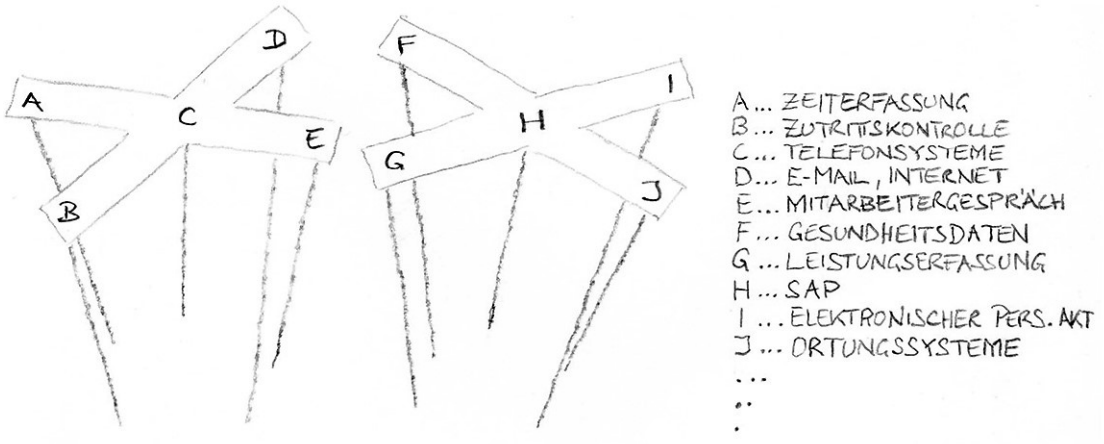

Bild 4: Steuerungsoptionen durch Kontrolle personenbezogener Datenbestände.

Lohnabhängige sind in der aus dem worst-case abgeleiteten Dystopie zu Marionetten degradiert bzw. auf den Wert digitaler Profile reduziert. Auf Basis ihrer Erwerbsabhängigkeit werden sie gezwungen, genau jene Daten selbst zu produzieren, durch sie vollständig überwachbar, aggregierbar und in Modellszenarien ausrechenbar sind.

Bild 5: Realität der Zustimmungspflicht

Der worst-case ist ein Gedankenexperiment. Die Realität sieht anders aus. In ihr haben Arbeitnehmer_innen Rechte. Sie haben Möglichkeiten, diese durchzusetzen. Wie sehen die Rechte, wie die Möglichkeiten aus?

Technische Systeme, die personenbezogene Daten verarbeiten und nicht unter die definierten Standardanwendungen fallen wie diese in der „ *Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000* “ festgeschrieben sind, müssen erstens im Datenverarbeitungsregister (DVR) gemeldet werden und sind zweitens, in Betrieben zwischen Arbeitnehmer_innen und Arbeitgeber, zustimmungspflichtig nach § 96 des Arbeitsverfassungsgesetzes.

„*Folgende Maßnahmen des Betriebsinhabers bedürfen zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates* “, setzt Absatz (1) an, um in Zeile 3 aufzuführen, „ *die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren*“.

Der Einsatz von E-Mail und Internet – beides berührt die Menschenwürde und bringt die technische Möglichkeiten zur Kontrolle durch den Arbeitgeber mit sich – ist also zustimmungspflichtig. Digitale Telefonsysteme, die Zeiterfassung, die Verwendung digitaler Personalakten, eine mobile Leistungserfassung, Videoüberwachung, auf Personendaten basierende Zutrittssysteme usw. … all das ist zustimmungspflichtig. Wer muss diese Zustimmung einholen und wer gib sie?

Wird ein personenbezogene Daten verarbeitendes System eingesetzt und es gibt keinen Betriebsrat im Betrieb, hat das Unternehmen die schriftliche Zustimmung von jeder einzelnen Arbeitnehme_in einzuholen. In vielen Betrieben geschieht dies auch, üblicherweise bei der Einstellung neuer Mitarbeiter_innen mit der Unterschrift unter den Dienstvertrag. Wird ein neues technisches System im Betrieb eingeführt, wird den Lohnabhängigen etwas zur Unterschrift vorgelegt, z.B. ein „code of conduct“, mit dem auch die Zustimmung zum Einsatz des Systems mitunterzeichnet wird. Unterzeichnen einzelne Mitarbeiter_innen dergleichen nicht, dürften ihre Daten im jeweiligen System nicht vorkommen und sie die Systeme nicht verwenden.

Gibt es einen Betriebsrat, müsste für zustimmungspflichtige technische Systeme eine eigene Betriebsvereinbarung (BV) zwischen Geschäftsführung (GF) und Betriebsrat (BR) unterzeichnet werden. Diese Betriebsvereinbarung, die es übrigens vor Einsatz solcher Systeme und auch schon für Probebetriebe geben sollte, regeln nicht nur die Zustim-

mung für die gesamte Belegschaft sondern halten auch vertraglich fest, wie ein techni - sches System im Betrieb eingesetzt wird, welche Daten erfasst werden dürfen, was mit ihnen geschehen darf, wer Zugang zu Auswertungen hat, wie in heiklen Fällen vorzu - gehen ist und über welche Instrumentarien der Betriebsrat als gesetzliche Vertretung der Beschäftigen seine Kontrollrechte umsetzen kann.

Freilich kommt es vor, dass technische Systeme in Betrieben ohne weitere Regelung und ohne Zustimmung im Einsatz sind. Diese dürften dann zwar nicht laufen, aber wo das nicht bekannt ist, oder wo das zwar bekannt ist, sich die Lohnabhängigen einzeln oder als Betriebsrat organisiert jedoch nicht durchsetzen, kümmert sich niemand darum, diese Systeme abzudrehen, bis ihr Einsatz für die Betroffenen zufriedenstellend geregelt ist. Das ist aber das Mittel, eine zufriedenstellende Regelung für alle zu treffen, mit der die spezifische Form des Ausgeliefertseins der gläsernen Lohnabhängigen möglichst vollends entschärft wird.

Lohnabhängige sollten sich aus ihrer prekären Situation heraus daher klären, (1) welche zustimmungspflichtigen technischen Systeme im Betrieb im Einsatz sind, (2) ob diese per Betriebsvereinbarungen geregelt sind, (3) wie diese Betriebsvereinbarungen und darin enthaltene Regelungen aussehen, (4) ob sie zufriedenstellend geregelt sind und (5) wie ihre Einhaltung im Fall des Falles kontrolliert werden kann.

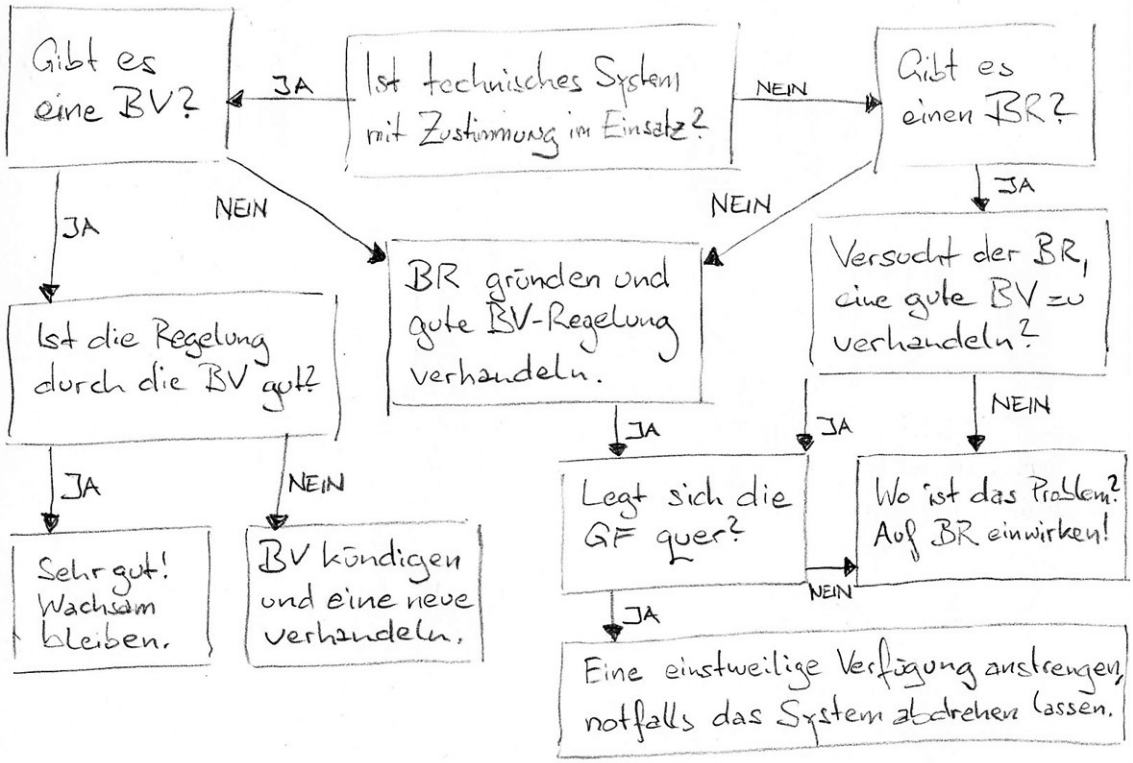

Bild 5: Fragen, die Lohnabhängige pro personenbezogene Daten verarbeitendem System klären sollten.

Gehen wir davon aus, dass es einen Betriebsrat gibt. Er will eine Betriebsvereinbarung erreichen. Wie gehen die Mitglieder des BR vor, worauf sollte geachtet werden?

Erstens gilt, dass es die GF sein sollte, die einen Entwurf für eine neue BV dem BR vorlegt. Sie ist es, die das System einführen will. Vor Unterzeichnung der BV lehnt der BR die Inbetriebnahme des technischen Systems ab. Auch der Testbetrieb wäre abzulehnen, sollten reale Daten von Mitabeiter_innen verwendet werden. Für den Testbetrieb sollte in dem Fall eine eigene BV denselben regeln, besonders die Frage, was nach Ablauf des Testbetriebs mit den Daten realer Mitarbeiter_innen geschieht.

Nehmen wir an, das neue System, das eingeführt werden soll, ist z.B. ein „*SAP Enterprise Resource Planning (ERP) Core Human Resources*“-System. Oder unser Unternehmen will eine Social Media Anwendung im Betrieb ausrollen, etwa Googles *g+* oder Microsofts *Yammer*. Als BR sind wir von diesen Plänen vorab zu informieren und haben Anspruch auf die schriftlichen detaillierten technischen Beschreibungen des Systems, wie es nach Absicht der GF eingeführt werden soll.

Diese technischen Spezifikationen sehen die BR-Mitglieder genau durch, holen sich Unterstützung in der Beurteilung, suchen nach Erfahrungen in anderen Betrieben und formulieren dann Fragen, die sich aus den technischen Spezifikationen und für den Einsatz notwendigen Daten ergeben. Wahrscheinlich bekommt der BR eine Verkaufspräsentation des Systems angeboten, die vom Anbieter *SAP*, *google* oder *Microsoft* vorgenommen wird.

Parallel zur Überprüfung der technischen Spezifikationen bittet der BR die GF um eine schriftliche Präsentation, was mit dem System im Betrieb erreicht werden soll. Was ist der Zweck der Einführung? Dieser Punkt, die schriftliche Definition des Zwecks, ist äußerst wichtig, wie wir gleich sehen werden. Vom Zweck ist nämlich abzuleiten, ob er für den Unternehmenserfolg notwendig gerechtfertigt ist, ob er den Einsatz eines konkreten Systems und die Erfassung bestimmter personenbezogener Daten durch ihn gerechtfertigt sind, ob er nicht auch anders und mit gelinderen Mitteln erreicht werden könnte und, falls der Zweck tatsächlich die Erfassung und Speicherung personenbezogener Daten gerechtfertigt, wann diese Daten wieder gelöscht werden können bzw. gelöscht werden müssen.

Die Ziele des BR müssen sein, dass erstens so wenig personenbezogene Daten als möglich erfasst und wo immer möglich anonymisiert verarbeitet werden. Zweitens sollte sichergestellt sein, dass einmal erfasste personenbezogene Daten bei erster Gelegenheit

gelöscht werden. Drittens sind technische Systeme und ihre Datenbanken so voneinander abzugrenzen, dass Verknüpfungen über ihre Datenbestände hinweg möglichst schwierig sind. Solche Auswertungen sind verboten, sie sollten also nicht zu einfach mit wenigen Operationen möglich sein. Es gilt Hürden einzubauen, nicht nur auf die rechtlichen vertrauend sondern technische einbauend.

Viertens sollte der BR die Kontrollrechte derart operationalisiert festschreiben lassen, dass sie der ungünstigen MitM-Ausgangslage zum Trotz und auch bei etwaigen Auslagerungen von IT-Dienstleistungen effektive Einsicht und guten Überblick ermöglichen. Mit dem Hebel der gesetzlichen Vertretung der Interessen der Mitarbeiter_innen im Betrieb müssen wir danach trachten, präventiv die pathologischen Auswüchse eines „*Datensammelwahns*“, einer „*Vorratsdatenspeicherung*“ und einer „*Rasterfahndung*“ auszuschließen.