Corona als Türöffner für Überwachung der Mitarbeiter

22.07.2020, von Tobias Riegel | Originalartikel

Auch private Unternehmen wollen nun Tracking-Apps zur internen „Kontaktverfolgung" der Mitarbeiter nutzen: als Vorbedingung für die angebliche „neue Normalität" in der Arbeitswelt. Das Vorhaben birgt grosse Gefahren, von „Freiwilligkeit" kann keine Rede sein. Es drohen Massnahmen zur Überwachung, die vor Corona undenkbar gewesen wären. Von **Tobias Riegel**.

Die offizielle „Corona-Warn-App" des Robert Koch-Instituts (RKI) soll helfen, Infektionsketten zu verfolgen. Etwas Ähnliches haben nun internationale Beratungsfirmen für den Einsatz in Firmen und Betrieben entworfen, wie Medien berichten. So erklärte ein Sprecher der internationalen Wirtschaftsprüfer-Firma Price-Waterhouse-Coopers (PWC) aktuell im „Deutschlandfunk" (DLF):

„Wir haben nicht nur eine App entworfen, sondern wir haben ein ganzes Ökosystem an Werkzeugen entworfen, die am Ende des Tages den Unternehmen helfen sollen, wieder zur Normalität zurückzukehren."

Die Einführung eines „Ökosystems" an Werkzeugen zur betriebsinternen Überwachung der Mitarbeiter wird von PWC mit dem „Schutz der eigenen Mitarbeiter in Bezug auf Hygiene und Infektionsrisiken" begründet. Die Software funktioniere im Grunde ähnlich wie die RKI-App, „verfügt aber über einen weitaus grösseren Funktionsumfang", so PWC. Denn: Während bei der RKI-App die Anonymität grossgeschrieben werde, hätten Unternehmen – im Gegensatz dazu – ein grosses Interesse daran, einzelne und konkrete Fälle zu identifizieren und Kontakte im Unternehmen nachzuvollziehen, erklärt mitfühlend der DLF.

Überwachung: „Freiwillige" Nutzung zum „Schutz" der Mitarbeiter

PWC will die App im eigenen Betrieb nutzen, aber auch international an andere (laut PWC zahlreiche) Interessenten verkaufen. Laut PWC würde sogar bereits ein DAX-Konzern die Werkzeuge nutzen – welcher, wird nicht verraten. Laut DLF haben auch andere IT-Firmen oder Unternehmensberatungen wie die Boston Consulting Group (BCG) erkannt, dass Firmen einen Bedarf an „Pandemie-Kontrollsystemen" hätten, und würden diese nun anbieten.

Dabei proklamieren die meisten Unternehmen, die Nutzung der Apps beruhe auf Freiwilligkeit der Mitarbeiterinnen und Mitarbeiter. Doch diese „Freiwilligkeit" ist gegenüber dem Arbeitgeber nicht gegeben. Der Anwalt Ifeoma Ajunwa von der US-amerikanischen Cornell University erklärte zudem gegenüber der österreichischen „Krone":

„Gefährlich werde es, wenn die von den Firmen über ihre Mitarbeiter gesammelten Daten missbraucht werden. (…) Verkaufen sie die Daten vielleicht an ein Versicherungsunternehmen? An Datenhändler? An Banken oder Autoversicherer, die uns dann die Versicherung verweigern oder Kreditraten erhöhen? Damit könnte alles Mögliche passieren."

Auch Diskriminierung drohe, wenn Chefs zu viel über das Privatleben der Mitarbeiter wüssten, so Ajunwa in dem Medium. In Unternehmen, in denen auf Covid-19 getestet wird, sei es zudem eine Möglichkeit, die DNA der Mitarbeiter zu analysieren – und dann beispielsweise auf dieser Basis besonders durch Covid-19 gefährdete Menschen eher zu entlassen als andere.

Corona als „11. September" für die Betriebsüberwachung

Die „Krone" berichtet von weiteren Systemen: So fänden Tracking-Armbänder zur betriebsinternen Mitarbeiter-Überwachung (etwa der Firma Microshare) „reissenden Absatz". Auch das Geschäft mit Bilderkennungs-Systemen „boome": Statt mit Armbändern zu überwachen, ob die Arbeiter Distanz halten, gehe das auch mit Systemen, die auf Künstlicher Intelligenz beruhten. Den gesellschaftlichen und den individuellen Widerstand gegen diese Massnahmen sieht etwa der Microshare-Firmenchef Mike Moran bereits bröckeln: So wie wir uns nach den Anschlägen vom 11. September an verstärkte Sicherheitskontrollen im öffentlichen Raum gewöhnt hätten, werde man sich auch an mehr solche Systeme im Arbeitsalltag gewöhnen. Eine nun verbreitete Losung lautet, dass die fragwürdigen Massnahmen angesichts „der Pandemie" von vielen Mitarbeitern akzeptiert würden, weil sie „sich selbst" den „bestmöglichen Schutz vor einer Ansteckung am Arbeitsplatz" wünschten.

Anna Elliott von der Anwaltskanzlei Osborne Clarke sagte dagegen laut „Krone" gegenüber der britischen BBC: „Manager könnten in Versuchung geraten, ins Privatleben der Mitarbeiter einzudringen. Mit wem verbringt der Mitarbeiter privat seine Zeit? Gibt es Risikofaktoren für das Unternehmen?" Solche Fragen gingen aber zu weit, so Elliott laut „Krone". Trotzdem könnten manche Firmen ins Privatleben der Mitarbeiter eindringen – schon allein, weil sich in einer Zeit hoher Arbeitslosigkeit wohl kaum jemand trauen würde, dem Chef beispielsweise das Ausfüllen eines intimen Fragebogens zu verweigern.

In Firmen weniger „Hürden" als in Demokratien

Das Magazin „T3N" betont, dass es „anders als in demokratischen Staaten im Verhältnis zwischen Bürger und Regierung" zwischen Arbeitgeber und Arbeitnehmer „weit weniger Hürden zu nehmen" gebe, wenn „Arbeitgeber ihre Arbeitnehmer zur App-Nutzung verpflichten wollen". PWC verspricht laut „T3N" die Einhaltung hoher Datenschutz- und Sicherheitsstandards. Der

Zugriff auf die gespeicherten Daten solle zwar zentral erfolgen. Der Zugriff sei jedoch auf wenige Personen mit Admin-Status begrenzt.

Solche fadenscheinigen Massnahmen zur „Vertrauensbildung" beschreibt auch das Medium „Netzwoche" aus der Schweiz: Demnach unterstreiche PWC die Notwendigkeit eines „angemessenen Change Managements während der Umsetzung". Und die französische Bank Crédit Agricole empfehle, „dass die Nutzung ihrer App auf einem Vertrauenspakt zwischen Arbeitgeber, Arbeitnehmern und Gewerkschaften basieren sollte". Auch Crédit Agricole hat demnach vor kurzem ihren Plan für eine „Rückkehr an den Arbeitsplatz" vorgestellt. Eine mit dem IT-Dienstleister Onepoint zusammen entwickelte COPASS-Anwendung ermögliche es den Mitarbeitern der Bank, ihre Gesundheit zu überwachen, so „Netzwoche".

Der „gläserne Mitarbeiter"?

Der auf Datenschutz spezialisierte Jurist Sylvain Métille stellt im gleichen Medium die Legitimität und Verhältnismässigkeit der vom Arbeitgeber angeforderten Informationen stark in Frage sowie die angebliche „Freiwilligkeit". In der „Netzwoche" ergänzt er:

„Skeptisch ist der Experte auch hinsichtlich der Anonymität der bereitgestellten Daten. Beispielsweise fragt die Lösung von Medikal Link nach der Telefonnummer des Mitarbeiters, und die PwC-App fordert den Mitarbeiter auf, Informationen über seine Geschäftsabteilung und die nächstgelegene Stadt anzugeben. Das macht es in einigen Fällen leicht, den betreffenden Mitarbeiter zu identifizieren."

Dass die hochproblematischen und bis vor kurzem noch undenkbaren Überwachungstechniken mit dem „Schutz" der Mitarbeiter begründet werden, sollte nicht überraschen – die Bürger sollten sich von diesen Lippenbekenntnissen aber nicht in die Irre führen lassen.

Auch haben die nun von privater Seite geplanten und bereits genutzten – mutmasslich teils illegalen – Werkzeuge eine ganz andere und bedrohlichere Qualität als die offizielle Corona-Warn-App. Und bereits bei dieser harmloseren Variante des RKI bestehen Zweifel, ob der Eingriff in die Selbstbestimmung der Daten und der un-dokumentierten Bewegungsfreiheit der Bürger mit dem Ergebnis gerechtfertigt werden können. Es scheint eher, dass auch hier potenzieller Schaden und realer Nutzen in einem Missverhältnis stehen, wie auch auf anderen Gebieten der „Pandemie"-Bekämpfung. Vor etwas über einem Monat hat die Bundesregierung die Corona-Warn-App vorgestellt. Ob die App so funktioniert, wie sie soll, ist nach wie vor unklar, wie „Heise Online" in diesem Artikel beschreibt: Hinweise auf einen nennenswerten Einfluss der App auf den Verlauf der SARS-CoV-2-Epidemie in Deutschland gebe es jedenfalls nicht.