TRANSPARENZ ERMÖGLICHEN:

INTELLIGENTE DIGITALE SYSTEME ZUR VERBESSERUNG DER SICHERHEIT UND GESUNDHEIT DER BESCHÄFTIGTEN

Intelligente digitale Systeme zur Verbesserung der Sicherheit und Gesundheit der Beschäftigten[1] sind Systeme, die digitale Technologien nutzen, um Daten zur Ermittlung und Bewertung von Risiken, zur Vermeidung und/oder Minimierung von Schäden sowie zur Förderung von Sicherheit und Gesundheit bei der Arbeit zu sammeln und zu analysieren.[2]

Häufig basieren diese Systeme auf Datenerfassungsgeräten wie Sensoren, Kameras, Mikrofonen usw., die Daten über Bluetooth, Radiofrequenz-Identifikation oder das Internet der Dinge an eine Cloud-Plattform übertragen. Im letzteren Fall verarbeiten Algorithmen der künstlichen Intelligenz (KI) und des maschinellen Lernens (ML) Daten und wandeln sie in Informationen um, die Arbeitgeber:innen nutzen können, um Risiken vorzubeugen oder auf sie zu reagieren. Natürlich gibt es auch andere Möglichkeiten: von intelligenten Überwachungssystemen, die erweiterte, virtuelle oder gemischte Realität nutzen, um Beschäftigte in Hochrisikosektoren zu schulen, bis hin zu Drohnen, die Ferninspektionen im Immobilien-, Bau-, Öl- und Gassektor[3] oder im Eisenbahnsektor durchführen, halten diese Systeme zunehmend Einzug am Arbeitsplatz und verändern die Bedingungen für das Sicherheitsmanagement.

Untersuchungen der Europäischen Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz (EU-OSHA) haben ergeben, dass Unternehmen und Organisationen die Sicherheit und die Gesundheit ihrer Beschäftigten mithilfe dieser Systeme verbessern können.[4] Allerdings sollten bestimmte Bedingungen erfüllt sein. Dazu gehört die Einbettung der intelligenten digitalen Systeme in den bestehenden Rahmen für Sicherheit und Gesundheit bei der Arbeit, anstatt sie zu nutzen, um ihn zu ersetzen, und das Verständnis, dass die intelligenten digitalen Systeme zusammen mit den Vorteilen Einschränkungen haben können.

Die Untersuchungen der EU-OSHA zeigen außerdem, dass die Beteiligung der Beschäftigten eine wichtige Voraussetzung für die wirksame Umsetzung intelligenter digitaler Systeme ist. Es muss sichergestellt werden, dass die Beschäftigten voll eingebunden sind, wenn ihr Arbeitgeber:innen neue Überwachungstechnologien einführt. Es ist von entscheidender Bedeutung, dass die Arbeitgeber:innen den Bedenken der Beschäftigten hinsichtlich der möglichen Nutzung dieser Systeme Rechnung tragen. Diese Bedenken betreffen in der Regel die mögliche Übertragung der Verantwortung für Sicherheit und Gesundheit von den Arbeitgeber:innen auf die Beschäftigten sowie die Möglichkeit der Nutzung der für die Leistungsmessung erhobenen Daten und die daraus resultierenden potenziellen negativen Auswirkungen auf die Beschäftigten.

Die Frage des Datenschutzes

Die Privatsphäre personenbezogener[5] oder sensibler[6] Daten ist eines der kritischsten Themen in der Debatte über die Nutzung intelligenter digitaler Systeme am Arbeitsplatz. Eines der größten Bedenken in

[1] Der Begriff wird synonym mit den Begriffen „neue Überwachungssysteme im Bereich Sicherheit und Gesundheit bei der Arbeit“ und „intelligente Systeme zur Überwachung“ verwendet.

[2] Europäische Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz (EU-OSHA), *Intelligente digitale Überwachungssysteme für Sicherheit und Gesundheit bei der Arbeit: Nutzen und Herausforderungen, 2023,* Abrufbar unter: https://osha.europa.eu/en/publications/smart-digital-monitoring-systems-occupational-safety-and-health-uses-and-challenges.

[3] EU-OSHA, Drohnen zur Inspektion von Baustellen eines Gasinfrastrukturbetreibers (id16), abrufbar unter: https://healthy-workplaces.osha.europa.eu/de/publications/drones-inspecting-worksites-gas-infrastructure-operator-id16

[4] Ebenda.

[5] Europäische Kommission (ohne Datum). *Was sind „personenbezogene Daten“?* https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

[6] Europäische Kommission (ohne Datum). *Welche personenbezogenen Daten gelten als sensibel?*https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

Bezug auf den Datenschutz ist der potenzielle Missbrauch von Daten von Beschäftigten für die Leistungsmessung, die dann als Grund für Diskriminierung oder in Fällen von ungerechtfertigter Entlassung genutzt werden könnten.

Ein Beispiel hierfür wäre ein intelligentes Überwachungssystem in einem Lagerhaus, das die physischen und physiologischen Merkmale der Beschäftigten erfasst. Ein solches System könnte Beschäftigte mit erhöhter Herzfrequenz oder hohem Stresspegel ermitteln, was bedeutet, dass sie als potenzielle Belastung für das Unternehmen gekennzeichnet werden könnten. Dies wiederum könnte zu Diskriminierung, z. B. in Bezug auf Beförderungen, oder zur Entlassung der Beschäftigten führen. Auch wenn es sich hierbei um extreme Beispiele handelt, so wird doch deutlich, wie wichtig es ist, die Daten von Beschäftigten zu schützen und sicherzustellen, dass sie ausschließlich für Zwecke der Sicherheit und der Gesundheit verwendet werden. Es zeigt auch, wie schwierig das Problem sein kann, insbesondere beim Umgang mit schwierigen Fragen. So bestehen beispielsweise Bedenken, ob es möglich ist, einen Schwellenwert für psychosoziale Faktoren festzulegen, z. B. wie viel „Stress“ an einem Arbeitsplatz akzeptabel ist. Dies wird zusätzlich durch die Tatsache erschwert, dass die einzelnen Personen unterschiedliche Schwellen für Stress haben. Hinzu kommen Fragen wie die Genauigkeit der gesammelten Daten und die Prozesse, die ihre Interpretation bestimmen.

Anhand von Beispielen aus der Praxis werden in diesem Kurzbericht praktische Möglichkeiten aufgezeigt, wie Hersteller:innen oder Entwickler:innen von intelligenten Überwachungssystemen für Sicherheit und Gesundheit bei der Arbeit und ihre Kundschaft, die Betreiber:innen[7] (die Arbeitgeber:innen), Fragen des Datenschutzes angehen und Instrumente zur Förderung der Gesundheit und Sicherheit der Beschäftigten entwickeln können.

Eingebauter Datenschutz

Das Konzept des eingebauten Datenschutzes scheint eine der wirksamsten Ansätze zum Umgang mit dem Datenschutz zu sein. Einige praktische Möglichkeiten, wie Hersteller:innen oder Entwickler:innen in diese Richtung arbeiten könnten, sind die folgenden:

Abbildung 1: Eingebauter Datenschutz

Anonymisierung

Die Anonymisierung personenbezogener Daten, z. B. durch die Zuweisung eindeutiger Kennungen anstelle von Namen der Beschäftigten oder durch den Einsatz von Anonymisierungstechniken, wie die Unschärfe von Gesicht und Körper oder Ghosting, kann eine wirksame und einfache Methode zur Verbesserung des Datenschutzes sein. Diese Lösung ist häufig leicht umsetzbar.

Datenminimierung

Gewährleistung der Datenminimierung. Mit dem technologischen Fortschritt und der kontinuierlichen Miniaturisierung von Sensoren wächst die Versuchung, mehrere Sensoren in Hardware-Geräte wie z. B. Wearables einzubauen und deren Messungen zu integrieren. In diesem Zusammenhang ist jedoch Vorsicht geboten, um zu verhindern, dass Daten erhoben werden, die für die Sicherheit und Gesundheit möglicherweise nicht relevant sind.

Einhaltung

Wenn sichergestellt wird, dass intelligente digitale Systeme die einschlägigen Datenschutzgesetze und -vorschriften einhalten, wie z. B. die allgemeine Datenschutzverordnung[8] in Europa, kann dies ebenfalls zur Verbesserung des Datenschutzes und zur Klärung potenzieller Fragen im Zusammenhang mit der Erhebung und Verwendung von Daten beitragen.

[7] In Veröffentlichungen der EU-OSHA wurden die Begriffe „Designer“, „Implementer“ und „Systemnutzer“ verwendet. Diese Veröffentlichungen wurden erstellt, bevor die Verordnung über künstliche Intelligenz (Verordnung (EU) 2024/1689) verabschiedet wurde. Mit der Verordnung über künstliche Intelligenz wurden auch neue Begriffe wie „Anbieter“ und „Betreiber“ eingeführt.

[8] Europäische Kommission (2016). Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR)Text von Bedeutung für den EWR https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434

Speicherung und Cybersicherheit

Die Speicherung der Daten auf sicheren Servern und die Anwendung strenger Cybersicherheitsmaßnahmen können dazu beitragen, das Risiko von Datenschutzverletzungen zu verringern, die die persönlichen Daten der Beschäftigten gefährden könnten, wenn sie nicht anonym sind.

Je nach dem spezifischen intelligenten Überwachungssystem gibt es auch andere Möglichkeiten, den eingebauten Datenschutz zu gewährleisten. So hat beispielsweise ein Entwickler aus Irland eine KI-Software entwickelt, die Videoaufnahmen analysiert, um unsichere Ereignisse am Arbeitsplatz zu erkennen. Diese KI-Software ist so konzipiert, dass sie „Anonymisierungstechniken“ wie die Unschärfe von Gesichtern und Körpern oder Ghosting einsetzt (siehe Abbildung 2).[9] Wie bereits dargelegt, können sich die meisten Entwickler:innen auch dafür entscheiden, Daten zu anonymisieren und/oder die Daten von Beschäftigten in aggregierter Form zu nutzen, was häufig die wertvollsten Erkenntnisse für Arbeitgeber:innen liefert.

Abbildung 2: Integration des eingebauten Datenschutzes in kamerabasierte intelligente Überwachungssysteme

Freiwilliger Datenschutz

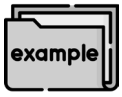
In manchen Fällen ist der eingebaute Datenschutz möglicherweise nicht der geeignetste Ansatz. So ist es beispielsweise in abgelegenen oder risikoreichen Umgebungen wie Bergwerken wichtig, dass intelligente Überwachungssysteme in der Lage sind, Beschäftigte aufzuspüren, insbesondere im Falle eines Rettungseinsatzes. Ebenso ist es in Fällen, in denen intelligente Überwachungssysteme darauf abzielen, die Risiken von Muskel- und Skeletterkrankungen (MSE) zu überwachen und Beschäftigten – unter anderem aufgrund ihres Alters, ihrer Größe, ihres Gewichts und anderer Merkmale – ein personalisiertes Feedback zu bieten, wichtig, dass Zugang zu persönlichen oder sensiblen Informationen besteht. In diesen Fällen kann der Datenschutz nach wie vor durch verschiedene Optionen gewahrt werden. Einige praktische Möglichkeiten, dies zu erreichen, sind in Abbildung 3 dargestellt.

[9] Siehe Präsentationsunterlagen unter euosha-events.eu (2023). „High-level Workshop Smart Monitoring Systems“. https://www.euosha-events.eu/smart-digital-systems/

Abbildung 3: Freiwilliger Datenschutz[10]

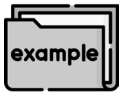
Regelung des Zugangs zu Daten

Die Beschränkung des Datenzugriffs auf bestimmte Personen kann ein wirksames Mittel sein, um sicherzustellen, dass die erfassten Daten ausschließlich für Zwecke der Sicherheit und Gesundheit verwendet werden.



Ein schwedisches Bergbauunternehmen, das ein intelligentes Überwachungssystem mit Geolokalisierungsfunktionen nutzt, speichert alle Daten von Beschäftigten auf einer Festplatte, die sich im Besitz des Arbeitnehmerverbands befindet und auf die ausschließlich dieser Zugriff hat. Unter außergewöhnlichen Umständen, z. B. bei Unfällen, werden Geolokalisierungsdaten an Rettungsteams weitergegeben, um die Zeit der Rettungsmaßnahmen für einzelne Beschäftigte zu verkürzen.

Bei einen in Frankreich ansässigen Entwickler, der intelligente Einlegesohlen herstellt, die mit „Worker-Down"- und freiwilligen Alarmfunktionen für Telebeschäftigte ausgestattet sind, wird das Geolokalisierungssystem der Einlegesohle ausschließlich in Notfällen ausgelöst. Wenn keine Notfälle vorliegen, ist das Geolokalisierungssystem ausgeschaltet.



Ein Entwickler mit Sitz im Vereinigten Königreich, der ein tragbares Gerät zur Überwachung der Risiken von Muskel- und Skeletterkrankungen herstellt, gibt den Beschäftigten direkte Rückmeldungen über Pieptöne und Vibrationen. Das tragbare Gerät ist mit einer begleitenden App verbunden, in der die Beschäftigten ihre individuellen Ergebnisse einsehen und an Mikro-Lernprogrammen teilnehmen können. Gleichzeitig werden dieselben Informationen anonymisiert und in zusammengefasster Form an Fachleute für Sicherheit und Gesundheit bei der Arbeit weitergeleitet, die sie für den Vergleich von Risiken zwischen Beschäftigten, Gruppen und Standorten nutzen können.

Ein niederländischer Entwickler, der eine Software erprobt, mit der Beschäftigte ihr Stressempfinden selbst angeben können, gewährt den Zugang zu diesen Informationen ausschließlich Fachleuten für Sicherheit und Gesundheit bei der Arbeit, z. B. Psychologen, die nicht mit den Personalabteilungen der Arbeitsplätze der Beschäftigten verbunden sind.

Fazit

Beschäftigte haben tendenziell eine positive Einstellung gegenüber der Nutzung intelligenter digitaler Systeme, sofern alle Bedenken hinsichtlich ihrer Nutzung angemessen ausgeräumt und geklärt werden.[11]

Was den Datenschutz betrifft, so können einige Bedenken der Beschäftigten bereits in der Entwurfsphase eines intelligenten Überwachungssystems berücksichtigt werden. Dies kann unter anderem durch die Anonymisierung von Daten, die Minimierung der Erhebung unnötiger Daten und die Einbeziehung von Funktionen wie die Unschärfe von Gesicht und Körper oder Ghosting erreicht werden, wie es bei Kamera-Systemen vorkommt.

[10] Sofern nicht anders angegeben, stammen die Angaben in dieser Abbildung aus euosha-events.eu (2023). „High-level Workshop Smart Monitoring Systems", Präsentationsunterlagen. https://www.euosha-events.eu/smart-digital-systems/

[11] EU-OSHA - Europäische Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz, *Intelligente digitale Überwachungssysteme für Sicherheit und Gesundheit bei der Arbeit: Arbeitsplatzressourcen für Konzeption, Umsetzung und Nutzung*, 2023. Abrufbar unter: https://osha.europa.eu/en/publications/smart-digital-monitoring-systems-occupational-safety-and-health-workplace-resources-design-implementation-and-use.

Wenn solche Maßnahmen nicht die geeignetste Option sind, kann die Festlegung von Dateneigentum und -zugang eine praktische Lösung sein, um datenbezogene Bedenken auszuräumen. Die Beschränkung des Datenzugangs auf Beschäftigte und Fachleute für Sicherheit und Gesundheit bei der Arbeit oder Ärzt:innen sowie die Deaktivierung bestimmter Optionen der intelligenten digitalen Systeme, z. B. die Weitergabe von Geolokalisierungsdaten, wenn keine Notfälle vorliegen, können wirksame Maßnahmen sein, um Bedenken hinsichtlich eines möglichen Missbrauchs dieser Systeme auszuräumen. Ebenso können die Anonymisierung und Aggregation von Daten demselben Zweck dienen.

Zu diesem Zweck können **Konsultationen zwischen Arbeitnehmerverbänden und ihren Mitgliedern** oder deren Vertreter:innen ein entscheidender Erfolgsfaktor für die wirksame Umsetzung intelligenter Überwachungssysteme am Arbeitsplatz sein. Dies kann Arbeitgeber:innen und Beschäftigten dabei helfen, gegenseitige Lösungen für die Nutzung von Daten aus intelligenten Überwachungssystemen zu finden und etwaige Bedenken der Beschäftigten zu klären.

Verfasser:innen: Kyrillos Spyridopoulos, Andrea Broughton (Ecorys).

Projektmanagement: Annick Starren, Ioannis Anyfantis, Europäische Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz (EU-OSHA)

Dieser Kurzbericht wurde von der Europäischen Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz (EU-OSHA) in Auftrag gegeben. Die Inhalte, einschließlich aller geäußerten Meinungen und/oder Schlussfolgerungen, sind ausschließlich diejenigen der Verfasser und geben nicht zwingend die Auffassung der EU-OSHA wieder.