IT-Sicherheitssysteme und Mitbestimmung des Betriebsrats

Katrin Haußmann

A. Der Mitbestimmungstatbestand: „technische Einrichtungen"

Die Einführung und Anwendung technischer Einrichtungen, die geeignet sind, Mitarbeiterverhalten oder -leistung zu kontrollieren, sind mitbestimmungspflichtig. Das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG ist darauf gerichtet,

> *„Arbeitnehmer vor Beeinträchtigungen ihres Persönlichkeitsrechts durch den Einsatz technischer Überwachungseinrichtungen zu bewahren, die nicht durch schutzwerte Belange des Arbeitgebers gerechtfertigt und unverhältnismäßig sind".*[1]

Regelungszweck dieses Mitbestimmungstatbestandes ist es, den Einsatz eines Systems mitzugestalten, so dass Arbeitnehmer nicht *„beliebig zum Objekt einer Überwachungstechnik gemacht"* werden können, die personen- oder leistungsbezogene Informationen verarbeitet.[2] Der Tatbestand wurde eingeführt, als es außer der klassischen Stechuhr und Überwachungskameras wenige technische Einrichtungen gab, die den Begriff erfüllten. Der Begriff der „Überwachung" wird weit ausgelegt und schon dann bejaht, wenn durch einen technische Vorgang Informationen über das Verhalten oder die Leistung von Arbeitnehmern erhoben und aufgezeichnet werden, um sie auch späterer Wahrnehmung zugänglich zu machen. Das Bundesarbeitsgericht dehnt in ständiger Rechtsprechung den Mitbestimmungstatbestand über die Grenzen des Wortlauts („*(…) zur Überwachung (…) bestimmt*") auf alle zur Kontrolle geeigneten Systeme aus.[3] Dazu zählt nahezu jede Software sowie deren spätere Änderung oder Aktualisierung.[4]

---

1 BAG NZA 2018, 673, 674 Rn. 15.
2 BAG NZA 2018, 673, 674 Rn. 15.
3 BAG NJW 1976, 261; zuletzt BAG NZA 2017, 657.
4 LAG Hamm BeckRS 2005, 31048701 Rn. 54 (Zit. ausgelassen): „Auch wenn die Software Windows 2000 lediglich die Vorgängerversion ersetzt hat, schließt dieser Neueinsatz das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG nicht aus. Das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG ist nämlich nicht nur bei der Einführung und erstmaligen Anwen-

IT-Sicherheitssysteme sind grundsätzlich geeignet, Mitarbeiterverhalten zu kontrollieren. Zeitgemäße Systeme vergleichen z.B. Aktivitäten eines Benutzerkontos mit dessen Normalverhalten, markieren Anomalien und bewerten Risiken, die sich daraus für die IT-Sicherheit ergeben können, ggf. zusammen mit anderen Risikofaktoren. Ist das Benutzerkonto einem Mitarbeiter eindeutig zugeordnet, liegen die Tatbestandsmerkmale des Mitbestimmungstatbestandes vor. Dem lässt sich zwar entgegenhalten, dass gerade die sicherheitsrelevanten Anomalien die konkrete Frage aufwerfen, ob ein Mitarbeiter selbst gerade den ihm zugeordneten Account nutzt, oder die Anomalie eher darauf hindeutet, dass ein anderer sich des individualisierten Zugangs bedient. Gleichwohl wird sich damit nicht begründen lassen, dass eine Verhaltensbeobachtung mit diesen Systemen nicht (auch) möglich wäre. Jedes System schreibt mindestens die sogenannten Log-Daten mit und erfasst damit das Nutzerverhalten. Im Regelfall lässt sich eine Nutzerkennung einer bestimmten Person zuordnen. Diese Daten können in sogenannten Security Information and Event Management-Systemen (kurz: „SIEM") ausgewertet und mit dem üblichen Nutzerverhalten eines Accounts verglichen werden. Soweit die Technik der User/Entity Behavior Analytics eingesetzt wird (kurz: „UEBA") wird der Normalwert, an dem das aktuelle Nutzerverhalten gemessen wird, individualisiert und variabilisiert.[5]

B. Reformvorschläge

Die derzeitige Auslegung des Mitbestimmungstatbestands zu technischen Systemen ist offensichtlich praxisfern. Sie wird den zeitlichen Abläufen von IT-Projekten nicht gerecht und berücksichtigt nicht die Geschwindigkeit, mit der generell Softwareanwendungen aktualisiert und speziell IT-Sicherheitssysteme dem Stand der Technik und der Sicherheitslage angepasst werden müssen. Es mehren sich die Vorschläge zu einer Reform des Mitbestimmungstatbestands.[6] Seit vielen Jahren wird vorgeschlagen, den Tatbestand auf seinen Wortlaut „*zur Überwachung (…) bestimmt*" zurückzu-

---

dung von EDV-Anlagen betroffen, sondern auch bei der Einführung eines neuen Programms oder bei der Änderung von vorhandenen Programmen."

5 Beispiel: Ein System dieser Art bieten Software-Anbieter wie Securonix oder SPLUNK an.

6 *Günther/Böglmüller*, NZA 2015, 1024, 1027; *Grimm*, ArbRB, 2015, 336, 339; *Ludwig/Rancke*, BB 2016, 2293; *Karthaus*, NZA 2017, 558, 561; *Wisskirchen/Schiller/Schwindling*, BB 2017, 2105.

führen.[7] Dann ließe sich bezogen auf IT-Sicherheitssysteme hervorheben, dass ihr primärer Zweck nicht die Mitarbeiterkontrolle selbst ist, sondern die IT-Sicherheit. Die Systeme kontrollieren als oberstes Suchkriterium typischerweise nicht namentlich identifizierte Mitarbeiter in ihrem Nutzerverhalten, sondern sie beobachten und bewerten sicherheitsrelevante Ereignisse („*incidents*" oder „*events*"). Bei der Aufklärung solcher Ereignisse ist u.U. die Einsicht in individualisierbare Nutzeraccounts erforderlich. Mit einer Rückführung des Mitbestimmungstatbestandes auf seinen Wortlaut ist derzeit nicht zu rechnen. Die Reduktion der Vorschrift auf den wesentlichen Regelungszweck ist dennoch dringend erforderlich. Da die Mitbestimmung kollektive Tatbestände erfassen soll, ist nicht einzusehen, warum schon die Möglichkeit der einzelfallbezogenen Einsichtnahme in personenbezogene Verhaltensdaten mit dem Betriebsrat geregelt werden sollte. Rechtfertigen lässt sich die Mitbestimmung bezogen auf solche technischen Systeme, die den Arbeitgeber in die Lage versetzen, automatisch Verhaltens- oder Leistungsdaten mehrerer Mitarbeiter vergleichend auszuwerten.[8] Außerdem könnte der Tatbestand mit dem Datenschutzrecht synchronisiert werden, indem an die Datenverarbeitung angeknüpft wird, und nicht an den Einsatz einer technischen Einrichtung. Weitere Reformvorschläge beziehen sich auf Verfahrensregelungen und schlagen Fristen für die Verhandlungen vor.[9] Erörtert wird auch die Einführung einer Erheblichkeitsschwelle.[10] Das Bundesarbeitsgericht lehnt eine – wie auch immer im Einzelnen verfasste – „Geringfügigkeitsschwelle" jedoch ab.[11] Nur vereinzelt hat das Bundesarbeitsgericht technische Systeme ausgenommen. Dies betraf zuletzt den Datenabgleich im Sanktionslistenscreening. In seiner Entscheidung vom 19. Dezember 2017[12] hat das Bundesarbeitsgericht den Abgleich von Terrorlisten und Mitarbeiterlisten mit Hilfe technischer Systeme von der Mitbestimmung ausgenommen. Die Begründung dazu lautet:

---

7 *Günther/Böglmüller*, NZA 2015, 1024, 1027; *Ludwig/Rancke*, BB 2016, 2293; *Wisskirchen/Schiller/Schwindling*, BB 2017, 2105.

8 *Haußmann/Thieme*, NZA 2019, 1612, 1618: Mitbestimmungspflichtig ist „[Nr. 6:] die automatisierte Verarbeitung personenbezogener Arbeitnehmerdaten zum Zwecke der vergleichenden Überwachung des Verhaltens oder der Leistung von Arbeitnehmern".

9 *Mengel*, NZA 2017, 1494, 1497 ff. für interne Untersuchungen.

10 *Kania,* in: Müller-Gloge et. al. (Hrsg.), ErfK zum Arbeitsrecht, 20. Aufl. 2020, § 87 BetrVG Rn. 57.

11 BAG BeckRS 2018, 27856.

12 BAG NZA 2018, 673.

> *„Die aufgrund des Datenabgleichs generierten Ergebnisse bilden weder ein konkretes Verhalten oder eine konkrete Leistung eines Arbeitnehmers ab, noch lassen sie auf solche schließen. Eine Identität dieser Statusdaten eines Arbeitnehmers, der auf einer „Terrorliste" geführten Person gibt Auskunft darüber, dass sich gegen diese eine Verbotsmaßnahme i.S.d. Bereitstellungsverbots richtet. Eine Aussage über ein tatsächliches betriebliches oder außerbetriebliches Verhalten des Arbeitnehmers, das einen Bezug zum Arbeitsverhältnis hat, ist damit nicht verbunden."*

Hier differenziert das Gericht also danach, ob tatsächlich Rückschlüsse auf das Verhalten eines Arbeitnehmers möglich sind. Auf andere Systeme bezogen ist diese Rechtsprechung übertragbar, wenn zwar mitarbeiterbezogene oder -beziehbare Daten verarbeitet werden, diese Daten aber keine Aussagen über das Verhalten oder die Leistung eines Mitarbeiters enthalten. Werden z.B. zur Korruptionsbekämpfung die letzten Ziffern der IBAN von Mitarbeiter-Lohnkonten einerseits und Bankkonten von Lieferanten oder Dienstleistern andererseits abgeglichen, ließe sich das Argument übertragen.

Allerdings ist in der arbeitsgerichtlichen Praxis und in Einigungsstellenverfahren zu beobachten, dass die Möglichkeit der Verhaltenskontrolle bejaht wird, soweit Nutzungs- oder Administratorenzugriffe von Mitarbeitern in Logdaten aufgezeichnet werden, die punktuell Informationen über Nutzerverhalten (wer hat wann lesend, schreibend oder ändernd auf Daten im System zugegriffen?) enthalten. Dann müsste sich aber jedenfalls die Betriebsvereinbarung nach § 87 Abs. 1 Ziff. 6 BetrVG auf diese konkrete Kontrollmöglichkeit beschränken. Solche eingeschränkten Vereinbarungen lassen sich in der Praxis gelegentlich durchsetzen, wenn nur technische Daten, z.B. zu den übertragenen Datenmengen durch E-Mail-Anhänge und dem Zeitpunkt der Übertragung ohne Nutzerkennung, aber keine mitarbeiterbezogenen Informationen verarbeitet werden. Dann sollte sich der Arbeitgeber jedoch mindestens das Recht zur Kontrolle der schreibenden und ändernden Zugriffe der Nutzer und Administratoren vorbehalten, um die Systemsicherheit zu gewährleisten und zugleich die Qualität der Datenverarbeitung zu sichern und z.B. eventuellen Rechenfehlern nachgehen zu können. Entsprechendes gilt für Test-Systeme und die Zugriffe der Tester, soweit noch keine Mitarbeiter-Daten, sondern nur „Dummys" verarbeitet werden. Auch hier muss der Arbeitgeber ggf. das Verhalten der Tester auswerten können, um Fehler nachverfolgen und das System weiterentwickeln zu können. Zugleich wäre die Speicherung von Logdaten in dem Umfang mitbestimmungsfrei, wie sie gesetzlich geboten ist.

C. Gesetzliche Vorgaben begrenzen die Mitbestimmung

Nur ausnahmsweise ist also eine technische Einrichtung, die Verhalten und Leistung von Arbeitnehmern erfasst, nicht dazu geeignet, diese auch zu „überwachen" im oben beschriebenen Sinne der Rechtsprechung zu § 87 Abs. 1 Ziff. 6 BetrVG. Der lesende Zugriff auf IT-Systeme dokumentiert, wann welcher Arbeitnehmer welche Informationen eingesehen hat. Dies gilt auch für IT-Administratoren von IT-Sicherheitssystemen. Soweit die regulatorischen Vorgaben des IT-Sicherheitsrechts und des Datenschutzrechts oder branchenspezifische Vorgaben im Bankaufsichtsrecht den Gestaltungsspielraum bei der Speicherung von Logdaten einengen, ist das Mitbestimmungsrecht des Betriebsrats ausgeschlossen, vgl. § 87 Abs. 1 Hs. 1 BetrVG. Dies gilt jedenfalls, soweit es keine für Arbeitnehmer weniger einschneidende, gleich wirksame Maßnahmen gibt und der Gestaltungsspielraum dadurch auf Null reduziert ist, weil es zu der Frage „ob" Administratorenzugriffe gespeichert werden, keine datenschutzrechtlich zulässige Alternative gibt. Dann bleibt nur zu prüfen, ob speziell bezogen auf das „Wie" der Verarbeitung gestaltende Entscheidungen noch verbleiben, auf die sich die Mitbestimmung beziehen könnte. Daher könnte zumindest das „Ob" der Speicherung von Zugriffsdaten der Administratoren von der Mitbestimmungspflicht ausgenommen sein, so dass die Mitbestimmung auf verbleibende gestaltbare Entscheidungen zum Einsatz und der Anwendung technischer Einrichtungen begrenzt wäre, in denen der Umfang der Speicherung und der Weiterverarbeitung von Zugriffsdaten gestaltet wird.

D. Entscheidungsspielraum für die Unternehmensleitung als Korridor für mitbestimmungspflichtige Entscheidungen

Einzelne Verarbeitungsvorgänge können vom Mitbestimmungsrecht ausgenommen sein (§ 87 Abs. 1 Hs. 1 BetrVG), wenn und soweit sie gesetzlich vorgegeben sind und dem Arbeitgeber kein eigener Gestaltungsspielraum zusteht.[13] Gesetz im Sinne dieser Bestimmung ist jedes zwingende förmliche oder materielle Gesetz und gesetzesvertretende Richterrecht, das den

13 *Richardi*, in: Richardi (Hrsg.), BetrVG, 16. Aufl. 2018, § 87 Rn. 148; *Kania*, in: Müller-Gloge et. al. (Hrsg.), ErfK zum Arbeitsrecht, 20. Aufl. 2020, § 87 Rn. 10.

Arbeitgeber bindet.[14] Ausreichend ist auch ein bindender Verwaltungsakt, der den Arbeitgeber zu bestimmten Maßnahmen verpflichtet.[15]

Verbleibt dem Arbeitgeber trotz gesetzlicher Regelung ein Gestaltungsspielraum, den er durch sein Direktionsrecht ausfüllen kann, darf der Betriebsrat im gleichen Umfang mitbestimmen:[16]

> *„Nach § 87 Abs. 1 Eingangshalbs. BetrVG hat der Betriebsrat u. a. nicht nach § 87 Abs. 1 BetrVG mitzubestimmen, soweit die betreffende Angelegenheit gesetzlich geregelt ist. Das beruht auf der Erwägung, dass für die Erreichung des Mitbestimmungszwecks kein Raum mehr verbleibt, wenn eine den Arbeitgeber bindende und abschließende gesetzliche Vorschrift vorliegt. Wird der Mitbestimmungsgegenstand durch diese inhaltlich und abschließend geregelt, fehlt es an einer Ausgestaltungsmöglichkeit durch die Betriebsparteien. Verbleibt dem Arbeitgeber dagegen trotz der bestehenden normativen Regelung ein Gestaltungsspielraum, ist ein darauf bezogenes Mitbestimmungsrecht des Betriebsrats eröffnet […].“*[17]

E. Einschätzungsprärogative des Arbeitgebers zu regulatorischen Vorgaben und technischen Details?

Während das Unternehmen als Arbeitgeber nebeneinander die Sicherheit informationstechnischer Systeme und den Arbeitnehmerdatenschutz gewährleisten muss, konzentriert sich das Engagement der Betriebsräte als Interessenvertreter in Verhandlungen über technische Einrichtungen auf den Arbeitnehmerdatenschutz und die Begrenzung der Mitarbeiterkontrolle. Dieses Ungleichgewicht prägt den Verlauf der Verhandlungen. Dadurch werden die Verhandlungen der Personalabteilung mit dem Betriebsrat zum Nadelöhr für die Umsetzung von IT-Sicherheitskonzepten. Für den erfolgreichen Abschluss der Verhandlungen kann daher ausschlaggebend sein, dass der Arbeitgeber den Betriebsrat schon in der Informationsphase gründlich darüber aufklärt, welche gesetzlichen und behördlichen Vorgaben zur IT-Sicherheit seinen eigenen Gestaltungsspielraum einschränken. Entsteht Streit über die Reichweite solcher Vorgaben, muss

14 *Richardi* (Fn. 13), § 87 Rn. 145 f., 148.
15 *Richardi* (Fn. 13), § 87 Rn. 149 m.w.N.
16 *Kania* (Fn. 13), § 87 Rn. 13; BAG NZA 2014, 1152 Rn. 14 zu Nr. 4 (Arbeitsentgelt); BAG NZA 2013, 913, 914 Rn. 19 zu Nr. 6 (Verhaltens- und Leistungskontrolle); BAG NZA 2002, 995 zu Nr. 7 (Arbeitsschutz).
17 BAG NZA 2014, 1151, 1152 Rn. 14.

den Fachabteilungen zu regulatorischen Vorgaben und zu der technischen Umsetzung und eventuellen Alternativlösungen, die dem Stand der Technik entsprächen, im Zweifel eine Einschätzungsprärogative zugestanden werden. Die Verantwortung des Unternehmens, sich so zu organisieren, dass Gesetze beachtet werden, liegt in der Aktiengesellschaft beim Vorstand, § 93 AktG.[18] Die Fachabteilungen tragen in der Organisation des Unternehmens die fachliche Verantwortung für die Einhaltung der gesetzlichen Vorgaben zur Datensicherheit und zur Vertraulichkeit, Verfügbarkeit und Integrität der Systeme und bewahren das Unternehmen vor behördlichen Sanktionen oder Schadensersatzansprüchen Dritter.

F. Verfahrensablauf in der Mitbestimmung

I. Innerbetriebliche Verhandlungen

Einigen sich Arbeitgeber und Betriebsrat auf den Einsatz eines Systems und den Umfang der Nutzung, ist für das Unternehmen damit nicht zuverlässig gesichert, dass es damit zugleich auch den regulatorischen Anforderungen an die Datensicherheit genügt. Der Betriebsrat gestaltet die Regeln zur Anwendung des Systems mit, er trägt aber nicht die Verantwortung im Interessenausgleich zwischen Arbeitnehmerdatenschutz einerseits und Datensicherheit, Integrität, Verfügbarkeit und Vertraulichkeit der Systeme andererseits. Wählt das Unternehmen hier den vorsichtigen Weg möglichst umfangreicher IT-Sicherheitssysteme, lässt sich eine Einigung mit dem Betriebsrat schwer erzielen. Dann kann im Einigungsstellenverfahren unter Umständen nur durch Spruch eine Regelung gefunden werden. Die Einigungsstelle hat dabei den Stand der Technik zu berücksichtigen, der durch Industriestandards (ISO 27000, 27001, 27002) und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (IT-Grundschutz) konkretisiert wird, vgl. § 8 BSiG, Art. 32 DSGVO.

II. Spruch der Einigungsstelle und dessen gerichtliche Überprüfung

Die Verhandlungen über die Mitbestimmung bei der Anwendung technischer Einrichtungen dauert nicht selten mehrere Monate: Zunächst tauschen sich die Betriebsparteien schriftlich über die Besetzung der Eini-

18 LG München I NZG 2014, 345.

gungsstelle aus. Im nächsten Schritt müssen gemeinsame Termine gefunden werden. Ein erster Termin dient meist dazu, dem Einigungsstellenvorsitzenden einen Überblick über den Gegenstand der Einigungsstelle zu verschaffen. Im zweiten Termin sind meist offene Fragen der Arbeitnehmervertreter zu den Funktionen der technischen Einrichtungen zu beantworten. In diesem und je nach Komplexität mindestens ein bis drei Anschlussterminen werden dann Regelungen zur Begrenzung der Leistungs- und Verhaltenskontrolle erörtert. Im Rahmen dieser Diskussion beantwortet der Arbeitgeber typischerweise auch Fragen des Betriebsrates dazu, ob der Einsatz des Systems den Arbeitnehmerdatenschutz wahrt. Dazu stehen dem Betriebsrat Informations- und Kontrollrechte gemäß § 80 BetrVG zu. Damit zwischen den Terminen Fragen beantwortet werden können und in Abhängigkeit von der Verfügbarkeit des Vorsitzenden und der Beisitzer liegen die Termine meist in einem Abstand von zwei bis sechs Wochen. Das passt nicht zu den zeitlichen Abläufen in typischen IT-Sicherheitsprojekten. Entscheidet die Einigungsstelle durch Spruch, ist der Spruch anfechtbar und kann in mindestens zwei Instanzen der Arbeitsgerichtsbarkeit auf Ermessens- und Rechtsfehler überprüft werden, § 2a Abs. 2, § 80 ArbGG, § 76 Abs. 5 BetrVG. Dieses Verfahren dauert über zwei Instanzen erfahrungsgemäß häufig 15 bis 18 Monate. Für die praktische Umsetzung der Sicherheitskonzepte bedeutsam ist, dass der Spruch betriebsverfassungsrechtlich bis zur rechtskräftigen Entscheidung über die Wirksamkeit des Einigungsstellenspruchs angewandt werden kann und der Betriebsrat, der einen Spruch zur Einführung und Anwendung eines technischen Systems anficht, nur ausnahmsweise im Wege des einstweiligen Rechtsschutzes die Anwendung stoppen kann.[19]

Mit der förmlichen Entscheidung der Einigungsstelle und der Zustellung des vom Vorsitzenden unterschriebenen Textes ist der Spruch der Einigungsstelle zunächst verbindlich, § 87 Abs. 2 S. 2 BetrVG. Es muss nicht im Nachgang noch eine von beiden Seiten unterschriebene Betriebsvereinbarung geschaffen werden. Der Spruch gilt als Betriebsvereinbarung, die unmittelbar gilt und umzusetzen ist, § 87 Abs. 2 S. 2 BetrVG. Das gilt zunächst einmal unabhängig davon, ob sie gerichtlich angegriffen wird. Diese betriebsverfassungsrechtliche und prozessuale Zwischenlösung schützt das Unternehmen allerdings nicht zuverlässig vor abweichenden eigenständigen Bewertungen der Datenschutzaufsichtsbehörde. Hält die Einigungsstelle ein System und die Art seiner Anwendung für datenschutzkonform und kann auf der Grundlage eines Spruchs der Einigungsstelle das

19 LAG Baden-Württemberg BeckRS 2016, 73644.

System zunächst betriebsverfassungsrechtskonform eingesetzt werden, ist damit jedenfalls theoretisch noch nicht beantwortet, ob die Datenschutzaufsicht später Datensicherheitsdefizite feststellen wird oder aber die arbeitnehmerdatenschutzrechtlichen Grenzen des Einsatzes anders bewertet. Dies wäre nur dann zuverlässig ausgeschlossen, wenn die Betriebsvereinbarung selbst zugleich als datenschutzrechtliche Rechtsgrundlage der Verarbeitung gestaltet wäre. In der Regel wird die Einigungsstelle aber nur prüfen, ob einer der datenschutzrechtlichen Erlaubnistatbestände (§ 26 BDSG oder Art. 6 DSGVO) die Verarbeitung der Arbeitnehmerdaten rechtfertigt, und dann durch Spruch über die Grenzen der Mitarbeiterkontrolle i. S. d. § 87 Abs. 1 Ziff. 6 BetrVG entscheiden.

Hat der Arbeitgeber durch Spruch der Einigungsstelle den Weg für den Einsatz eines IT-Sicherheitssystems gebahnt, bleibt dem Betriebsrat der Weg, den Einigungsstellenspruch im arbeitsgerichtlichen Beschlussverfahren anzufechten. Wenn er nicht nur Rechtsfehler, sondern auch Ermessensfehler geltend macht, muss die Anfechtung innerhalb von zwei Wochen nach Zuleitung des Beschlusses beim Arbeitsgericht eingereicht und begründet werden, § 76 Abs. 5 S. 4 BetrVG. Auch nach Ablauf der Zwei-Wochen-Frist bleibt der Rechtsweg offen für eine Anfechtung mit der Begründung, dass der Spruch gegen Rechtsvorschriften verstoße. Insbesondere die Behauptung des Betriebsrats, dass das Arbeitnehmer-Datenschutzrecht mit einem Spruch, der die Einführung eines technischen Systems unter bestimmten Bedingungen gestattet, nicht hinreichend beachtet würde, kann Gegenstand der Rechtskontrolle sein. Auch der Vorwurf, dass rechtliches Gehör nicht gewährt worden wäre, könnte nach Ablauf der Zwei-Wochen-Frist noch geltend gemacht werden, § 2a Abs. 2 ArbGG, § 80 ArbGG.

Die Arbeitsgerichtsbarkeit muss dann die Interessenabwägung zwischen Datensicherheit und Arbeitnehmerdatenschutz überprüfen und dabei ggf. auch fachgesetzliche Vorgaben anwenden. Sowohl die technischen Sachverhalte als auch die nicht-arbeitsrechtlichen Rechtsquellen sind dabei für Arbeitsrichter unter Umständen Neuland. Zu der Frage, ob ein System dem Stand der Technik entspricht und wie die IT-Sicherheitsrisiken branchen- und unternehmensspezifisch zu bewerten sind, können ggf. ergänzend zu den veröffentlichten ISO-Standards und Katalogen des BSI technische Gutachten einzuholen sein. Gutachten zur Auslegung deutscher Gesetze, insbesondere des § 25 KWG oder § 8a BSiG, lassen sich mit der Prozessordnung aber nur ausnahmsweise vereinbaren. Die Frage der Zulässigkeit der Einholung eines Rechtsgutachtens zu inländischen Rechtsfragen durch ein deutsches (Zivil-)Gericht wird nicht einheitlich beurteilt. Der BGH hielt in einer Entscheidung zum Steuerrecht die Einholung eines Rechtsgutachtens eines Steuerfachmanns für möglich, sofern das Gericht

dessen Meinung in vollem Umfang überprüft.[20] Bei außerordentlich speziellen oder entlegenen Rechtssätzen wird eine analoge Anwendung des § 293 ZPO in erwogen.[21] Die überwiegende Meinung im Schrifttum lehnt dagegen eine analoge Anwendung der Vorschrift bei außerordentlich „speziellen" oder „entlegenen" Rechtssätzen ab.[22] Bezogen auf den Strafprozess hat das OLG Celle festgestellt, dass Bestand und Auslegung des inländischen Rechts sowie seine Anwendung auf den Entscheidungsfall einer Beweiserhebung nicht zugänglich seien.[23]

III. Einstweiliger Rechtsschutz

Der Betriebsrat könnte während der gerichtlichen Auseinandersetzung über die Wirksamkeit des Einigungsstellenspruchs die Einführung eines IT-Sicherheitssystems nur aufhalten, wenn er beim Arbeitsgericht eine einstweilige Verfügung erwirken könnte, die sich gegen die Anwendung eines Einigungsstellenspruches während der gerichtlichen Auseinandersetzung über die Wirksamkeit des Einigungsstellenspruchs richtet. Eine solche einstweilige Verfügung könnte bei „besonders krassen und offensichtlichen Rechtsverstößen" erlassen werden.[24]

1. Verfügungsanspruch

Einigungsstellensprüche sind grundsätzlich unmittelbar umzusetzen. Anfechtungsverfahren, unabhängig davon, welche Seite den Angriff gegen den Spruch der Einigungsstelle betreibt, haben keinen Suspensiveffekt.[25] Dies gilt nicht nur in Fällen, in denen der Betriebsrat oder Gesamtbetriebsrat das Interesse an der Durchführung einer durch Spruch der Einigungs-

20 BGH NJW 1999, 638.
21 *Thole*, in: Stein/Jonas, Kommentar zur ZPO, 23. Aufl. 2013, § 293 Rn. 17.
22 Vgl. *Sanger*, in: Saenger (Hrsg.), Zivilprozessordnung, 8. Aufl. 2019, § 293 Rn. 6; *Prütting*, in: MüKoZPO, 6. Aufl. 2020, § 293 Rn. 22; so auch der hessische Staatsgerichtshof LKRZ 2012, 14 oder im Steuerrecht vgl. *Tipke* NJA 1976, 2200; *Nickl*, NJW 1989, 2093.
23 OLG Celle BeckRS 2015, 11588 Rn. 9 m.w.N.
24 So zusammenfassend zur Instanzrechtsprechung Fitting, BetrVG, 30. Aufl. 2020, § 76 Rn. 165, insbesondere LAG Köln NZA 2000, 334.
25 *Korinth*, Einstweiliger Rechtsschutz im Arbeitsgerichtsverfahren, 3. Aufl. 2015, Abschnitt K, Rz. 175 mit Verweis auf LAG Berlin v. 6.12.1984 – 4 TaBV 2/84; LAG Hessen v. 16.12.2004 – 4 Ta 165/04; LAG Köln v. 20.4.1999 – 13 Ta 243/98.

stelle zustande gekommenen Regelung hat, sondern auch dann, wenn die Durchführung des Einigungsstellenspruchs im Interesse des Arbeitgebers liegt oder vom Arbeitgeber sogar für zwingend erforderlich gehalten wird.[26] Einstweilige Verfügungen, die die Durchführung eines Einigungsstellenspruchs verhindern sollen, sind nur ausnahmsweise zulässig, wenn der Spruch der Einigungsstelle krasse Rechtsverstöße enthält und dies zudem offensichtlich ist.[27] Für diese restriktive Handhabung gibt es auch eine vollstreckungsrechtliche Begründung: Mit dem Streit über eine einstweilige Verfügung werden für die Dauer des Anfechtungsverfahrens durch die Instanzen die Risiken zwischen den Betriebsparteien verteilt. Diese Risikoverteilung findet im Urteilsverfahren einen Ausgleich durch den Schadensersatzanspruch des § 945 ZPO.[28] Eine Zwischenregelung durch einstweilige Verfügung, die sich nach einer Entscheidung in der Hauptsache als von Anfang an ungerechtfertigt erweist, verpflichtet im Urteilsverfahren den Gegner zum Schadensersatz (§ 945 ZPO). Dieser Schadensersatz steht dem Arbeitgeber im Beschlussverfahren nicht zur Verfügung, da die Vorschriften über das Beschlussverfahren nicht auch auf die Bestimmung verweisen, die einen Ausgleich für die gerichtliche Risikoverteilung schafft.[29] Erweist sich im Beschlussverfahren in der zweiten oder dritten Instanz eine vorläufige Regelung als von Anfang an ungerechtfertigt, hat allein der Arbeitgeber die Risiken daraus zu tragen.[30] Er hat keinen Schadensersatzanspruch gegen den Betriebsrat nach § 945 ZPO und auch keine anderen Regressansprüche gegen handelnde Personen.[31]

Bezogen auf den Einsatz notwendiger IT-Sicherheitssysteme wären die Folgen einer Unterlassungsverfügung bis zum rechtskräftigen Abschluss des Streits um die Wirksamkeit des Einigungsstellenspruchs nicht hinnehmbar. Der Arbeitgeber wäre nicht nur unternehmerischen Risiken ausgesetzt, sondern auch dem aufsichtsbehördlichen Vorwurf, seine Aufgaben in der Gefahrenabwehr nicht beachtet zu haben und damit dem Risiko, dass Sanktionen gegen ihn verhängt werden:

Je länger sich die Einführung eines IT-Sicherheitssystems verzögert, desto größer wäre die Wahrscheinlichkeit, dass bestehende Sicherheitslücken tatsächlich für einen Cyberangriff genutzt würden. Dies würde für das Unternehmen ein unternehmerisches Risiko darstellen. Vertrauliche Informa-

26 LAG Köln NZA 2000, 334.
27 LAG Köln NZA 2000, 334.
28 BGH NJW 1996, 198; *Drescher*, in: MüKoZPO, 6. Aufl. 2020, § 945 Rn. 2.
29 LAG Baden-Württemberg NZA 1990, 286; *Olderog* NZA 1985, 753, 756.
30 LAG Baden-Württemberg NZA 1990, 286.
31 LAG Baden-Württemberg NZA 1990, 286.

tionen könnten an Wettbewerber gelangen, Kundendaten könnten gestohlen werden oder Arbeitsabläufe gefährdet werden. Zudem wäre damit die Reputation des Unternehmens beschädigt, wenn Sicherheitslücken öffentlich bekannt werden.[32] Darüber hinaus hätte das Unternehmen oder dessen Organe[33] auch (behördliche) Sanktionen zu befürchten: In einer Aktiengesellschaft haben die Vorstandsmitglieder gemäß § 93 Abs. 1 AktG bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Zu den Pflichten des Gesamtvorstands gehört die Einrichtung eines funktionierenden Compliance-Systems.[34] Ein gesetzeskonformes System der IT-Sicherheit ist ein notwendiger Bestandteil davon. Ungenügende organisatorische Vorkehrungen stellen eine Pflichtverletzung dar und können zur Schadensersatzpflicht gegenüber der Gesellschaft führen.[35] Eine Schadensersatzpflicht kann den Vorstand darüber hinaus auch dann treffen, wenn er es gemäß § 91 Abs. 2 AktG unterlässt, geeignete Maßnahmen zu treffen, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Die Früherkennung eines Cyber-Angriffs lässt sich unter diesen Begriff fassen.[36]

Jedenfalls seit der Anwendbarkeit der DSGVO können auch Datenschutzverstöße zu bestandsgefährdenden Bußgeldern führen. Bußgelder sind in der DSGVO in Art. 83 vorgesehen. Nach dessen Absatz 4 können Geldbußen von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden. Auch der Verstoß gegen Art. 32 DSGVO ist gem. Art. 83 Abs. 4 lit. a bußgeldbewehrt. Die Norm gibt technische und organisatorische Maßnahmen vor, die im Unternehmen ergriffen werden müssen, um ein angemessenes Schutzniveau in Bezug auf die Datensicherheit zu erzielen. Genügt ein bisher verwendetes IT-System diesen Anforderungen nicht und verzögert sich die Einführung des neuen datenschutzkonformen IT-Sicherheitssystems, kann es zur Verhängung eines Bußgeldes kommen.

---

32 Vgl. die Berichtserstattung zum Cyber-Angriff auf die Funke-Mediengruppe im Dezember 2020 (etwa *Finanznachrichten.de* vom 4.1.2021, „Cyberangriff auf Funke-Mediengruppe hält weiter an“) oder die Berichterstattung zum Cyber-Angriff auf die British Airways 2018 (etwa *Der Tagesspiegel* vom 7.9.2018, „Hacker erbeuten 380.000 Kundendaten bei British Airways“) zu nennen.

33 Dazu unter Ziffer V.

34 *Bicker*, AG 2012, 542; *Fleischer*, in: BeckOGK, 15.1.2020, AktG, § 91 Rn. 47 ff.

35 LG München I NZG 2014, 345.

36 *Behling*, ZIP 2017, 697, 698.

Betreiber Kritischer Infrastrukturen (vgl. zur Legaldefinition § 1 Abs. 10 BSIG), wie etwa Banken, trifft darüber hinaus auch die Verpflichtung aus § 8a BSIG, angemessene, organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Kommen sie dieser Verpflichtung nicht nach, etwa durch Implementierung eines den Anforderungen genügenden IT-Sicherheitssystems, rechtfertigt auch dies die Verhängung eines Bußgeldes gem. § 14 BSIG.

2. *Anforderungen an den Verfügungsgrund*

Da die Durchführung des Einigungsstellenspruchs während eines Anfechtungsverfahrens der Regelfall ist und nur höchst ausnahmsweise ein Verfügungsanspruch überhaupt in Betracht kommt, sind besonders hohe Anforderungen an den Verfügungsgrund zu stellen. Eine nicht rechtskräftige Entscheidung des Arbeitsgerichts ist kein Verfügungsgrund; sie kann mit ihrer Begründung aber in die Bewertung des Verfügungsanspruchs einbezogen werden. Der Antragsteller muss für den Verfügungsgrund vielmehr darlegen, dass ihm bei – auch bloß zeitweiliger – Durchführung des Einigungsstellenspruchs Nachteile drohen, gegenüber denen die Interessen des Antragsgegners zweifelsfrei zurückzutreten haben.[37] Der Einsatz eines Systems der IT-Sicherheit müsste also in der Verarbeitung von Mitarbeiterdaten offensichtlich eine nicht mehr reversible Verletzung deren Persönlichkeitsrechts begründen. Diese Voraussetzungen liegen im Zweifel nicht vor. Wäre der Eingriff durch Verarbeitung von Verhaltensdaten über die Nutzeraktivitäten zu intensiv, könnten die Daten gelöscht werden. Der Eingriff wäre nicht irreversibel.

3. *Keine Ausnahme von den Anforderungen an Verfügungsanspruch und -grund*

Für den besonderen Fall von Überstunden von Verkäuferinnen in einem Kaufhaus hatte das LAG Hamburg im Jahr 2000[38] ausnahmsweise eine einstweilige Verfügung erlassen, die dem Arbeitgeber die Durchführung

37 LAG Baden-Württemberg NZA 1990, 286.
38 3 TaBV 6/00 mit Anm. *Bertelsmann*, AIB 2001, 51.

eines Einigungsstellenspruchs untersagen sollte, der die Überstunden gestattete. Dies wurde ausdrücklich auf die einzelfallbezogene Begründung gestützt, dass ohne den einstweiligen Rechtsschutz die Hauptsache in der Sache vollständig erledigt wäre. Diese Überlegung ist hier nicht übertragbar, da eine vorläufige Durchführung des Einigungsstellenspruchs zum Einsatz und zur Anwendung eines IT-Sicherheitssystems die Hauptsache nicht erledigt. Das System wird in der Regel über Monate und Jahre eingesetzt. Die Entscheidung in der Hauptsache könnte die Rahmenbedingungen für den Einsatz bestimmen für den Zeitraum nach Abschluss des Verfahrens im einstweiligen Rechtsschutz.

G. Fazit

Mitbestimmungsrechte des Betriebsrates bei der Einführung von IT-Sicherheitssystemen sollten im Projektplan für die Einführung technischer Systeme von Anfang an eingeplant werden. Andernfalls kann es zu erheblichen Verzögerungen kommen, bis durch Abschluss einer Betriebsvereinbarung oder Spruch der Einigungsstelle der Einsatz des Systems betriebsverfassungsrechtlich legitimiert ist. Gelingt eine Einigung nicht und muss das Einigungsstellenverfahren durch Spruch beendet werden, können sich aus Folgestreitigkeiten über die Wirksamkeit des Einigungsstellenspruchs im Beschlussverfahren durch zwei oder drei Instanzen über längere Zeiträume Rechtsunsicherheiten ergeben.