ARBEITSRECHTLICHE RISIKOABSCHÄTZUNG

PROJEKT ITS.APT DELIVERABLE 2.1

Autoren:

für die Westfälische Wilhelms-Universität Münster, Institut für Informations- Telekommunikations- und Medienrecht:

Tim Hey
Robert Ortner

für das Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein:

Meiko Jensen
Hannah Obersteller

Inhalt

A. Einleitung

I. zum Projekt

IT-Infrastrukturen werden immer häufiger das Ziel von Cyberattacken, mit teils großen wirtschaftlichen und ideellen Schäden. Möglich sind in etwa Beeinträchtigungen des Betriebs der betroffenen Institution, sowie Datenverluste, die die Reputation beeinträchtigen oder gar Haftungsfälle generieren. Denkbar ist außerdem der Verlust von personenbezogenen Informationen und Betriebsgeheimnissen. Besonders gravierend sind die Folgen eines solchen Angriffs dann, wenn kritische Infrastrukturen, wie Krankenhäuser, Versorgungs- oder Verkehrseinrichtungen betroffen sind, da diese eine besonders wichtige Bedeutung für das staatliche Gemeinwesen haben.[1]

Zur Bewertung der IT-Sicherheit in Unternehmen werden in die Regel sog. penetration tests durchgeführt. IT-Sicherheitsdienstleister versuchen dabei in das IT System einzudringen, um Sicherheitsschwachstellen oder Lücken zu ermitteln, die dann geschlossen werden können. Die Überprüfung der Verwundbarkeit von IT-Infrastrukturen ist dabei jedoch auf Aspekte der technischen Sicherheit limitiert. Außen vor bleiben Risiken, die auf Seiten der Nutzer des Systems entstehen, indem sie bspw. unangemessen auf Sicherheitshinweise reagieren

Dieses Defizit ist der Ausgangspunkt eines neuen vom BMBF geförderten Forschungsprojekts namens ITS.APT, das es sich zum Ziel gesetzt hat, das IT Sicherheitsbewusstsein der Nutzer eines IT Systems zu messen und Wege zu finden, es zu verbessern. Dazu wird eine Software entwickelt, die IT Attacken auf das Computersystem, wie Phishing Mails oder sog. SQL-Injections, simuliert. Der Nutzer nimmt diese in Form von angezeigten Artefakten, also fremd anmutenden Anzeigen auf dem Bildschirm, wahr. Die Reaktionen der Nutzer auf die IT Angriffe werden, ebenfalls mittels der Software, protokolliert und können schließlich Erkenntnisse über deren IT Sicherheitsbewusstsein liefern. Beispielsweise spricht das direkte Löschen einer Phishing E-Mail eher für ein erhöhtes Sicherheitsbewusstsein, während das Anklicken eines Links in der Phishing E-Mail eher für das Gegenteil spricht.

In einem groß angelegten Feldtest am Universitätsklinikum Schleswig-Holstein (UKSH) sollen die Arbeitnehmer des Klinikums als Nutzer der dortigen IT Systeme getestet werden.

[1] vgl. dazu auch § 2 Abs. 10 BSIG.

Der Test findet dabei heimlich und unter normalen Arbeitsbedingungen statt, um möglichst authentische Ergebnisse zu gewährleisten. Im Anschluss an diesen ersten Test sollen die Nutzer gezielt, aber unterschiedlich auf das Bemerken von IT Angriffen geschult werden. Anschließend wird die gleiche Testgruppe wiederum durch simulierte IT Angriffe getestet, um zu evaluieren, welche Schulungsmaßnahme am effektivsten ist und das IT Sicherheitsbewusstsein am besten steigert.

II. zum Dokument

Da die Tests in einem Betrieb, in diesem Fall dem UKSH, stattfinden und Arbeitnehmer getestet werden, muss das Vorhaben arbeitsrechtlich eingeordnet und bewertet werden. Das ist das Ziel dieses Gutachtens. Dazu sollen die einschlägigen arbeitsrechtlichen Bestimmungen herausgearbeitet und auf das Projektszenario angewendet werden. Darauf aufbauend werden eigene Vorgaben aufgestellt, die bei der Durchführung der verschiedenen Projektphasen aus rechtlicher Sicht zu beachten sind.

Dafür wird im folgenden zweiten Kapitel ein kurzer Überblick über die im Projekt vorgesehen Angriffsszenarien und die hierbei erhobenen Daten gegeben. Dies dient als Grundlage für die weitere rechtliche Beurteilung.

Darauf aufbauend wird im dritten Kapitel das generelle Spannungsverhältnis zwischen Arbeitgeber und Arbeitnehmer behandelt. Es wird erläutert, welche jeweiligen Interessen bestehen und wie sie rechtlich geschützt sind. Außerdem wird darauf eingegangen, wie das Recht, allgemein betrachtet, die sich häufig widerstreitenden Interessen im Arbeitsverhältnis in Einklang bringt und auf diese Weise arbeitsrechtliche Interessenkonflikte löst.

Daran anschließend wird im vierten Kapitel untersucht, wie der Arbeitnehmer datenschutzrechtlich geschützt ist. Dabei wird insbesondere der Frage nachgegangen, nach welcher Erlaubnisnorm sich die Datenerhebung in den Tests richtet und auf welcher Rechtsgrundlage die Übermittlung an, sowie Nutzung der erhobenen Daten durch ITS.APT erfolgen kann.

Das folgende fünfte Kapitel befasst sich mit den Bestimmungen des kollektiven Arbeitsrechts. Dort soll erörtert werden, ob und wie Arbeitnehmervertretungen in den verschiedenen Testphasen zu beteiligen sind. Da für die getesteten Arbeitnehmer sowohl Betriebs- als auch Personalräte zuständig sind, wird sowohl auf die Vorgaben des Betriebsverfassungsgesetzes (BetrVG) als auch auf die des Gesetzes über die Mitbestimmung der Personalräte des Landes Schleswig-Holstein (MBG S-H) eingegangen.

Im sechsten Kapitel werden die Auswirkungen der Tests auf das Persönlichkeitsrecht der Arbeitnehmer analysiert und rechtlich beurteilt. Dazu wird die Testsituation mit der Überwachung des betrieblichen Telefon- und E-Mailverkehrs, sowie mit Testkäufen verglichen. Die dort herausgearbeiteten Grundsätze bezüglich der Überwachung von Arbeitnehmern werden auf die Testsituation übertragen, um so konkrete Vorgaben zu entwickeln, wie das Persönlichkeitsrecht der Arbeitnehmer ausreichend beachtet werden kann.

B. Beschreibung der Angriffsszenarien

Im Rahmen des Projektes ITS.APT sollen verschiedene „Angriffe“ auf das Universitätsklinikum Schleswig-Holstein (UKSH) durchgeführt werden: Das Versenden von „Phishing-Mails“ an Dienst-E-Mail-Adressen von Angestellten des UKSH, sowie das Einbringen von weiteren „Artefakten“ in das IT-System, die Arbeitnehmern auffallen und als Hinweise auf mögliche Angriffe auf die IT gedeutet werden sollten.

Bei den Phishing-Angriffen soll „klassisches Phishing“[2] simuliert werden. Der Begriff „phishing“ leitet sich von der Intention des Angreifers ab: „Password fishing“ (dt.: Passwort angeln).[3] Der Angreifer versendet eine E-Mail an die E-Mail-Adresse des Opfers. Die E-Mail scheint von einem dem Opfer bekannten Kontakt zu kommen; im Fall von ITS.APT können dies Geschäftspartner oder Kollegen (andere Mitarbeiter des UKSH) sein, etwa aus der UKSH-eigenen IT-Support-Abteilung. In der E-Mail wird das Opfer – unter Angabe von Gründen – aufgefordert, auf einen mitübersandten Link zu klicken. Kommt das Opfer dieser Aufforderung nach, wird es über den Link zu einer durch den Angreifer gestalteten Website geleitet. Dort wird es aufgefordert, Nutzername und Passwort einzugeben. Tut es dies, werden dem Angreifer so die Zugangsdaten des Opfers zu diesem Webportal bekannt. Die Website ist in der Regel so gestaltet, dass sie den Eindruck eines normalen – „echten“ – Webauftritts (z.B. des realen Geschäftspartners) vermittelt. Verfügt der reale Geschäftspartner über ein eigenes Nutzerportal, kann die Website des Angreifers diesem originalgetreu nachempfunden sein, sodass dem Opfer nicht unmittelbar auffällt, dass es sich nicht um die „echte“ Website handelt.[4] Typischerweise versuchen Angreifer auf diese Weise Online-Banking-Zugangsdaten (sowie TANs) von Bankkunden zu „phishen“, um sodann Transaktionen vom Bankkonto des Opfers auf andere Konten vornehmen zu können. Auch Kundendaten von Versandhändlern

[2] *Borges*, NJW 2005, 3313 (3313).
[3] Wabnitz/Janovsky, Kap. 14, Rn. 32.
[4] Vgl. *Popp*, MMR 2006, 84 (84).

werden auf diese Weise häufig in Erfahrung gebracht, um sodann – auf Rechnung des tatsächlichen Kunden – Waren zu bestellen und weiter zu veräußern.[5]

Im Rahmen von ITS.APT werden Phishing-Mails verschiedener Inhalte an die dienstlichen E-Mail-Adressen der Arbeitnehmer versandt. Der Testaufbau ermöglicht sodann eine Protokollierung der Reaktion des Arbeitnehmers, wie z.B. ein unmittelbares Löschen der E-Mail aus dem eigenen Postfach oder aber auch das Öffnen der E-Mail und Anklicken eines eventuell enthaltenen Links.

Ein weiteres Angriffsszenario ist die Einspeisung von Artefakten auf den Bildschirm von PC-Arbeitsplätzen. Hierbei kann es sich z.B. um das unvermittelte Einblenden einer Videosequenz, Fehler in der Darstellung von Webseiten oder plötzliches lautes Aufbrausen eines Gehäuselüfters handeln. Anormalitäten dieser Art können typischerweise auftreten, wenn Angriffe auf die IT – d.h. unberechtigte Zugriffe auf oder Manipulationen an der IT – vorgenommen werden. Auch hier sollen die Reaktionen der Arbeitnehmer getestet werden.

Im Ergebnis ermöglicht die Testdurchführung, bzw. das Programm, die Reaktion der Arbeitnehmer auf bestimmte dienstlich erhaltene E-Mails zu überprüfen. D.h., es wird das Verhalten der Arbeitnehmer bei der Arbeit kontrolliert: Die Mitarbeiter sind dabei wenigstens über ihre Kennung/E-Mail-Adressen identifizierbar. Das in das IT-System des UKSH eingespielte Programm protokolliert die Verkehrsdaten, die der Mitarbeiter durch seine Reaktion am PC erzeugt. Zudem ist der technische Support-Dienst – als den Mitarbeitern bekannte Kontaktstelle bei Problemen mit der hausinternen IT – über die Testdurchführung informiert und wird ankommende Kontaktaufnahmen und Fragen der Arbeitnehmer manuell protokollieren. Begrifflich werden damit Verkehrs- bzw. Verbindungsdaten erhoben und weiterverarbeitet. Konkret wird es sich dabei nach bislang vorliegenden Informationen um folgende Datengruppen handeln: Kennung/E-Mail des Mitarbeiters (soweit er eingeloggt ist); Kennung des Arbeitsplatzes von dem aus die protokollierten Handlungen vorgenommen werden; Beginn, Art und ggfs. Ende der ausgelösten Benutzeraktivität, sowie Art der Benutzerreaktion.

Inhaltsdaten – d.h. z.B. das Telefongespräch zwischen dem Arbeitnehmer und dem Support-Mitarbeiter – werden nicht aufgezeichnet. Ebenso wenig wird auf das E-Mail-Postfach der Arbeitnehmer zugegriffen. Auch soweit ein Arbeitnehmer dem Support eine E-Mail schreibt, werden lediglich die Verkehrsdaten dieses Vorgangs geloggt.

[5] *Borges*, NJW 2005, 3313 (3313).

Diese Erhebung und Weiterverarbeitung personenbezogener Daten darf nur unter Beachtung des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen (LDSG S-H), sowie der einschlägigen arbeitsrechtlichen Normen erfolgen.[6]

C. Arbeitsrechtliche Herausforderungen

Um die dargestellten Tests umfassend rechtlich beurteilen zu können, wird im Folgenden das Spannungsverhältnis zwischen Arbeitnehmer und Arbeitgeber allgemein dargestellt, bevor in den späteren Kapiteln auf einzelne arbeitsrechtliche Fragen eingegangen wird. Allgemein stellt sich nämlich in dem Projekt die Frage, wie die widerstreitenden Interessen des UKSH als Arbeitgeber und die des Arbeitnehmers in Einklang zu bringen sind.

Das UKSH verfolgt mit dem Projekt das Ziel, seine informationstechnischen Systeme noch besser zu schützen. Mit Hilfe der geplanten Tests sollen zu diesem Zweck möglichst viele Informationen über das Verhalten der Arbeitnehmer gesammelt werden, die Rückschlüsse auf ihr IT Sicherheitsbewusstsein ermöglichen. Der Arbeitnehmer hat hingegen ein Interesse daran, dass seine Persönlichkeit bei den Tests umfassend beachtet wird, insbesondere dass möglichst wenige Informationen über ihn und erst Recht keine mit privatem Bezug erfasst werden.

Das Interesse eines Jeden, autonom über seine Lebensgestaltung zu bestimmen und unerwünschte Eingriffe darein zu unterbinden, wird durch das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG geschützt.[7] Daneben gibt es zahlreiche spezialgesetzliche Regelungen, die diesen Schutz vervollständigen, etwa die Bundes- und Landesdatenschutzgesetz (BDSG bzw. in diesem Fall LDSG S-H) oder bestimmte Vorgaben des BetrVG. Auf europäischer Ebene ist das

[6] Siehe hierzu sogleich unter D.II S. 13 ff.

[7] Das allgemeine Persönlichkeitsrecht umfasst verschiedenste Aspekte der privaten Lebensführung und schützt die Privat-, Geheim- und Intimsphäre (vgl. etwa *BVerfG*, Beschl. v. 16.7.1969 - 1 BvL 19/63, BVerfGE 27, 1 (6) - Mikrozensus; Beschl. v. 15.1.1970 - 1 BvR 13/68, BVerfGE 27, 344 (350 f.) - Scheidungsakten; Beschl. v. 8.3.1972 - 2 BvR 28/71, BVerfGE 32, 373 (379) - Arztkartei; Beschl. v. 21.12.1977 - 1 BvL 1/75, 1 BvR 147/75, BVerfGE 47, 46 (73) - Sexualkundeunterricht; Beschl. v. 11.10.1978 - 1 BvR 16/72, BVerfGE 49, 286 (298) - Transsexuelle), das Verfügungsrecht über die Darstellung der eigenen Person (Beschl. v. 5.6.1973 - 1 BvR 536/72, BVerfGE 35, 202 (220) - Lebach), das Recht am gesprochenen Wort (Beschl. v. 31.1.1973 - 2 BvR 454/71, BVerfGE 34, 238 (246) - heimliche Tonbandaufnahme), unter bestimmten Umständen das Recht, von der Unterschiebung nicht getaner Äußerungen verschont zu bleiben (vgl. Beschl. v. 14.2.1973 - 1 BvR 112/65, BVerfGE 34, 269 (282 f.) - Soraya), das Recht auf schuldenfreien Übertritt in die Volljährigkeit (Beschl. v. 13.5.1986 - 1 BvR 1542/84, BVerfGE 72, 155 - elterliche Vertretungsmacht), das Recht die eigene Abstammung zu erfahren (Beschl. v. 31.1.1989 - 1 BvL 17/87, BVerfGE 79, 256 - Kenntnis der eigenen Abstammung), das Recht auf informationelle Selbstbestimmung (Urt. v. 15.12.1983 - 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 - Volkszählung) und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Urt. .v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 - Online-Durchsuchung).

Persönlichkeitsrecht durch Art. 7 und 8 der Europäischen Grundrechtecharta (GrCha), Art. 8 der Europäischen Menschenrechtskonvention (EMRK), sowie sekundärrechtlich geschützt.

Im Zusammenhang mit dem Projektszenario sind vor allem die Auswirkungen relevant, die durch eine Überwachung des Arbeitgebers entstehen. Dabei ist sowohl im deutschen, als auch im europäischen Rechtsraum anerkannt, dass sich der Schutz des Allgemeinen Persönlichkeitsrechts auch auf das Arbeitsverhältnis erstreckt.[8] Aufgrund von Bekanntschaften oder Austausch zwischen Personen während der Arbeit, ist es untrennbar mit dem Privatleben verbunden. Außerdem kann eine Person derart in ihrer Arbeit aufgehen, dass sie zum Mittelpunkt ihrer Lebensführung wird.[9] Dementsprechend hat bspw. das Bundesverfassungsgericht das gesprochene Wort eines Arbeitnehmers als besondere Ausprägung seines Allgemeinen Persönlichkeitsrechts als besonders schützenswert angesehen.[10] Ebenso hat der Europäische Gerichtshof für Menschenrechte festgestellt, dass der Arbeitgeber nicht ohne Weiteres die E-Mail Korrespondenz seines Arbeitnehmers überwachen darf.[11]

Der Schutz des Arbeitnehmers ist allerdings nicht grenzenlos. Vielmehr können berechtigte Interessen Dritter zu Einschränkungen führen, im Projektszenario also die oben genannten Interessen des Arbeitgebers. Diese sind rechtlich durch seine Berufsfreiheit aus Art. 12 GG und sein Eigentumsrecht aus Art. 14 GG geschützt. Auf europäischer Ebene wird dieser Schutz durch Art. 15 und 16 GrCha, sowie Art 1 des ersten Zusatzprotokolls zur EMRK gewährleistet.

Aus rechtlicher Perspektive betrachtet, stehen sich daher im Projekt das Allgemeine Persönlichkeitsrecht des Arbeitnehmers und die Berufs- bzw. Eigentumsfreiheit des Arbeitgebers gegenüber. Da keines dieser Rechte abstrakt vorrangig ist, müssen beide so in Einklang miteinander gebracht werden, dass jedem Recht ein größtmöglicher Anwendungsspielraum zukommt.[12] Diese Zielvorgabe wird auch als praktische Konkordanz bezeichnet.[13] Dazu müssen die hinter dem Recht stehenden Interessen angemessen

[8] Für Deutschland: *BVerfG*, Beschl. v. 19.12.1991 - 1 BvR 382/85; *BAG*, Beschl. v. 27.05.1986 - 1 ABR 48/84; für Europa: *EGMR*, Urt. v. 12.1.2016 - 61496/08 (Bărbulescu/Rumänien); Urt. v. 5.10.2010 - 420/07 (Köpke/Deutschland); Urt. v. 3.4.2007 - 62617/00 (Copland/GB); Urt. v. 25.6.1997 - 20605/92 (Halford/GB); Urt. v. 16.12.1992 – 13710/88 (Niemitz/Deutschland); Urt. .v. 2.8.1984 - 8691/79 (Malone/GB).

[9] *EGMR*, Urt. v. 16.12.1992 - 13710/88 (Niemitz/Deutschland), Rn. 29.

[10] *BVerfG*, Beschl. v. 31.1.1973 - 2 BvR 454/71, BVerfGE 34, 238 - heimliche Tonbandaufnahme.

[11] *EGMR*, Urt. v. 3.4.2007 - 62617/00 (Copland/GB).

[12] Grundlegend *BVerfG*, Urt. v. 15.1.1958 - 1 BvR 400/51, BVerfGE 7, 198 - Lüth.

[13] So der auf *Hesse* zurückgehende Begriff: *Hesse*, § 72, Rn. 318.

berücksichtigt und bewertet werden. Dieser Prozess soll Gegenstand der folgenden Ausführungen sein.

D. Arbeitnehmerdatenschutz

I. Grundlegendes zum Arbeitnehmerdatenschutz

Im Rahmen des Projektes ITS.APT werden personenbezogene Daten der Mitarbeiter des UKSH verarbeitet. Entsprechend der Beschreibung der Angriffsszenarien wird die Reaktion der Mitarbeiter auf durch ITS.APT versandte Phishing-E-Mails, sowie weitere Artefakte untersucht. Es findet zwar keine Kontrolle der E-Mail-Postfächer der Mitarbeiter statt in dem Sinne, dass Einsicht in Absender und Adressaten der im Postfach gespeicherten E-Mails oder gar in E-Mail-Inhalte genommen wird. Aber eine Kontrolle des Verhaltens der Mitarbeiter in Bezug auf Telekommunikationsvorgänge wird insofern ermöglicht, als ihre Reaktion auf von ITS.APT erstellte Artefakte gespeichert und für den dem UKSH zugehörigen Testleiter sichtbar gemacht wird. Es werden Verkehrsdaten automatisiert erhoben und gespeichert.[14]

Die Tests finden am UKSH statt. Alle Probanden befinden sich in einem Beschäftigungsverhältnis mit dem UKSH. Datenschutz im Arbeitsverhältnis ist aus mehreren Gründen als besonders problematisch zu betrachten. In erster Linie liegt das an der Annahme einer „strukturellen Unterlegenheit“ des Arbeitnehmers gegenüber seinem Vertragspartner[15] begründet, die es dem Arbeitnehmer erschwert, ein angemessenes Datenschutzniveau gegenüber dem Arbeitgeber mit privatrechtlichen Mitteln sicherzustellen. Zudem hat der Arbeitgeber auch in einem gewissen Umfang ein berechtigtes Interesse, Daten seiner Arbeitnehmer zu erheben, um deren Arbeitsleistung zu kontrollieren. Auch wenn er mit solchen Verhaltenskontrollen in das Recht auf informationelle Selbstbestimmung seiner Arbeitnehmer eingreift, kann dieser Eingriff gerechtfertigt sein.

Hinsichtlich der durch den Arbeitgeber erhobenen Daten ist zu unterscheiden: Zunächst muss der Arbeitgeber selbstverständlich einige Daten seiner Arbeitnehmer erheben und auch übermitteln; dies betrifft insbesondere den Bereich der Personaldaten, die zu Abrechnungs-, sowie Verwaltungszwecken (bspw. Anmeldung bei der Sozialversicherung) benötigt werden. Ebenso müssen im Laufe des Beschäftigungsverhältnisses z.B. genaue Angaben zu Höhe von Lohn oder Gehalt gemeldet werden, um dem Finanzamt die Ermittlung der genauen Höhe der fälligen Lohnsteuer zu ermöglichen.

[14] Vgl. insoweit bereits unter B S. 7.
[15] Simitis/*Seifert*, BDSG, § 32 Rn. 5.

Daneben fallen aber – je nach Art der Beschäftigung – auch weitere personenbezogene Daten der Arbeitnehmer beim Arbeitgeber an. Im Falle computergestützter Arbeitsplätze mit Internetzugang wird i.d.R. protokolliert, welche Websites durch die Arbeitnehmer besucht wurden. Im Falle eines Kurierdienstes mit sog. live-tracking-Funktion kann dank des im Fahrzeug installierten GPS-Senders nicht nur der Kunde den Weg seiner Lieferung verfolgen, sondern auch der Arbeitgeber den genauen Weg – inklusive Pausen – seines Fahrers. Diese Fälle sind aufmerksam zu betrachten und zu bewerten, um sicher zu stellen, dass nur zu bestimmten vorab definierten Zwecken von einzelnen Daten Gebrauch gemacht wird und z.B. in größeren Unternehmen auch klare Zugriffsberechtigungen bestehen.[16]

Bei computergestützten Arbeitsplätzen fallen v.a. „Verkehrsdaten" an. „Verkehrsdaten" sind gem. § 3 Nr. 30 TKG solche, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Erfasst sind mithin alle Daten einer Kommunikation, die keine Inhaltsdaten sind. Die Telekommunikations-, bzw. Verkehrsdaten der Arbeitnehmer sind personenbezogene Daten, die der Arbeitgeber durch Speicherung und Zugriff erhebt und verarbeitet. Personenbezogene Daten sind gemäß der Legaldefinition in § 3Abs. 1 Bundesdatenschutzgesetz (BDSG) „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)". Es wird also auch beim Vorliegen (lediglich) personenbeziehbarer Daten der Anwendungsbereich des Datenschutzrechts als eröffnet betrachtet. „Bestimmbar" ist eine Person, wenn ihre Identität nicht direkt anhand des Datums, aber – objektiv gesehen – durch (ggf. mehrere) Zwischenschritte festgestellt werden kann.[17] Wenn im Rahmen des Projektes ITS.APT demnach bspw. das Anklicken des Links in einer Spam-E-Mail einem bestimmten E-Mail-Konto zugerechnet werden kann und dieses E-Mail-Konto aufgrund der internen E-Mail-Adress-Zuteilung einem bestimmten Mitarbeiter – und das entwickelte Programm die Rückführbarkeit auch nicht per se ausschließt – handelt es sich bei der Feststellung des Verhaltens um die Verarbeitung eines personenbeziehbaren Datums des Mitarbeiters. Gleiches gilt, wenn über die IP-Adresse des abrufenden Rechners auf die abrufende Person geschlossen werden kann.[18]

[16] Däubler/Klebe/Wedde/Weichert/*Wedde*, BDSG, § 32 Rn. 69.
[17] Däubler/Klebe/Wedde/Weichert/*Weichert*, BDSG, § 3 Rn. 13.
[18] Zur Personenbeziehbarkeit von IP-Adressen vgl. *BGH*, Beschl. v. 28.10.2014 - VI ZR 135/13. Der EuGH hat zum Zeitpunkt der Erstellung dieses Dokuments noch nicht über die Vorlagefrage entschieden. Nach h.M. wird jedoch von einer Personenbeziehbarkeit sowohl statischer, als auch dynamischer IP-Adressen ausgegangen. Vgl. statt vieler Gola/Schomerus/*Gola/Klug/Körffer*, BDSG, § 3 Rn. 10.

Verantwortliche Stelle, d.h. verantwortlich für die Einhaltung der Datenschutzvorschriften, ist gem. § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Der Arbeitgeber ist bzgl. der Personal-, wie auch dienstlichen Kommunikationsdaten seiner Arbeitnehmer daher unproblematisch verantwortliche Stelle im Sinne des Gesetzes. Das LDSG S-H bezeichnet den Verantwortlichen mit „datenverarbeitende Stelle“ und definiert diese als „jede öffentliche Stelle im Sinne von § 3 Abs. 1 [LDSG S-H], die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt“ (§ 2 Abs. 3 LDSG S-H). Zwar werden vorliegend im Interesse des gesamten Projektes ITS.APT zusätzliche Verkehrsdaten der UKSH-Mitarbeiter erhoben. Allerdings erfolgt diese Erhebung faktisch durch das UKSH (bzw. seine IT-Gesellschaften). Mitarbeitern des Projektes ITS.APT, die nicht zugleich auch Mitarbeiter des UKSH (bzw. der IT-Gesellschaften) sind, wird kein direkter Zugriff auf die IT-Systeme des UKSH (bzw. der IT-Gesellschaften) gewährt. Die personenbezogenen Daten werden durch das UKSH als datenverarbeitende Stelle erhoben und dem Projekt pseudonymisiert (bzw. soweit möglich anonymisiert) zur Verfügung gestellt, d.h. übermittelt. Im Einzelnen wird diese Vorgehen in TAP 2.3 „Datenschutzrechtliche Betrachtung“ analysiert. Auch bzgl. der datenschutzrechtlichen Bewertung des Verhältnisses zwischen dem UKSH und den privaten IT-Tochtergesellschaften wird auf das Dokument TAP 2.3 „Datenschutzrechtliche Betrachtung“ verwiesen.

II. Testdurchführung

1. Anwendbare Gesetze

Normen, die – auch – dem Schutz personenbezogener Daten dienen, sind nicht ausschließlich im BDSG bzw. den Landesdatenschutzgesetzen (LDSG) zu finden. BDSG und LDSGe sind vielmehr lediglich Auffanggesetze, die subsidiär anzuwenden sind, soweit keine spezielleren Regelungen für den zu beurteilenden Sachverhalt existieren[19] (Vgl. auch Subsidiaritätsklauseln z.B. in § 1 Abs. 3 BDSG oder § 3 Abs. 3 LDSG S-H.). Soweit es um die Verarbeitung personenbezogener Daten im Rahmen von sog. Telekommunikations- und Telemediendiensten geht, genießen demnach das Telekommunikations-, bzw. das Telemediengesetz als jeweilige bereichsspezifische Spezialgesetze Anwendungsvorrang. Allgemein gesprochen beschäftigt sich das Telekommunikationsgesetz (TKG) hierbei mit der rein technischen Kommunikationsinfrastruktur und -übertragung („Übertragung von

[19] Däubler/Klebe/Wedde/Weichert, BDSG, Einleitung Rn. 71.

Signalen“) als solcher, während das Telemediengesetz (TMG) den Umgang mit (Kommunikations-)Inhalten adressiert.

a. Telekommunikationsgesetz

Telekommunikationsdienste sind gemäß § 3 Nr. 24 TKG in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen. Diensteanbieter ist nach § 3 Nr. 6 TKG jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt.

Nur der Vollständigkeit halber sei erwähnt, dass Telekommunikationsdienste wiederum von Telemediendiensten abzugrenzen sind. Die spezialgesetzliche Regelung hierzu ist das TMG. Gemäß § 2 Nr. 1 TMG ist (Telemedien-)Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert.

Bei gestatteter privater Nutzung betrieblicher E-Mail-Systeme stellt sich die Frage, inwiefern der Arbeitgeber seinen Arbeitnehmern gegenüber Telekommunikationsdiensteanbieter ist; denn in diesem Fall verschafft der Arbeitgeber – bei streng am Wortlaut orientierter Betrachtung – Dritten (seinen Arbeitnehmern) die Möglichkeit zur Nutzung von Telekommunikationsdiensten. Ist – wie am UKSH der Fall – die private Nutzung hingegen untersagt, stellt sich die Frage nicht und das TKG kommt nicht zur Anwendung. Eine Erlaubnisnorm für die Testdurchführung aus dem TKG kommt mithin schon aus diesem Grund nicht in Betracht.

Bei gestatteter privater Nutzung ist die Telekommunikationsanbietereigenschaft des Arbeitgebers in Rechtsprechung und Literatur umstritten. Während die herrschende Lehre und insbesondere die Datenschutzaufsichtsbehörden die Auffassung vertreten, dass der Arbeitgeber in diesem Falle Telekommunikationsdiensteanbieter i.S.d. TKG ist[20] und folglich u.a. gem. § 88 TKG das Fernmeldegeheimnis zu beachten hat, lehnt eine in der

[20] Vgl. statt vieler: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Private sowie dienstliche Internet- und E-Mail-Nutzung, http://datenschutzzentrum.de/uploads/privatwirtschaft/private-und-dienstliche-internetnutzung.pdf.

Rechtsprechung zuletzt überwiegend vertretene Auffassung[21] die Anwendung des TKG im Arbeitsverhältnis ab.

Im Rahmen des Anwendungsbereichs des TKG schützt § 88 TKG das Fernmeldegeheimnis aus Art. 10 GG. Dem Fernmeldegeheimnis unterliegen gemäß § 88 Abs. 1 TKG neben dem Inhalt der Telekommunikation auch ihre näheren Umstände und insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche. Dem Arbeitgeber wäre es folglich untersagt, auch nur den E-Mail-Eingang an den Arbeitnehmer, die auf dem betrieblichen Server gespeichert sind, einzusehen.[22]

Soweit die Rechtsprechung die Anwendbarkeit des § 88 TKG ablehnt, wird maßgeblich darauf abgestellt, dass § 88 TKG eine spezielle Schutzvorschrift für personenbezogene Daten, die im Rahmen eines Telekommunikationsvorgangs anfallen und eine einfachgesetzliche Ausprägung des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) sei. Der Schutzbereich sei nicht eröffnet. Art. 10 Abs. 1 GG schütze lediglich den Kommunikationsvorgang als solchen, nicht die bereits im Postfach des Arbeitnehmer – und damit „im Herrschaftsbereich des Telekommunikationsteilnehmers“[23] – gespeicherten E-Mails. Nach Abschluss des Kommunikationsvorgangs greife nicht mehr das Fernmeldegeheimnis, sondern die Kommunikationsinhalte seien (nur) durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) geschützt.[24] Das Bundesverfassungsgericht grenze den Schutzbereich des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG in ständiger Rechtsprechung auf die Bewahrung des privaten, vor der Öffentlichkeit und den Eingriffen unbefugter Dritter unbehelligt ablaufenden Austauschs von Informationen während des Kommunikations- oder Übertragungsvorgangs ein.[25]

Dies betrifft Fälle, in denen der Arbeitgeber etwa das E-Mail-Postfach des Arbeitnehmern durchsuchen möchte, in dem Sinne, dass er in lokal auf dem Rechner des Arbeitnehmer gespeicherte E-Mails Einsicht nimmt, oder gespeicherte Verbindungsdaten nach Abschluss des Telekommunikationsvorganges einsieht und auswertet, beantwortet aber nicht die Frage,

[21] Zuletzt erneut in diesem Sinne *LAG Berlin-Brandenburg*, Urt. v. 14.01.2016 - 5 Sa 657/15.
[22] Wybitul, NJW 2014, 3605 (3607).
[23] *LAG Berlin-Brandenburg*, Urt. v. 14.01.2016 - 5 Sa 657/15, Rn. 116.
[24] *VGH Kassel*, Beschl. v. 19. 5. 2009 - 6 A 2672/08.Z; *LAG Berlin-Brandenburg*, Urt. v. 16.2.2011 - 4 Sa 2132/10; *LAG Niedersachsen*, Urt. v. 31.5.2010 - 12 SA 875/09.
[25] *VG Karlsruhe*, Urt. v. 27.5.2013 - 2 K 3249/12.

ob der Arbeitgeber grds. als Telekommunikationsdiensteanbieter anzusehen, und damit an die Vorgaben des TKG gebunden ist.

Das VG Karlsruhe[26] hat in einer Entscheidung aus dem Jahr 2013 darüber hinaus ausgeführt, Arbeitgeber seien jedenfalls keine Telekommunikationsdiensteanbieter, da der Gesetzeszweck des § 88 TKG dem entgegenstünde. Aus § 1 TKG folge, dass es sich um ein Gesetz zur Förderung des privaten Wettbewerbs im Bereich der Telekommunikation handele, dass also auf die Rechtsbeziehungen zwischen dem Staat und den Telekommunikationsanbietern sowie diejenigen zwischen den Telekommunikationsanbietern untereinander abgezielt werde. Das Gesetz wolle nicht die unternehmens- beziehungsweise behördeninternen Rechtsbeziehungen – wie zwischen Arbeitgeber und Arbeitnehmer – regeln. Ähnlich argumentiert das LArbG Berlin-Brandenburg in seinem Urteil aus Januar 2016; § 3 Nr. 10 TKG setze voraus, dass das Angebot der Telekommunikation sich an außerhalb der Sphäre des Diensteanbieters liegende Dritte richte.[27] Dies sei im Arbeitgeber-Arbeitnehmer-Verhältnis nicht der Fall.

Dem ist nicht zu folgen. Aus der Formulierung „in der Regel gegen Entgelt“, sowie der Definition des § 3 Nr. 10 TKG[28] ergibt sich, dass Anbieter von Telekommunikationsdiensten nicht unbedingt mit Gewinnerzielungsabsicht handeln müssen. Sie müssen den Telekommunikationsdienst auch nicht zwingend selbst erbringen; eine Mitwirkung hieran genügt, sodass grds. auch bspw. Hotels oder Krankenhäuser unter den Begriff fallen, soweit sie ihren Gästen oder Patienten die Möglichkeit zur Nutzung von Telekommunikationsdiensten einräumen.[29] Diese stehen – als Anbieter von Telekommunikationsdiensten – auch nicht im Wettbewerb, dennoch haben sie das Fernmeldegeheimnis ihrer Kunden zu beachten. Aus der Tatsache, dass der Arbeitgeber nicht in diesem Sinne im Wettbewerb steht, kann kein geringerer Grundrechtsschutz der Arbeitnehmer folgen.

b. Bundesdatenschutzgesetz und Landesdatenschutzgesetz

Im Übrigen finden die Datenschutzgesetze Anwendung. Datenschutzgesetze gibt es sowohl auf Bundesebene (Bundesdatenschutzgesetz – BDSG), als auch auf Länderebene (Landesdatenschutzgesetz – LDSG). Auf das UKSH als Anstalt öffentlichen Rechts mit Sitz

[26] *VG Karlsruhe*, Urt. v. 27.5.2013 - 2 K 3249/12.
[27] *LAG Berlin-Brandenburg*, Urt. v. 14.01.2016 - 5 Sa 657/15, Rn. 116.
[28] § 3 Nr. 10 TKG: „geschäftsmäßiges Erbringen von Telekommunikationsdiensten“ das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht.
[29] Geppert/Schütz/*Schütz*, TKG, § 3 Rn. 15.

im Land Schleswig-Holstein findet das Landesdatenschutzgesetz Schleswig-Holstein (LDSG S-H) Anwendung. Zu Einzelheiten hierzu vgl. TAP 2.3 „Datenschutzrechtliche Betrachtung". Im Rahmen dieses Dokuments soll im Folgenden maßgeblich auf die Rechtslage nach LDSG S-H abgestellt werden, um Wiederholungen zu vermeiden. Zu Vergleichszwecken wird die entsprechende Rechtsnorm nach Bundesrecht jeweils kurz erwähnt und auf grundlegende Unterschiede – soweit vorhanden – aufmerksam gemacht.

2. Datenerhebung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit es gesetzlich erlaubt oder angeordnet ist oder der Betroffene eingewilligt hat (vgl. § 4 Abs. 1 BDSG; § 11 Abs. 1 LDSG S-H.).

Wie bereits unter C[30] ausgeführt, ergeben sich aus dem zwischen Arbeitgeber und Arbeitnehmer bestehenden Arbeitsverhältnis rechtliche Besonderheiten. Dies gilt auch für die datenschutzrechtlichen Erwägungen.

Weiterhin ist zu berücksichtigen, dass im Rahmen des Projekts Daten der Arbeitnehmer zu wissenschaftlichen Zwecken verarbeitet werden sollen. Erst basierend auf den Forschungsergebnissen können und sollen ein Werkzeug sowie ein Schulungskonzept entwickelt werden, welche im Praxiseinsatz zu einer Erhöhung des IT-Sicherheitsbewusstseins der Arbeitnehmer führen und so zur Verbesserung der IT-Sicherheit in Organisationen beitragen. Dennoch ist eine Erhöhung der IT-Sicherheit im UKSH bereits durch die Durchführung des Forschungsprojekts und der in diesem Rahmen erfolgenden Mitarbeiterschulungen ein in der Abwägung zu berücksichtigender Faktor.

Schließlich hängt die rechtliche Zulässigkeit auch davon ab, welche Daten erhoben werden sollen, bzw. auf welche Daten zugegriffen werden soll. Wie bereits unter B[31] ausgeführt, werden im Rahmen der Testdurchführung lediglich solche Daten erhoben, die als „Verkehrsdaten" im Sinne des TKG zu klassifizieren sind.[32]

Zu berücksichtigen ist ferner, ob (auch) personenbezogene Daten i.S.d. § 11 Abs. 3 LDSG S-H, d.h. personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben sowie von Daten, die

[30] Siehe dazu oben S. 9.
[31] Siehe dazu oben S. 7.
[32] Unabhängig von der vorliegenden Nichtanwendbarkeit des TKG, soll auf die dort festgelegte Terminologie bzgl. der zu verarbeitenden Daten zurückgegriffen werden.

einem besonderen Berufs- oder Amtsgeheimnis unterliegen, erhoben und verarbeitet werden oder nicht. Im Rahmen des Projekts ITS.APT werden diese Kategorien von Daten nicht erhoben.

a. § 32 BDSG/§ 23 LDSG S-H

Wie einleitend ausgeführt, befinden sich die Probanden in einem Beschäftigungsverhältnis mit einem der Projektpartner, dem UKSH.

Für den Umgang mit Arbeitnehmerdaten ist § 32 BDSG die zentrale Norm für die Erhebung und Verarbeitung von personenbezogenen Daten im Rahmen von Beschäftigungsverhältnissen auf Bundesebene. Zwecke der Datenverarbeitung sind danach Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses. Daten dürfen zu diesen Zwecken erhoben und verarbeitet werden, wenn und soweit dies erforderlich ist. Im Rahmen der Durchführung des Beschäftigungsverhältnisses ist grds. auch eine Datenerhebung zum Zwecke des Arbeitsverhaltens gestattet.

Für das UKSH als öffentliche Stelle auf Landesebene in Schleswig-Holstein ist § 23 LDSG S-H die zentrale Norm für die Verarbeitung von Arbeitnehmerdaten. (Bzgl. Einzelheiten zur Eigenschaft des UKSH als verantwortliche Stelle im Sinne des Datenschutzrechts bzgl. der personenbezogenen Daten seiner Arbeitnehmer vgl. Dokument TAP 2.3 „Datenschutzrechtliche Betrachtung“.) Anders als im Bundesrecht gibt es mithin nach Landesrecht Schleswig-Holstein keine Norm, die speziell die Erhebung von Arbeitnehmerdaten regelt. § 23 LDSG S-H beschränkt sich auf Regelung der *Verarbeitung* von – denklogisch – bereits vorhandener, zuvor rechtmäßig erhobener Arbeitnehmerdaten. Für spezielle Regelungen verweist er im Übrigen auf das Landesbeamtengesetz Schleswig-Holstein (LBG S-H), das insofern auch Anwendung auf Beschäftigte findet.[33]

b. § 40 BDSG/§ 22 LDSG S-H

Allerdings erfolgt die Datenerhebung in ITS.APT zwar im arbeitsrechtlichen Kontext, aber doch vornehmlich zu wissenschaftlichen Zwecken. Mit den Vorschriften „Datenverarbeitung für wissenschaftliche Zwecke“ (§ 22 LDSG S-H), bzw. „Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen“ (§ 40 BDSG) bestehen hierfür eigene gesetzliche Erlaubnisnormen.

[33] Vgl. Begründung zum Entwurf des Landesdatenschutzgesetzes, https://www.datenschutzzentrum.de/material/recht/ldsg-novellierung/begruend.htm#Par23.

§ 40 Abs. 1 BDSG gestattet die Verarbeitung und Nutzung von für Zwecke der wissenschaftlichen Forschung erhobenen oder gespeicherten personenbezogenen Daten. Ausweislich seines Wortlautes ist § 40 BDSG damit keine Datenerhebungsgrundlage, sondern lediglich eine Rechtsnorm, die die Nutzung und (Weiter-)Verarbeitung bereits für Forschungszwecke erhobener Daten regelt. Dem liegt die Wertung zugrunde, dass es dem Kern des informationellen Selbstbestimmungsrechts der Betroffenen zuwider sein würde, ohne oder gegen seinen Willen zum Objekt von Datenverarbeitung (hier zugunsten wissenschaftlicher Forschung) zu werden. [34]

Der hier maßgebliche § 22 LDSG S-H gestattet indes eine sehr umfassende Datenverarbeitung zu wissenschaftlichen Zwecken. § 22 Abs. 1 Alt. 1 LDSG S-H gestattet pauschal die „Verarbeitung" von personenbezogenen Daten durch öffentliche Stellen. „Datenverarbeitung" umfasst das Erheben, Speichern, Übermitteln, Sperren, Löschen, Anonymisieren und Pseudonymisieren personenbezogener Daten (§ 2 Abs. 2 LDSG S-H). Allerdings soll jegliche Verarbeitung anonym, bzw., soweit dies nicht möglich ist, pseudonym erfolgen (§ 22 Abs. 1 S. 3 LDSG S-H), d.h. auch die Erhebung.

„Pseudonymisieren" bezeichnet nach LDSG S-H „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können" (§ 2 Abs. 2 Nr. 7 LDSG S-H), „anonymisieren" „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können" (§ 2 Abs. 2 Nr. 6 LDSG S-H).

Das BDSG definiert Pseudonymisieren indes als „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren" (§ 3 Abs. 6a BDSG) und „Anonymisieren" als „Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können" (§ 3 Abs. 6 BDSG).

Entscheidend für die Abgrenzung dieser oftmals verwechselten Begriffe ist mithin das Bestehen einer (Re-)Identifizierungsmöglichkeit der Betroffenen, ob also der Personenbezug

[34] Gola/Schomerus/Körffer/Klug/*Gola*, BDSG § 40 Rn. 5.

(wieder)herstellbar ist oder nicht.[35] Im Falle einer Pseudonymisierung verfügt die verantwortliche Stelle über eine Referenzdatei (sog. Kreuzliste), die eine Auflösung der Pseudonyme ermöglicht. Ohne diese können einzelne Daten nicht (mehr) einzelnen Betroffenen zugeordnet werden.

Eine Unterscheidung beider Begriffe voneinander ist notwendig, nicht zuletzt, da das Recht unterschiedliche Folgen an das Vorliegen anonymisierter bzw. pseudonymisierter Daten knüpft. Während die Datenschutzgesetze auf anonyme bzw. anonymisierte (= nicht personenbeziehbare) Daten keine Anwendung finden, gelten sie doch für die Verarbeitung pseudonymer bzw. pseudonymisierter Daten. Erst bei Nicht(mehr)herstellbarkeit eines Personenbezugs, d.h. wenn eine Reanonymisierung unmöglich ist, sind Daten per Definition anonymisiert und ist das Datenschutzrecht nicht mehr anwendbar. Zur Definition von „Personenbezug" bzw. „Personenbeziehbarkeit" vertreten werden der sog. absolute und der sog. relative Personenbegriff.

Für Vertreter des relativen Personenbegriffs ist entscheidend, ob die verantwortliche Stelle über das zur Reanonymisierung bzw. Identifikation erforderliche (zusätzliche) Wissen verfügt. Die Zusatzinformation muss nicht schon (oder noch) vorhanden sein und es muss auch keine Absicht der Reanonymisierung bzw. Identifikation bestehen. Es ist eine aus objektiver Sicht zu treffende Einzelfallentscheidung geboten: Ist die individuelle verantwortliche Stelle bereit, den unverhältnismäßig hohen Aufwand zu betreiben, sind die Daten nicht anonym.[36]

Dem absoluten Personenbegriff folgend muss es indes jedermann unmöglich sein, einen Personenbezug (wieder)herzustellen. Es kommt mithin nicht auf die individuellen Kenntnisse der verantwortlichen Stelle oder ihren Willen, den unverhältnismäßig hohen Aufwand zu betreiben an, sondern ob das erforderliche Zusatzwissen objektiv nur unter einem „unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft beschafft werden kann".[37] Daraus folgt im Ergebnis, dass – aufgrund der Möglichkeiten der modernen IT – praktisch eine Anonymisierung oft unmöglich ist und auch, dass früher als „anonymisiert" geltende Datenbestände dies nach heutigen Möglichkeiten nicht mehr sind. Einzelheiten zu Pseudoymisierung werden im Dokument TAP 2.3 „Datenschutzrechtliche Betrachtung" ausgeführt.

[35] Simitis/*Scholz*, BDSG, § 3 Rn. 215.
[36] Gola/Schomerus/*Gola/Körffer/Klug*, BDSG § 3 Rn. 44.
[37] Däubler/Klebe/Wedde/Weichert/*Weichert*, BDSG, § 3 Rn. 47.

Aus Vorgesagtem ergibt sich, dass in der in ITS.APT gegebenen Konstellation weder eine Anonymisierung, noch eine Pseudonymisierung möglich ist. Eine Anonymisierung würde den Forschungszweck, Unterschiede zwischen verschiedenen Personengruppen (z.B. nach Alter oder Geschlecht) herauszufinden unmöglich machen. Eine pseudonyme Erhebung im UKSH scheidet aus, da das UKSH selbst im Besitz der sog. Kreuzliste, d.h. der Zuordnungsfunktion ist. (Vgl. grundlegendend zu den Voraussetzungen des § 22 LDSG S-H TAP2.3 „Datenschutzrechtliche Betrachtung“.) Aus dem „Forschungsprivileg“ des weiten § 22 LDSG S-H ergeben sich mithin an dieser Stelle (noch) keine Besonderheiten. Wegen der fehlenden Anonymisierungs- bzw. Pseudonymisierungsmöglichkeit sollte für die Erhebung von personenbezogenen Daten im Rahmen von ITS.APT aber eine andere Rechtsgrundlage gefunden werden, wobei die Besonderheit, dass diese Datenerhebung aus Sicht der Probanden im Rahmen ihres Beschäftigungsverhältnisses erfolgt, zu berücksichtigen ist.

c. Vorhandene Daten

Das UKSH verfügt über eine umfassende IT und erhebt und speichert im gesetzlich zulässigen Rahmen u.a. Daten, die Rückschlüsse auf das Nutzungsverhalten der Arbeitnehmer zulassen. Der gesetzlich zulässige Rahmen wird in erster Linie durch §§ 5, 6 LDSG S-H bestimmt. Hiernach ist die verantwortliche Stelle berechtigt, unter engen Voraussetzungen solche personenbezogene Daten zu speichern, die zur Gewährleistung der IT-Sicherheit erforderlich sind. (Vgl. hierzu im Einzelnen TAP 2.3 „Datenschutzrechtliche Betrachtung“.)

Allerding besteht insoweit gem. § 23 Abs. 2 LDSG S-H ein Verarbeitungsverbot zu Zwecken der Verhaltenskontrolle. Hiernach dürfen personenbezogene Daten von Arbeitnehmern vorbehaltlich besonderer gesetzlicher oder tarifvertraglicher Regelungen nur nach Maßgabe der §§ 85 bis 92 des Landesbeamtengesetzes (LBG S-H) verarbeitet (Abs. 1), und Daten von Arbeitnehmern, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach den §§ 5 und 6 gespeichert oder in einem automatisierten Verfahren gewonnen werden, nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden (Abs. 2). Weiterhin ist zu bedenken, dass die von ITS.APT benötigten Daten erst für das Projekt erzeugt und erhoben werden, indem ein zusätzliches Programm in das IT-System eingebracht wird. Es handelt sich mithin um einen anderen Datenerhebungsvorgang als er gewöhnlich im Rahmen der §§ 5, 6 LDSG S-H erfolgt.

Für die Testdurchführung in ITS.APT kann mithin nicht auf Daten i.S.d. § 23 Abs. 2 LDSG S-H zugegriffen werden. Es ergibt sich auch keine andere Wertung aus der Tatsache, dass die Daten zu Forschungszwecken verwendet werden sollen und nur zu diesem

Zwecke eine Verhaltenskontrolle stattfindet, statt – wie § 23 Abs. 2 LDSG S-H vornehmlich zu verhindern sucht – eine solche zur heimlichen, lückenlosen Überprüfung des Nutzungsverhaltens mit Fokus auf Arbeitsleistung und mögliche Sanktionierungen durch den Arbeitgeber[38] unter Umgehung der Regelungen zur zweckgebundenen Erhebung und Verarbeitung personenbezogener Daten.

d. §§ 11, 13 LDSG S-H

aa. §§ 11, 13 Abs. 1 S. 1 LDSG S-H

Mangels speziellerer Erhebungsgrundlagen, ist auf die allgemeine Regelung zur Datenerhebung zurückzugreifen. §§ 11, 13 Abs. 1 S. 1 LDSG S-H regelt die grundsätzliche Zulässigkeit der Erhebung von personenbezogenen Daten. Dies darf demnach nur mit der Kenntnis der Betroffenen geschehen, soweit nicht die Voraussetzungen des § 13 Abs. 3 Nr. 1, 2 oder 4 LDSG S-H vorliegen.

„Mit Kenntnis der Betroffenen" würde im vorliegenden Fall jedoch bedeuten, dass die zu testenden Mitarbeiter umfassend über Art und Umfang der Testdurchführung aufzuklären wären, d.h. die Identität der verantwortlichen Stelle, Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und ggf. der Kategorien der zu erhebenden Daten.[39] Diese Wertung von „Kenntnis" ergibt sich aus den Anforderungen der eigentlich bestehenden Informationspflicht; es ist anzunehmen, dass der Gesetzgeber nicht differenzieren wollte zwischen „informierten" Betroffenen, die bei der Datenerhebung persönlich aufgeklärt wurden, und solchen denen nur mitgeteilt werden muss, dass man sich Daten über sie beschafft hat.[40] Weiterhin müsste in einem nächsten Schritt – um die Rechtmäßigkeit der weiteren Verarbeitung im Projektkontext zu gewährleisten – die Einwilligung jedes einzelnen (potenziell) Betroffenen eingeholt werden. Diese Einwilligung müsste den Anforderungen der §§ 11 Abs. 1, 12 LDSG S-H genügen. (Siehe hierzu auch TAP 2.3 „Datenschutzrechtliche Betrachtung".)

In Anbetracht des Testzweckes, nämlich u.a. das im Arbeitsalltag gewöhnlich vorhandene Verhalten und IT-Sicherheitsbewusstsein der Arbeitnehmer zu erfassen und zu analysieren, wäre eine datenschutzrechtlich wirksame Einwilligung, d.h. eine solche, die alle Anforderungen an Informiertheit erfüllt, nicht die optimale Lösung. Die Teilnehmer wären

[38] *Schierbaum*, CuA 2015, 33 (37).
[39] Zur Auslegung des Begriffs „Kenntnis" kann auf die Literatur zu § 33 BDSG zurückgegriffen werden, der den Begriff in vergleichbarem Kontext verwendet.
[40] Gola/Schomerus/*Körffer/Gola/Klug*, BDSG § 33 Rn. 6.

unmittelbar über die Vorgehensweise unterrichtet, was wahrscheinlich bereits ihre Aufmerksamkeit erhöhen und so nicht zu einem authentischen Ergebnis führen würde. Hinzu kommen praktische Durchführungsprobleme. Die Einwilligung wäre zwingend so zu gestalten, dass die Betroffenen sie jederzeit mit Wirkung für die Zukunft zurückziehen könnten (§ 12 Abs. 2 S. 3 LDSG S-H), mit der Folge, dass dann unmittelbar auch die bislang von dem Betroffenen erhobenen Daten zu löschen wären, wobei (nur) bereits anonymisierte Ergebnisse einer bereits erfolgten Auswertung erhalten blieben.

bb. §§ 11, 13 Abs. 1 S. 2 i.V.m. 13 Abs. 3

Mithin ist muss eine Erlaubnisnorm gefunden werden, die die Erhebung per Definition „ohne Kenntnis" der Betroffenen gestattet. Eine Erhebung ohne Kenntnis der Betroffenen ist gestattet, wenn eine Rechtsvorschrift dies erlaubt (§ 13 Abs. 1 S. 2 i.V.m. Abs. 3 Nr. 1 LDSG S-H), die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit, persönliche Freiheit oder sonstiger schwerwiegender Beeinträchtigungen der Rechte einzelner dies gebietet (§ 13 Abs. 1 S. 2 i.V.m. Abs. 3 Nr. 2 LDSG S-H) oder wenn die Einholung der Einwilligung nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre und offensichtlich ist, dass die Verarbeitung im Interesse der oder des Betroffenen liegt und sie oder er in Kenntnis des anderen Zwecks die Einwilligung erteilen würde (§ 13 Abs. 1 S. 2 i.V.m. Abs. 3 Nr. 4 LDSG S-H).

Zur „Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit, persönliche Freiheit oder sonstiger schwerwiegender Beeinträchtigungen der Rechte einzelner" geboten ist die Datenerhebung im Kontext des Projektes nicht. Selbst wenn man IT-Sicherheitsvorfälle – verursacht durch unachtsame Arbeitnehmer– als „erheblichen Nachteil für das Allgemeinwohl" klassifizieren würde, werden durch die erstmalige Datenerhebung im Projektkontext lediglich Informationen über das IT-Verhalten der Arbeitnehmer gesammelt. Diese Erhebung führt weder unmittelbar zu einer Erhöhung des IT-Sicherheitsbewusstseins der Arbeitnehmer, noch ist sicher vorauszusagen, dass im Rahmen des Projektes gelingen wird, das IT-Sicherheitsbewusstsein signifikant zu erhöhen. Die Formulierung „zur Abwehr geboten" deutet indes auf den allgemeinen Grundsatz der Erforderlichkeit hin, der im Datenschutzrecht gilt und meint, dass eine Verarbeitung nur insoweit zulässig ist, wie zur Erreichung des Zwecks notwendig.[41] In diesem Rahmen ist

[41] *Wolff/Brink*, Syst. A, Rn. 23.

objektiv geboten, was objektiv tauglich ist, den festgelegten Zweck zu erreichen.[42] Das ist hier vorab schwer zu beurteilen, sodass eine andere Rechtsgrundlage gefunden werden muss.

Die Einwilligung jedes Betroffenen einzuholen würde den Projektzweck gefährden (vgl. oben), wäre aber weder unmöglich noch unverhältnismäßig: Alle Arbeitnehmer des UKSH sind problemlos über ihre jeweiligen dienstlichen E-Mail-Adressen – die auch für die Durchführung der Tests benutzt werden – zu erreichen. Grds. kann sich die Unverhältnismäßigkeit allein aus der Anzahl der Betroffenen ergeben, allerdings ist in die Abwägung auch die „Sensitivität" der Daten für die Betroffenen einzubeziehen.[43] Insbesondere unter Berücksichtigung der besonderen Konstellation, dass bei den Betroffenen hier Daten im Zusammenhang mit ihrem bestehenden Beschäftigungsverhältnis erhoben werden sollen, erscheint die Einholung der Einwilligung jedes Einzelnen nicht unverhältnismäßig. Weiterhin müsste die Erhebung ohnehin offensichtlich im Interesse des Betroffenen liegen, sowie dieser bei Kenntnis die Einwilligung erteilen. Dies ist in Anbetracht der grundsätzlichen Wertung, dass niemand ohne oder gegen seinen Willen zum „Versuchskaninchen" gemacht werden soll (vgl. oben), sehr zweifelhaft.

Es bleibt mithin die Möglichkeit der Datenerhebung aufgrund einer Rechtsvorschrift, die dies erlaubt. In Betracht kommt der Abschluss einer Dienstvereinbarung. Eine Dienstvereinbarung nach Mitbestimmungsgesetz Schleswig-Holstein (MBG S-H) kann grds. eine Rechtsvorschrift in diesem Sinne sein:

Während Dienstvereinbarungen unzweifelhaft keine – das BDSG verdrängende – Rechtsvorschriften (des Bundes) i.S.d. § 1 Abs. 3 BDSG sein können, können sie aber grds. Erlaubnisnormen i.S.d. § 4 Abs. 1 BDSG sein.[44] Entsprechendes gilt für die landesrechtliche Norm § 13 Abs. 3 Nr. 1 LDSG S-H.

Nach BDSG muss eine Betriebs- oder Dienstvereinbarung für Zwecke des Arbeitsverhältnisses den Vorgaben des § 32 BDSG genügen, d.h. die Individualvereinbarung ist anhand des Schutzniveaus des § 32 BDSG zu prüfen[45] und an „grundgesetzlichen Wertungen, zwingendem Gesetzesrecht und den sich aus allgemeinen Grundsätzen des Arbeitsrechts ergebenden Beschränkungen" zu messen.[46] Ob eine Betriebsvereinbarung das Schutzniveau des BDSG im kollektiven Interesse „nach unten korrigieren" darf, ist

[42] *Wolff/Brink*, Syst. A, Rn. 28.
[43] Vgl. etwa zur Benachrichtigungspflicht: Gola/Schomerus/*Klug/Gola/Körffer*, BDSG, § 33 Rn. 36.
[44] Däubler/Klebe/Wedde/Weichert/*Weichert*, BDSG, § 1 Rn. 12.
[45] *BAG*, Beschl. v. 15.4.2014 - 1 ABR 2/13.
[46] *BAG*, Beschl. v. 27.5.1986 - 1 ABR 48/84.

umstritten.[47] Richtigerweise sind Fälle, in denen eine Datenverarbeitung nach BDSG rechtswidrig, durch eine Betriebsvereinbarung aber rechtmäßig wären, in Anbetracht der vom BAG zu späteren Zeitpunkten vertretenen Auffassung[48] kaum denkbar; auch im Hinblick auf den sich aus § 75 Abs. 2 BetrVG für Arbeitgeber und Betriebsrat ergebenden Schutzauftrag.[49]

Das vorliegend maßgebliche LDSG S-H ist indes nicht so ausdifferenziert. Die § 32 BDSG entsprechende Norm, § 23 Abs. 1 LDSG, verweist auf die §§ 85-92 des LBG S-H, das sich in diesem Abschnitt aber prinzipiell nur mit der Datenerhebung für die Führung von Personalakten beschäftigt, nicht mit Datenerhebung zur allgemeinen Verhaltenskontrolle. Aus § 85 Abs. 1 LBG[50] wird jedoch – sozusagen als „Parallelwertung" – auch allgemein, nicht nur für die Führung von Personalakten, gefolgert, dass eine Dienstvereinbarung grds. als Rechtsgrundlage zur Datenerhebung genügen kann, sodass im Ergebnis nichts anderes als nach BDSG und der hierzu entwickelten Rechtsprechung des BAG gelten sollte. Allerdings ist zu beachten, dass eine Dienstvereinbarung nur für den Teil der Arbeitnehmer Bindungswirkung hat, der vom Personalrat vertreten wird. Leitende Angestellte werden nicht erfasst und kommen mithin auch nicht als Probanden in Betracht.

3. Personaldaten

Ziel des Projektes ist es auch herauszufinden, ob sich das IT-Sicherheitsbewusstsein bestimmter Personengruppen von dem anderer grundlegend unterscheidet, bzw. ob diese Personengruppen möglicherweise auf Schulungen anders reagieren als andere. Soweit im Rahmen des Projektes hierzu Personaldaten, also zusätzliche personenbezogene Daten über die Arbeitnehmer, die an den Tests teilnehmen, benötigt werden (wie etwa Alter, Geschlecht etc.), sollten diese nicht durch Einsichtnahme in die Personalakten der Arbeitnehmer erhoben werden. § 89 LBG S-H trifft insofern eine abschließende Regelung, die nicht durch eine Dienstvereinbarung abbedungen werden kann. Nach § 89 Abs. 1 LBG S-H dürfen Personalakten ohne Einwilligung der Betroffenen nur zu den dort genannten Zwecken und nur den dort genannten Personenkreisen vorgelegt werden, bzw. hieraus Auskunft erteilt. Forschungszwecke sind nicht erfasst. § 89 Abs. 2 LBG S-H gestattet die Nutzung und

[47] In diesem Sinne das *BAG*, Beschl. v. 27.5.1986 - 1 ABR 48/84; allerdings wurde diese Auffassung nur einmalig vertreten. Kritisch hierzu z.B. Simitis/*Scholz/Sokol*, BDSG, § 4 Rn. 17 m.w.N.

[48] Vgl. bereits Fn. 26; *BAG*, Beschl. v. 9.7.2013 - 1 ABR 2/13; *BAG*, Beschl. v. 15.4.2014 - 1 ABR 2/13.

[49] Gola/Schomerus/*Klug/Gola/Körffer*, BDSG, § 4 Rn. 10a.

[50] „Der Dienstherr darf personenbezogene Daten über Bewerberinnen und Bewerber, Beamtinnen und Beamte sowie ehemalige Beamtinnen und Beamte nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift oder eine Vereinbarung nach dem Mitbestimmungsgesetz Schleswig-Holstein dies erlaubt."

Weitergabe ohne Einwilligung der Betroffenen u.a. zu Besoldungs- und Versorgungszwecken. Einschlägig für den Projektkontext ist § 89 Abs. 3 LBG S-H, der Auskünfte an Dritte regelt: Grds. bedürfen solche der Einwilligung der Betroffenen. Eine Ausnahme greift, soweit ein glaubhaftes rechtliches Interesse an der Kenntnis der zu übermittelnden Daten vorliegt und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an der Geheimhaltung überwiegen. Auch hier gilt, dass unter Berücksichtigung der grds. Wertung, dass niemand ohne sein Wissen Versuchskaninchen sein soll, die Betroffenen ein überwiegendes schutzwürdiges Interesse an der Nichtpreisgabe haben. In Betracht käme mithin, die Einwilligung der Betroffenen zur Einsichtnahme in ihre Personalakten durch das Projekt, bzw. einzelne Projektpartner, einzeln einzuholen. Unter Berücksichtigung des Grundsatzes der Datensparsamkeit (vgl. § 3a LDSG S-H), wonach schon die Erhebung personenbezogener Daten an dem Ziel auszurichten ist, so wenig personenbezogene Daten wie möglich zu erheben, erscheint es aber zwingend erforderlich, nicht die gesamte Personalakte einzusehen, wenn es keinen unverhältnismäßig größeren Aufwand bedeutet, die wenigen daraus tatsächlich benötigten persönlichen Daten über die Betroffenen unmittelbar von den Betroffenen durch Fragebögen zu erheben. Bei diesem Ansatz ist sodann § 51 MBG S-H zu beachten.[51]

4. Speicherung und Nutzung

Grundsätzlich wäre es denkbar, auch die Speicherung und Nutzung der für ITS.APT erhobenen Daten durch eine Dienstvereinbarung zu regeln. § 11 Abs. 1 Nr. 2 LDSG S-H bestimmt, dass die Verarbeitung personenbezogener Daten zulässig ist, wenn „dieses Gesetz [das LDSG S-H] oder eine andere Rechtsvorschrift sie erlaubt“. Auch in diesem Kontext kann „eine andere Rechtsvorschrift“ eine Dienstvereinbarung sein.

Im Rahmen des Projekts ITS.APT erfolgt eine Erhebung und Verarbeitung personenbezogenen Daten der Arbeitnehmer am UKSH zu wissenschaftlichen Zwecken. Nach § 22 Abs. 1 LDSG S-H soll die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken durch öffentliche Stellen und die Übermittlung personenbezogener Daten durch öffentliche Stellen an Dritte, die die Daten zu wissenschaftlichen Zwecken verarbeiten wollen (Datenverarbeitung für wissenschaftliche Zwecke) in anonymisierter Form erfolgen. Ist eine Anonymisierung nicht möglich, sollen die Daten pseudonymisiert werden, wobei gem. § 11 Abs. 6 LDSG S-H dann die empfangende

[51] Siehe dazu unten S. 35 ff.

Stelle keinen Zugriff auf die Zuordnungsfunktion haben darf und die Zuordnungsfunktion im alleinigen Zugriff der übermittelnden Stelle verbleibt.

Wie einleitend ausgeführt[52] soll das Projekt Erkenntnisse zur Reaktion von Arbeitnehmern in kritischen Infrastrukturen auf Phishing-Angriffe bringen und ein Konzept zu Verbesserungen im Umgang mit solchen Angriffen auf die betroffenen IT-Infrastrukturen erarbeiten. Hierbei handelt es sich um einen wissenschaftlichen Zweck. Das UKSH als verantwortliche Stelle ist eine öffentliche Stelle, die ITS.APT-Projektpartner sind „Dritte" im Sinne der Norm.

Eine genaue Subsumtion unter die Erlaubnistatbestandsmerkmale des § 22 LDSG S-H und sich ergebende Anforderungen an die Testdurchführung finden sich im Dokument TAP 2.3 „Datenschutzrechtliche Betrachtung".

5. Änderung der Rechtslage durch die DS-GVO

Die Verabschiedung und das Inkrafttreten der europäischen Datenschutz-Grundverordnung (DS-GVO) steht zum Zeitpunkt der Fertigstellung der Dokumente TAP 2.1 und TAP 2.3 unmittelbar bevor. Die Trilog-Fassung des Verordnungstextes liegt bereits vor,[53] erfährt aktuell jedoch noch redaktionelle Änderungen, bevor der Text zur Annahme dem Europäischen Rat und dem Europäischen Parlament vorzulegen ist.[54] Nach ihrem Inkrafttreten wird die DS-GVO erst nach einer Übergangsfrist von zwei Jahren Anwendung finden.[55] Während der Durchführung des Projektes ITS.APT wird die DS-GVO mithin für die Rechtslage nicht maßgeblich sein. Dennoch soll an dieser Stelle kurz auf arbeitsrechtlich relevante Aspekte in diesem Zusammenhang eingegangen werden.

Hinsichtlich des Arbeitnehmerdatenschutzes enthält die DS-GVO mit Art. 82 eine Öffnungsklausel, die es den Mitgliedstaaten gestattet, durch Gesetz oder Kollektivvereinbarung bereichsspezifische Regelungen zu treffen. Der Abschluss einer Betriebsvereinbarung würde durch die Öffnungsklausel grds. auch ermöglicht.[56] Soweit die Mitgliedstaaten hiervon keinen Gebrauch machen, wird die Zulässigkeit der

[52] vgl. Beschreibung der Angriffsszenarien, S. 7.
[53] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=DE.
[54] Art. 289 Abs. 1, 294 AEUV
[55] Art. 91 DS-GVO Trilog
[56] *Gola/Klug*, NJW 2016, 691 (693); *Wybitul/Sörup/Pötters*, ZD 2015, 559 (561);

Datenverarbeitung im Beschäftigungsverhältnis vornehmlich nach Art. 6 DS-GVO zu beurteilen sein.[57]

E. Beteiligung des Betriebs- und Personalrates

Bei der Durchführung des Projekts im UKSH müssen Beteiligungsrechte der dort bestehenden Mitarbeitervertretungen gewahrt werden, sofern die ihrem Zuständigkeitsbereich unterfallenden Arbeitnehmer Adressaten der Projektmaßnahmen sind. Mitarbeitervertretungen haben allgemein die Aufgabe zu gewährleisten, dass die Rechte der Arbeitnehmer geachtet werden.[58] In der öffentlichen Verwaltung, also beispielsweise im UKSH als Anstalt des öffentlichen Rechts, nehmen Personalräte diese Aufgaben wahr. Die für sie maßgeblichen gesetzlichen Regelungen finden sich in den Personalvertretungsgesetzen des Bundes und der Länder, im Falle des UKSH im MBG S-H. In Betrieben der Privatwirtschaft übernehmen Betriebsräte diese Aufgabe. Ihre Rechte und Pflichten bestimmen sich nach dem BetrVG. Für die dem UKSH angehörenden, aber privatrechtlich organisierten GmbHs ist damit das BetrVG anwendbar. Je nach dem aus welchen Bereichen des UKSH Mitarbeiter getestet werden, sind also sind Rechte von Personalräten und Betriebsräten zu wahren, sodass im Folgen auf die Interessen beider eingegangen wird.

I. Beteiligungsrechte des Betriebsrats nach dem BetrVG

In diesem Abschnitt wird untersucht, ob die Durchführung des Projekts Beteiligungsrechte des Betriebsrats tangiert. Konkret wird das Bestehen möglicher Informations- und Mitbestimmungsrechte im Rahmen des Projekts betrachtet.

1. Mitbestimmungsrechte

Das BetrVG nennt in dem § 87 Abs. 1 Nr. 1, 6 BetrVG sowie den §§ 94 Abs.1, 2 und 98 Abs. 1, 3 BetrVG Mitbestimmungsrechte des Betriebsrats, die bei der Projektdurchführung relevant sein können. Da diese Normen sich auf unterschiedliche betriebliche Maßnahmen beziehen, muss jede Projektphase einzeln auf seine Mitbestimmungspflichtigkeit hin überprüft werden. Im Folgenden wird daher zunächst auf die Konzeption der Tests und ihre erstmalige Durchführung (a) eingegangen, anschließend auf die Auswertung der Testergebnisse (b) und die Schulungen (c). Abschließend wird die erneute Durchführung der Tests (d) untersucht.

[57] *Wybitul/Pötters*, RDV 2016, 10 (11).
[58] Vgl. beispielsweise § 80 Abs. 1 BetrVG.

a. 1. Projektphase: Konzeption und erstmalige Durchführung der Tests

aa. Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 1 BetrVG

Gemäß § 87 Abs. 1 Nr. 1 BetrVG hat der Betriebsrat ein obligatorisches Mitbestimmungsrecht bei Angelegenheiten, die Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb betreffen. Unabhängig von der Frage, ob die Durchführung der Tests die Ordnung des Betriebs oder das Verhalten des Arbeitnehmers betrifft, scheidet ein Mitbestimmungsrecht nach dieser Norm schon aus einem anderen Grund aus. Denn sie erfasst lediglich die Normierung von Verhaltens- und Ordnungspflichten, nicht aber deren Überwachung[59] und schon gar nicht die Überwachung mittels technischer Einrichtungen. Letzteres wird ausdrücklich nur von § 87 Abs. 1 Nr. 6 BetrVG erfasst. Im Rahmen der Tests werden keine Regeln aufgestellt, sondern vielmehr auf technischem Wege kontrolliert, ob bestehende Regeln, im vorliegenden Fall sich IT sicherheitskonform zu verhalten, eingehalten werden. Für den Fall ergibt sich gerade kein Mitbestimmungsrecht des Betriebsrats aus § 87 Abs. 1 Nr. 1 BetrVG.

bb. Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG

Nach § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Die Norm dient dem Schutz vor den besonderen Gefahren für die Persönlichkeit, die von einer technischen Überwachung ausgehen.[60] Sie erfolgt oft heimlich, so dass sich der Betroffene nur unter erschwerten Voraussetzungen gegen sie zu wehren vermag.[61] Das in § 87 Abs. 1 Nr. 6 BetrVG normierte Mitbestimmungsrecht des Betriebsrats soll diese Gefahr verringern.
Zentraler Begriff der Norm ist deshalb der der technischen Einrichtung. Darunter ist jedes optische, mechanische, akustische oder elektronische Gerät zu verstehen.[62] Auch Software fällt im Zusammenspiel mit der benötigten Hardware unter diesen Begriff. Mit dem Einsatz

[59] *BAG*, Urt. v. 21.8.1990 – 1 AZR 567/89, NZA 1991, 154; *Decker/Deckers*, NZA 2004, 139 (140); i.E. genauso: *BAG*, Beschl. v. 18.4.2000 - 1 ABR 22/99, NZA 2000, 1176 (1177f.); *BAG*, Urt. v. 14.1.1986 – 1 ABR 82/83, BAGE 50, 337; *Schmitt*, AP BetrVG 1972 § 77 Nr. 24; Rolfs/Giesen/Kreikebohm/Udsching/*Werner*, § 87, Rn. 29.
[60] BT-Drucks. VI/1786, S. 49.
[61] *Richardi*, § 87, Rn. 480, 483.
[62] *BAG*, Urt. v. 8.11.1994 - 1 ABR 20/94, NJW 1984, 1476; Glögem /Preis/Schmidt/*Kania*, § 87, Rn. 48; Düwell/*Kohte*, § 87, Rn. 67; *Hanau*/*Hoeren*, S. 78.

der im Projekt entwickelten Software, die die Reaktion der Nutzer beispielsweise auf Phishing-Mails protokolliert, liegt daher eine technische Einrichtung vor.[63]

Mit Hilfe der technischen Einrichtung müsste auch eine Überwachung der Arbeitnehmer stattfinden. Als Überwachen gilt das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten, die der menschlichen Wahrnehmung zugänglich gemacht werden.[64] Im Projekt findet aufgrund des elektronischen Protokollierens der Reaktionen der Arbeitnehmer auf die Phishing-Mail ein solches Erheben personenbezogener Daten statt. Die gewonnen Informationen sind zudem auf einem Bildschirm wahrnehmbar. Der Einsatz der Software bewirkt daher eine Überwachung der Arbeitnehmer im UKSH.

Gegenstand der Überwachung muss ferner das Verhalten oder die Leistung der Arbeitnehmer sein. Verhalten wird als jedes individuell gesteuerte Tun oder Unterlassen definiert.[65] Die bei den Tests aufgezeichnete Reaktion der Arbeitnehmer, etwa das Anklicken der Phishing-Mail oder ein Anruf in der IT Abteilung, stellt ein Handeln oder Unterlassen dar. Damit liegt ein Verhalten als Gegenstand der Überwachung vor.

Erforderlich ist darüber hinaus, dass sich die erhobenen Daten den jeweiligen Arbeitnehmern zuordnen lassen.[66] Da dazu alleine die Möglichkeit einer Zuordnung ausreicht, lässt eine pseudonymisierte Datenerhebung ein Mitbestimmungsrecht nicht entfallen. Es besteht lediglich dann nicht, wenn die Daten anonymisiert im Sinne des § 3 Abs. 6 BDSG erhoben werden.[67]

Schlussendlich muss die technische Einrichtung auch zur Überwachung bestimmt sein. Ausreichend ist dazu bereits die objektive Eignung zur Beurteilung des Verhaltens der Arbeitnehmer,[68] auf den vom Arbeitgeber verfolgten Zweck kommt es nicht an.[69] Da die Projektsoftware sogar gezielt zum Protokollieren der Reaktionen der Arbeitnehmer eingesetzt wird, ist sie in jedem Fall zur Überwachung der Arbeitnehmer bestimmt.

---

[63] *Richardi*, § 87, Rn. 487.
[64] *BAG*, Urt. v. 6.12.1983 - 1 ABR 43/81, BAGE 44, 285; Glögem/Preis/Schmidt/*Kania*, § 87, Rn. 48; *Richardi*, § 87, Rn. 488-492.
[65] Stellv. *BAG*, Urt. v. 22.7.2008 - 1 ABR 40/07, BAGE 127, 146; *Hanau*/*Hoeren*, S. 81 f.; *Richardi*, § 87, Rn. 494; *Däubler*, Rn. 734; a.A. *Müllner*, DB 1984, 1677; dem Leistungsbegriff kommt keine eigenständige Bedeutung zu, er wird vom Verhaltensbegriff eingeschlossen, s. Glögem/Preis/Schmidt/*Kania*,§ 87, Rn. 50.
[66] *BAG*, Urt. v. 6.12.1983 - 1 ABR 43/81, BAGE 44, 285; *Hanau*/*Hoeren*, S. 81; Rolfs/Giesen/Kreikebohm/Udsching/*Werner*, § 87, Rn. 94; Glögem/Preis/Schmidt/*Kania*, § 87, Rn. 53; Richardi/Wißmann/Wlotzke/Oetker/*Matthes*, § 248, Rn. 23; *Weißnicht*, MMR 2003, 448 (452); *Deckers*/*Deckers*, NZA 2004, 139 (141); *Gebhardt/Umnuß*, NZA 1995, 103 (110).
[67] Glögem/Preis/Schmidt/*Kania*, § 87, Rn. 53; *Weißnicht*, MMR 2003, 448 (452); *Deckers*/*Deckers*, NZA 2004, 139 (141).
[68] Einhellige Auffassung, vgl. nur *BAG*, Urt. v. 9.9.1975 - 1 ABR 20/74, BAGE 27, 256; Glögem/Preis/Schmidt/*Kania*, BetrVG § 87, Rn. 55; Düwell/*Kohte*, § 87, Rn. 71; *Hanau*/*Hoeren*, S. 85.
[69] *Richardi*, § 87, Rn. 501; *Hanau*/*Hoeren*, S. 85.

Im Ergebnis hat der Betriebsrat deshalb ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG. Es umfasst zum einen die Einführung technischer Einrichtungen an sich, also ob eine technische Kontrolleinrichtung implementiert wird. Zum anderen erstreckt es sich auch auf die Modalitäten der Anwendung, d.h. wie die Überwachung konkret durchgeführt wird. Der Betriebsrat ist daher beispielsweise bei der Festlegung des Überwachungszeitraums oder der Auswahl der betroffenen Arbeitnehmer zu beteiligen.[70]

cc. Mitbestimmungsrecht aus § 94 Abs. 2 Hs. 2 BetrVG

Darüber hinaus könnte auch nach § 94 Abs. 2 Hs. 2 BetrVG ein Mitbestimmungsrecht bestehen. Das wäre der Fall, wenn im Rahmen der Projektdurchführung allgemeine Beurteilungsgrundsätze aufgestellt würden, also Regelungen, die der objektiven und einheitlichen Erfassung und Bewertung der Leistung der Arbeitnehmer dienen.[71] Die Projekttests werden so konstruiert, dass das erfasste Verhalten der Arbeitnehmer eine Aussage darüber ermöglicht, ob die Arbeitnehmer sich IT sicherheitskonform verhalten, mithin welche Leistung sie im Bereich IT Sicherheit erbringen. Im Rahmen der Testentwicklung werden zu diesem Zweck Kriterien festgelegt. Im Phishing-Mail-Angriffsszenario indiziert beispielsweise das Anklicken des Links ein geringes IT Sicherheitsbewusstsein, wohingegen ein sofortiges Löschen eher für das Gegenteil spricht. Diese Kriterien dienen mithin der Erfassung und Bewertung der Leistung der Arbeitnehmer, sodass Beurteilungsmerkmale aufgestellt werden.

Im Ergebnis besteht daher ein Mitbestimmungsrecht des Betriebsrats aus § 94 Abs. 2 Hs. 2 BetrVG, sodass er im Hinblick auf die Festlegung der Beurteilungsmerkmale bei der Testentwicklung zu beteiligen ist. Die Existenz des Mitbestimmungsrechts bedeutet indes nicht, dass der Betriebsrat verhindern kann, dass überhaupt Beurteilungsgrundsätze aufgestellt werden. Er hat vielmehr durch sein Zustimmungserfordernis mittelbar Einfluss auf die inhaltliche Ausgestaltung der Beurteilungsgrundsätze. Nicht mitbestimmungspflichtig ist indes die Durchführung der Beurteilung im Einzelfall.[72]

[70] Glögem/Preis/Schmidt/*Kania*, § 87, Rn. 58 f.; *Richardi*, § 87, Rn. 513 ff.; Richardi/Wißmann/Wlotzke/Oetker/*Matthes*, § 248, Rn. 33.
[71] *BAG*, Urt. v. 23.10.1984 - 1 ABR 2/83, NZA 1985, 224; Richardi/*Thüsing*, § 94, Rn. 58 m.w.N.
[72] Richardi/*Thüsing*, § 94, Rn. 73 m.w.N.

b. 2. Projektphase: Auswertung der Tests mittels Einführung von Personalfragebögen

Nach der Durchführung der Tests soll in einer zweiten Projektphase ermittelt werden, ob unter den Teilnehmern, beispielsweise je nach Berufsgruppe, Altersklasse oder Geschlecht, ein unterschiedliches IT Sicherheitsbewusstsein besteht. Da diese Daten nicht mit den Tests erhoben wurden, muss entweder eine gesonderte Erhebung erfolgen oder auf einen existierenden Datenbestand zurückgegriffen werden.

Tatsächlich sind alle oben genannte Daten als Personaldaten beim UKSH als Arbeitgeber hinterlegt. Allerdings ist eine Zuordnung zu den Testergebnissen aus datenschutzrechtlichen Gründen nicht ohne Weiteres zulässig, da sie ursprünglich für einen anderen Zweck erhoben wurden (Zweckbindungsgrundsatz). Rechtlich zulässig ist eine Zuordnung vielmehr nur dann, wenn diesbezüglich eine Einwilligung der Arbeitnehmer eingeholt wird.[73] Entscheidet man sich für die Zuordnung der Testergebnisse zu den bereits existierenden Personaldaten, ist der Betriebsrat nicht zu beteiligen.

Sollten die Daten jedoch separat über einen Fragebogen erhoben werden, könnte ein Mitbestimmungsrecht des Betriebsrats bestehen. Denn nach § 94 Abs. 1 S. 1 BetrVG ist dieser bei der Verwendung von sog. Personalfragebögen zu beteiligen. Das sind Formulare, mittels derer Informationen über persönliche Verhältnisse des Arbeitnehmers wie Geschlecht und Alter erhoben werden.[74] Da ebendiese Daten gesammelt werden sollen, würde es sich um Personalfragebögen und damit um eine mitbestimmungspflichtige Maßnahme handeln. Das Mitbestimmungsrecht erstreckt sich allerdings nicht auf die Frage, ob das Personal überhaupt mittels Fragebogen befragt wird, sondern lediglich darauf, wie er inhaltlich ausgestaltet sein soll.[75]

c. 3. Projektphase: Schulungen

In einer dritten Projektphase finden Schulungen der Mitarbeiter statt, um ihr IT Sicherheitsbewusstsein zu verbessern. Diesbezüglich könnte ein Mitbestimmungsrecht des Betriebsrates nach § 98 Abs. 1 BetrVG bestehen, wenn es sich bei den Schulungen um Maßnahmen der betrieblichen Berufsbildung handelt. Dann müssten in den Schulungen Kenntnisse vermittelt werden, die der einzelne Arbeitnehmer für die Erledigung der

[73] Siehe bereits D. II. 3.
[74] *BAG*, Urt. v. 21.9.1993- 1 ABR 28/93, NZA 1994, 375; Richardi/*Thüsing*, § 94 Rn. 6; Düwell/*Kreuder*, § 94, Rn. 9.
[75] Richardi/*Thüsing*, § 94, Rn. 30, 32-33, 35.

arbeitsplatzspezifischen Aufgaben benötigt.[76] Zu den Aufgaben eines jeden Arbeitnehmers gehört der sichere Umgang mit den Betriebsmitteln.[77] Mit Hilfe der Schulungen sollen Kenntnisse im Bereich der IT Sicherheit vermittelt werden, die für eine sichere Verwendung der Betriebsmittel erforderlich sind. Außerdem sollen an den Schulungen nur solche Mitarbeiter teilnehmen, deren Aufgaben (auch) mittels IT gestützter Betriebsmittel erledigt werden, sodass die vermittelten Kenntnisse auch für ihre spezifische berufliche Tätigkeit erforderlich sind. Somit handelt es sich bei den Schulungen um Maßnahmen der Berufsbildung im Sinne des § 98 Abs. 1 BetrVG.

Darüber hinaus müsste es sich bei den Schulungen um innerbetriebliche Maßnahmen handeln. Eine solche liegt vor, wenn der Arbeitgeber Veranstalter oder Träger der Maßnahme ist.[78] Im Projekt sind zwar Dritte an der der Erstellung und Durchführung der Schulungen beteiligt, aber gleichermaßen auch das UKSH in Gestalt der Stabsstelle Informationstechnologie (siehe TAP 6.4.4 sowie TAP 6.4.5). Mithin ist das UKSH selbst Veranstalter der Schulungen, sodass eine innerbetriebliche Bildungsmaßnahme vorliegt.

Hinsichtlich der Durchführung der Schulungen besteht daher ein Mitbestimmungsrecht des Betriebsrats. Es umfasst lediglich die Modalitäten der Durchführung. Kein Mitbestimmungsrecht besteht dahingehend, ob überhaupt Schulungen durchgeführt werden.[79] Diesbezüglich besteht lediglich ein Beratungsrecht des Betriebsrats (§ 97 Abs. 1 BetrVG).

Zusätzlich besteht auch ein Vorschlagsrecht des Betriebsrats bei der Auswahl der Arbeitnehmer, die an den Schulungen teilnehmen sollen (§ 98 Abs. 3 BetrVG).[80]

d. 4. Projektphase: Erneute Durchführung der Tests

Im Anschluss an die Schulungen werden die Mitarbeiter erneut getestet, um festzustellen, ob bei ihnen eine Veränderung des IT Sicherheitsbewusstseins eingetreten ist. Hinsichtlich dieser erneuten Testdurchführung besteht ein Mitbestimmungsrecht des Betriebsrats aus § 87 Abs. 1 Nr. 6 BetrVG im oben beschriebenem Umfang.

2. Informationsrechte

Neben Mitbestimmungsrechten können einem Betriebsrat auch Informationsrechte zustehen. Im vorliegenden Fall könnte sich ein solches aus § 80 Abs. 2 BetrVG ergeben. Nach dieser

[76] *BAG*, Beschl. v. 10.2.1988 - 1 ABR 39/86, BAGE 57, 295; Richardi/*Thüsing*, § 98 Rn. 11.
[77] Düwell/*Kreuder*, § 96, Rn. 5 m.w.N.
[78] Siehe hierzu auch: Raab, NZA 2008, 270, 272.
[79] Düwell/*Kreuder*, § 98, Rn. 2, 9; Richardi/*Thüsing*, § 98, Rn. 13; *Raab*, NZA 2008, 270 (272); *BAG*, Beschl. v. 24.8.2004 - 1 ABR 28/03, NZA 2005, 371 (373 f.).
[80] Richardi/*Thüsing*, § 98, Rn. 57.

Norm hat der Betriebsrat das Recht, all diejenigen Informationen vom Arbeitgeber zu Verfügung gestellt zu bekommen, die er zur Wahrnehmung seiner Aufgaben benötigt. Zu diesen Aufgaben gehört es, nach § 80 Abs. 1 Nr. 1 BetrVG zu überwachen, ob arbeitnehmerschützende Gesetze eingehalten werden, mithin auch, ob im Rahmen des Projekts die datenschutzrechtlichen Vorschriften eingehalten werden.[81] Außerdem ist die Wahrnehmung der Mitbestimmungsrechte einschließlich der Entscheidung, ob solche vorliegen, als Aufgabe des Betriebsrats im Sinne der Norm erfasst.[82] Da vom Projekt sowohl datenschutzrechtliche Belange betroffen sind, als auch Mitbestimmungsrechte bestehen, hat eine Information des Betriebsrats zu erfolgen. Wichtig ist, dass sie rechtzeitig erfolgt, d.h. der Betriebsrat ausreichend Zeit hat, sich mit den Angelegenheiten zu befassen. Das ist nur dann der Fall, wenn er noch auf den Ausgang der Entscheidung Einfluss nehmen und sich alle dafür eventuell nötigen Informationen beschaffen kann.[83] Außerdem müssen die Informationen inhaltlich so umfassend sein, dass der Betriebsrat die für die Wahrnehmung seiner Aufgaben erforderliche Kenntnis erhält.[84]

3. Zusammenfassung

Bei der Durchführung des ITS.APT-Projekts ist der Betriebsrat umfassend zu beteiligen. Mitbestimmungsrechte bestehen bezüglich des ersten Tests der Mitarbeiter zum einen gemäß § 87 Abs. 1 Nr. 6 BetrVG (Mitbestimmung bzgl. Einführung und Anwendung) als auch nach § 94 Abs. 2 Hs. 2 BetrVG (Mitbestimmung bzgl. des Inhalts der Bewertungsmaßstäbe). Bei der Ausgestaltung der Personalfragebögen ist der Betriebsrat inhaltlich zu beteiligen (§ 94 Abs. 1 S. 1 BetrVG), ebenso bei den Schulungen (§ 98 Abs. 1 BetrVG). Bei letzteren besteht bereits ein Beratungsrecht hinsichtlich ihrer Einführung nach § 97 Abs. 1 BetrVG. Ferner hat er ein Vorschlagsrecht bei der Auswahl der Schulungsteilnehmer (§ 98 Abs. 3 BetrVG). Die zweite Testdurchführung ist wiederum nach § 87 Abs. 1 Nr. 6 BetrVG mitbestimmungspflichtig.

Des Weiteren ist der Betriebsrat inhaltlich und zeitlich so zu informieren, dass er seine Mitbestimmungsrechte wahrnehmen kann und das Einhalten der datenschutzrechtlichen Vorschriften überprüfen kann.

---

[81] *Zimmer*/*Heymann*, BB 2010, 1853 (1855); Düwell/*Kohte/Schulze-Doll*, § 80, Rn. 22.
[82] *BAG*, Beschl. v. 8.6.1999 – 1 ABR 28/97, NZA 1999, 1345 (1346); *Hanau*/*Hoeren*, S. 90 ff.; Düwell/*Kohte/Schulze-Doll*, § 80 Rn. 47.
[83] *BAG*, Beschl. vom 17.3.1987 - 1 ABR 59/85, NZA 1987, 747 (750).
[84] *Richardi*/Thüsing, § 80, Rn. 62.

II. Beteiligungsrechte des Personalrats nach dem MBG S-H

Im Folgenden werden nun die Mitbestimmungs- und Informationsrechte der Personalräte des UKSH im ITS.APT-Projekt erörtert. Für das UKSH als Anstalt des öffentlichen Rechts bestimmen sich die Rechte des Personalrats nach dem MBG S-H.

1. Mitbestimmungsrechte

Die Struktur des MBG S-H unterscheidet sich hinsichtlich der Beteiligungsrechte der Personalvertretungen erheblich von der des BetrVG. Das MBG S-H enthält keinen enumerativen Katalog mitbestimmungspflichtiger Maßnahmen. Vielmehr richten sich die Mitbestimmungsrechte des Personalrats nach dem Grundsatz der „modifizierten Allzuständigkeit“ (§§ 51 Abs. 1, 2 MBG S-H).[85] Das bedeutet, dass der Personalrat bei allen personellen, sozialen, organisatorischen und sonstigen innerdienstlichen Maßnahmen mitbestimmt, die die Arbeitnehmern der Dienststelle insgesamt, Gruppen von ihnen oder einzelne Arbeitnehmer betreffen oder sich auf sie auswirken und auf eine Veränderung des bestehenden Zustandes abzielen.[86] Die mit dem Projekt einhergehenden Veränderungen im Betrieb zielen auf eine Einwirkung auf die Arbeitnehmer ab, indem deren IT Sicherheitsbewusstsein gemessen und anschließend verbessert werden soll. Das gesamte Projekt bezweckt eine Verbesserung der IT Sicherheit im UKSH und stellt aufgrund dieser dienststelleninternen Auswirkung auch einen innerdienstlichen Sachverhalt dar.[87] Der Personalrat ist daher im Rahmen der Projektdurchführung umfassend zu beteiligen.

Um die Rechte der Personalräte im konkreten Fall wahren zu können, ist aber, über diese pauschale Feststellung hinaus, eine Konkretisierung der Allzuständigkeit auf einzelne Maßnahmen innerhalb des Projekts erforderlich. Fraglich ist daher, welche Maßnahmen genau mitbestimmungspflichtig sind. Das Prinzip der Allzuständigkeit legt die Vermutung nahe, dass damit jedenfalls alle oben im Rahmen des BetrVG genannten mitbestimmungspflichtigen Maßnahmen auch nach dem MBG Schl. H. mitbestimmungspflichtig sind.

Diese Vermutung wird zum einen durch die Gesetzesbegründung zu § 51 MBG S-H gestützt, in der zur Bestimmung mitbestimmungspflichtiger Maßnahmen auf das Gesetz von 1982 verwiesen wird.[88] Dort sind beispielsweise die Aufstellung von Beurteilungs- und

[85] *Kersten*, RdA 2001, 23 (24).
[86] *Donalies/Hübner-Berger*, § 51, Ziff. 1.4.
[87] Zum Merkmal des innerdienstlichen Sachverhalts siehe *Donalies/Hübner-Berger*, § 51, Ziff. 1.6.
[88] LT-Drs. Schl.H. 12/996, insb. S. 106ff.

Bewertungsgrundsätzen, die Regelung der Ordnung in der Dienststelle und des Verhaltens der Mitarbeiter sowie die Festlegung der Methoden der Arbeitsüberwachung als mitbestimmungspflichtig aufgeführt. Der Wille des Gesetzgebers war es daher, diese Maßnahmen auch weiterhin der betrieblichen Mitbestimmung zu unterwerfen.

Auch der Wille des Bundesgesetzgebers[89] spricht für ein Mitbestimmungsrecht hinsichtlich dieser Maßnahmen. Nach § 104 S. 1 Hs. 2 BPersVG soll nämlich in den Bundesländern, bezogen auf Mitbestimmungsrechte des Personalrats, eine Regelung angestrebt werden, wie sie im BPersVG festgelegt ist. Dort werden mitbestimmungspflichtige Maßnahmen, ähnlich ausdifferenziert wie im BetrVG, aufgelistet. Mitbestimmungspflichtig sind nach § 75 Abs. 3 BPersVG beispielsweise die Durchführung der Berufsausbildung bei Arbeitnehmern (Nr. 6), die Auswahl der Teilnehmer an Fortbildungsveranstaltungen für Arbeitnehmer (Nr. 7), Inhalte von Personalfragebögen für Arbeitnehmer (Nr. 8), Beurteilungsrichtlinien für Arbeitnehmer (Nr. 9) und die Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmern zu überwachen (Nr. 17).

Legt man die Allzuständigkeit des § 51 MBG S-H im Lichte der Gesetzesbegründung und der Vorgabe des § 104 S. 1 Hs. 2 BPersVG aus, sind die nach dem BetrVG mitbestimmungspflichtigen Maßnahmen auch nach dem MBG S-H mitbestimmungspflichtig. Da über die oben genannten Maßnahmen hinaus keine anderen Maßnahmen geplant sind, ist der Personalrat in gleichem Umfang und in gleicher Weise wie der Betriebsrat zu beteiligen.

2. Informationsrechte

Auch dem Personalrat stehen zur Wahrnehmung seiner Aufgaben Informationsrechte zu. Er ist gemäß § 52 Abs. 2 S. 1, 2 MBG S-H sowie gemäß § 49 Abs. 1 MBG S-H über die Angelegenheiten zu informieren, die seine Mitbestimmungsrechte betreffen. Die oben aufgezeigten Grundsätze zum Informationsrecht nach dem BetrVG gelten hier entsprechend, d.h. der Personalrat ist umfassend und rechtzeitig zu informieren, sodass er ausreichend Zeit hat, sich mit dem Thema zu beschäftigen.[90]

[89] Dieser Wille ist auch weiterhin beachtlich. Der Bund hatte nämlich vor der Föderalismusreform aus der Rahmengesetzgebungskompetenz nach Art. 75 Abs. 1 Nr. 1 GG a.F die Kompetenz allgemeine Vorgaben zu mitbestimmungspflichtigen Maßnahmen zu erlassen. Das drauf basierende Recht gilt nach Art. 125a Abs. 1 GG fort, in diesem Fall die §§ 94 ff. BPersVG.

[90] Vgl. *Donalies/Hübner-Berger*, § 52, Ziff. 2.2.

3. Zusammenfassung

Die Personalräte im UKSH sind daher im gleichen Umfang und in gleicher Weise zu beteiligen und zu informieren wie die Betriebsräte.

III. Empfehlungen zur Wahrung der Mitbestimmungsrechte

Nachdem festgestellt wurde, dass die Mitarbeitervertretungen diverse Informations- und Mitbestimmungsrechte haben, stellt sich die Frage, welche Schritte vom Konsortium zu unternehmen sind, um diese Rechte zu wahren.

Hinsichtlich der Informationsrechte ist für die rechtmäßige Durchführung des Projekts zu empfehlen, die Mitarbeitervertretungen so früh wie möglich, spätestens mit Abschluss der Planungsphase, über das gesamte Projekt zu unterrichten. Sie sollten zudem vor jeder neuen Projektphase über den aktuellen Stand informiert werden.

In Bezug auf die Mitbestimmungsrechte reicht theoretisch eine formlose Absprache aus.[91] Vorzugswürdig ist jedoch eine schriftliche Betriebsvereinbarung zwischen Arbeitgeber und dem Betriebsrat bzw. eine Dienstvereinbarung zwischen Arbeitgeber und Personalrat. Diese gewährleistet durch ihre schriftliche Fixierung mehr Rechtssicherheit und kann gleichzeitig als datenschutzrechtliche Erlaubnisnorm dienen.[92] Im Ergebnis muss daher vor Durchführung der Tests eine Betriebs- bzw. Dienstvereinbarung abgeschlossen werden, die, so detailliert wie möglich, die ausgehandelten Ergebnisse hinsichtlich aller Mitbestimmungsrechte fixiert.

[91] *Richardi*, § 87, Rn. 527; Richardi/*Thüsing*, § 94, Rn. 43, 69, § 98, Rn. 17; Düwell/*Kohte*, § 87, Rn. 24.
[92] Vgl. hierzu oben Arbeitnehmerdatenschutz, insb. S. 23 ff.

IV. Tabellarische Übersicht zur betrieblichen Mitwirkung

		Betriebsrat	Personalrat
MITBESTIMMUNG	**Tests** (vor der Schulung)	**§ 87 I Nr. 6 BetrVG**: Mitbestimmung hinsichtlich der Einführung und Anwendung technischer Einrichtungen zur Überwachung des Verhaltens **§ 94 II 2. Hs. BetrVG**: Mitbestimmung hinsichtlich der inhaltlichen Ausgestaltung allgemeiner Beurteilungsgrundsätze, die in die Konstruktion der Tests einfließen	**§ 51 Abs. 1, 2 MBG S-H:** Mitbestimmung hinsichtlich aller personellen, sozialen, organisatorischen und sonstigen innerdienstlichen Maßnahmen (Allzuständigkeit)
	Personal-fragebögen	**§ 94 I 1 BetrVG**: Mitbestimmung hinsichtlich der inhaltlichen Ausgestaltung von Fragebögen	
	Schulungen	**§ 98 I BetrVG:** Mitbestimmung hinsichtlich der inhaltlichen Ausgestaltung von Maßnahmen der betrieblichen Berufsbildung	
	Tests (nach der Schulung)	**§ 87 I Nr. 6 BetrVG:** (s.o.)	
INFORMATION	**Tests** (vor der Schulung)	**§ 80 Abs. 2 BetrVG**: Rechtzeitige und umfassende Unterrichtung, damit ihm die Durchführung seiner Aufgaben möglich ist	**§ 49 Abs. 1 MBG S-H**: Rechtzeitige, umfassende und fortlaufende Unterrichtung hinsichtlich aller Angelegenheiten, die sich auf die Arbeitnehmern auswirken **§ 52 Abs. 2 MGB Schl.-H.**: (Begründete) Unterrichtung durch die Dienststellenleitung hinsichtlich der beabsichtigten Maßnahme
	Personal-fragebögen		
	Schulungen		
	Tests (nach der Schulung)		
BERATUNG / VORSCHLAG	**Schulungen**	**§ 97 Abs. 1 BetrVG:** Beratungsrecht hinsichtlich der Durchführung von betrieblichen Berufsbildungsmaßnahmen **§ 98 Abs. 3 BetrVG**: Vorschlagsrecht hinsichtlich der Teilnahme bestimmter Arbeitnehmer an den Schulungen	

F. Interessenabwägung zwischen dem Allgemeinen Persönlichkeitsrecht des Arbeitnehmers und dem Interesse des Arbeitgebers an einer verbesserten Sicherheit informationstechnischer Systeme in kritischen Infrastrukturen

Die Betriebs- bzw. Dienstvereinbarung unterliegt ihrerseits Schranken. Der Inhalt der Vereinbarungen muss also erneut anhand bestimmter Normen auf seine Rechtmäßigkeit hin überprüft werden. Gemäß § 75 Abs. 2 BetrVG haben Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb Arbeitnehmern Arbeitnehmer zu schützen und zu fördern. Nach § 1 Abs. 2 MBG S-H sollen Dienststelle und Personalrat eng und gleichberechtigt unter Beachtung der Gesetze zusammenarbeiten, um den Grundrechten der in der Dienststelle tätigen Arbeitnehmern zu praktischer Wirksamkeit im Arbeitsleben zu verhelfen. Betriebs- und Dienstvereinbarungen müssen also die grundrechtlich geschützten Rechte der Arbeitnehmer ausreichend berücksichtigen.[93] Im Projektszenario kommen vor allem das Allgemeine Persönlichkeitsrecht der Arbeitnehmer aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG in Betracht. Diese werden ausreichend berücksichtigt, wenn sie unter Abwägung mit dem berechtigten Interesse des Arbeitgebers an einer verbesserten Sicherheit informationstechnischer Systeme in kritischen Infrastrukturen nicht unverhältnismäßig eingeschränkt werden.[94]

Dazu müssen die Maßnahmen im Rahmen des Projekts einem legitimen Zweck dienen, geeignet, erforderlich und angemessen sein. Um dies zu erreichen, sollen in einem ersten Schritt Prinzipien herausgearbeitet werden, die von der Rechtsprechung und der Literatur in vergleichbaren Überwachungsszenarien entwickelt wurden. Speziell die Telefon- und E-Mail-Überwachung am Arbeitsplatz sowie Testkäufe sind mit der zu beurteilenden Situation komparabel, da diesen wegen des elektronischen und heimlichen Vorgehens die gleiche Gefährdung für das Allgemeine Persönlichkeitsrecht inne wohnt.[95] In einem zweiten Schritt sollen diese grundsätzlichen Wertungen auf das Testszenario übertragen werden, um

[93] *Richardi*, § 77, Rn. 100-102; *BAG*, Beschl. vom 26.8.2008 - 1 ABR 16/07, BAGE 127, 276; *BAG*, Urt. v. 12.12.2006 - 1 AZR 96/06, BAGE 120, 308.

[94] *BAG*, Urt. v. 11.720.00 - 1 AZR 551/99, BAGE 95, 221; *BAG*, Beschl. v. 26.8.2008 - 1 ABR 16/07, BAGE 127, 276; *Linsenmaier*, RdA 2008, 1 (8 f.).

[95] Glögem/Preis/*Schmidt*, Art. 2 GG, Rn. 43; *BVerfG*, Urt. v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, MMR 2008, 315; *BAG*, Urt. v. 29.10.1997 - 5 AZR 508–96, NJW 1998, 1331.

abschließend zu beurteilen, unter welchen Voraussetzungen die Betriebs- und Dienstvereinbarungen verhältnismäßig sind. Denn erst dann stellt sie eine wirksame Rechtsgrundlage für die Datenerhebung und -verarbeitung dar und erfüllt die Anforderungen, die an die betriebliche Mitwirkung gestellt werden.

I. Vorhandene Überwachungs- und Kontrollmethoden im Arbeitsverhältnis

Zunächst soll hier die Überwachung der dienstlichen Telefonkommunikation dargestellt werden. Historisch gesehen stellte dies die erste Möglichkeit dar, die Arbeitnehmer elektronisch und heimlich zu überwachen. Die rechtlichen Grundsätze zum Schutz der Angestellten wurden daher bereits bei der Telefonüberwachung entwickelt und dann auf neue Kommunikationstechniken, insbesondere den E-Mail-Verkehr, übertragen. Die Beurteilung von dessen rechtmäßiger Überwachung wird demzufolge anschließend an die Telefonüberwachung dargestellt. Zuletzt wird auf Testkäufe eingegangen.

1. Überwachung der betrieblichen Telefonkommunikation

In der Regel steht jedem Mitarbeiter ein Telefonapparat oder auch ein Mobiltelefon für die dienstliche Nutzung zur Verfügung. Um einem möglichen Missbrauch der Telefonnutzungsmöglichkeit entgegenzuwirken, hat der Arbeitgeber ein Interesse zu erfahren in welchem Umfang und zu welchem Zweck seine Angestellten telefonieren.[96] Außerdem hat er häufig ein Interesse an den Inhalten der dienstlichen Gespräche, um sich beispielsweise in einer bestimmten Angelegenheit auf den aktuellen Stand zu bringen.[97] Rechtlich sind diese Interessen durch seine Berufsfreiheit aus Art. 12 GG und sein Eigentumsrecht aus Art. 14 GG geschützt.[98]

Bei der Überwachung der Telefonkommunikation sind aber auch die Interessen der betroffenen Mitarbeiter zu beachten. Wenn der Arbeitgeber die Verkehrsdaten einsieht oder den konkreten Inhalt eines Gesprächs mithört, stellt dies ein Eingriff in das Allgemeine Persönlichkeitsrecht des Arbeitnehmers aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar.[99]

---

[96] *Mengel*, BB 2004, 1445 (1447); *Versteyl*, NZA 1987, 7.
[97] Hoeren/Sieber/Holznagel/*Elschner*, 22.1, Rn. 168; *Mengel*, BB 2004, 1445 (1447).
[98] *BVerfG*, Urt. v. 10.6.2009 – 1 BvR 706, 814, 819, 832, 837 f., NJW 2009, 2033; *Richardi*, § 12, Rn. 64; *Altenburg/v. Reinersdorff/Leister*, MMR 2005, 135 f.
[99] *BVerfG*, Beschl. v. 9.10.2002 – 1 BvR 805/98, NJW 2002, 3619 für Mithöreinrichtungen; *BAG*, Urt. v. 29.10.97 – 5 AZR 508/96, NZA 1998, 307; auf europäischer Ebene hat der EGMR entsprechend festgestellt, dass die Telefonüberwachung in den Schutzbereich vom Art. 8 EMRK fällt, siehe *EGMR*, Urt. v. 25.6.1997 – 20605/92 (Halford/GB); Urt. v. 2.8.1984 - 8691/79 (Malone/GB).

Dabei kann sowohl das Recht auf informationelle Selbstbestimmung[100] als auch das Recht am eigenen Wort betroffen sein.[101] Bei einer technischen Überwachung ist der Eingriff zudem besonders intensiv, da der Betroffene diesen nicht ohne weiteres erkennen kann und seine Abwehrmöglichkeiten daher begrenzt sind.[102] In vielen Fällen liegt zusätzlich ein Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG vor. Dieses schützt neben dem Kommunikationsinhalt auch die näheren Umstände der Kommunikation. Darunter fällt beispielsweise die Information über die Kommunikationspartner oder die Länge des Gesprächs.[103] Für die Zulässigkeit einer solchen Überwachung muss daher das Interesse des Arbeitgebers mit den Interessen des Arbeitnehmers im konkreten Einzelfall im Sinne praktischer Konkordanz abgewogen werden.[104]

Entscheidend ist dabei zum einen, ob dem Arbeitnehmer die private Nutzung der dienstlichen Telefone erlaubt ist oder nicht. Denn im ersten Fall hat er eine höhere Erwartung an den Schutz seiner Privatsphäre.[105] Zum anderen ist danach zu differenzieren, welche Art von Daten überwacht wird, da diese eine unterschiedliche Persönlichkeitsrelevanz aufweisen können.[106]

a. Verbot der privaten Nutzung

In einem ersten Schritt soll hier das Szenario untersucht werden, in dem die private Nutzung verboten ist.

[100] Zum Recht der informationellen Selbstbestimmung siehe *BVerfG*, Urt. v. 15.12.1983 – 1 BvR 209/83, NJW 1984, 419; für den grundrechtlichen Bezug des Datenschutzes siehe *BVerfG*, Urt. v. 27.6.1991 – 2 BvR 1493/89, DStR 1991, 971 (973); vgl. auch *Mengel*, BB 2004, 1445 (1447).

[101] *BVerfG*, Beschl. v. 19.12.1991 – 1 BvR 382/85, NJW 1992, 815; *BAG*, Urt. v. 29.10.1997 – 5 AZR 508/96, AP BGB § 611 Persönlichkeitsrecht Nr. 27; Schaub/*Linck* , § 3, Rn. 7; Moll/*Dendorfer*, § 35, Rn. 184; Richardi/Wlotzke/Wißmann/Oetker/*Reichold*, § 86, Rn. 10; *Dannhorn/Mohnke*, AuA 2006, 210 (211); *Ernst*, NZA 2002, 585 (589).

[102] *BVerfG*, Beschl. v. 3.3.2004 - 1 BvF 3/92, BVerfGE 110, 33; *Puschke/Singelnstein*, NJW 2005, 3534 (3535); *Richardi*, § 87, Rn. 480, 483.

[103] BVerfG, Urt. v. 2.3.2006 - 2 BvR 2099/04, BVerfGE 115, 166, NJW 2006, 976; Paal/*Gersdorf*, Art. 10 GG, Rn. 14; Maunz/Dürig/*Durner*, Art. 10 GG, Rn. 86.

[104] *BAG*, Beschl. v. 27.5.1986 – 1 ABR 48/84, NZA 1986, 643 (647); Hoeren/Sieber/Holznagel/*Elschner*, 22.1, Rn. 167; zur Notwendigkeit einer Einzelfallabwägung auf EU-Ebene: *EGMR*, 05.10.10 – 420/07 (Köpke/Deutschland).

[105] *BAG*, Beschl. vom 27.5.1986 - 1 ABR 48/84, NZA 1986, 643; Moll/*Dendorfer*, § 35, Rn. 188; *Mengel*, 7, Rn. 15; dies ergibt sich im Übrigen auch aus den Vorgaben des Europarechts: *EGMR*, Urt. v. 25.6.1997 - 20605/92 (Halford/GB), Rn. 45; Urt. v. 3.4.2007 - 62617/00 (Copland/GB), Rn. 42; Urt. v. 12.1.2016 - 61496/08 (Bărbulescu/Rumänien), Rn. 39.

[106] *EGMR*, Urt. v. 2.8.1984 - 8691/79 (Malone/GB), Rn. 84; Urt. v. 3.4.2007 - 62617/00 (Copland/GB), Rn. 43; ARTIKEL 29 – Datenschutzgruppe 2002, 5401/01/DE/endg. WP 55, S. 22 f., abrufbar unter: www.ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_de.pdf (zuletzt abgerufen am 16.03.16); Thüsing/*Traut*, § 10, Rn. 2.

aa. Einfache Verkehrsdaten

Verkehrsdaten sind nach § 3 Nr. 30 TKG solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Dazu zählen beispielsweise Angaben über Uhrzeit, Dauer oder beteiligte Nummern des Kommunikationsvorgangs. Obwohl sie in der Regel konkreten Mitarbeitern zuordenbar sind,[107] darf der Arbeitgeber die Daten überwachen.[108] Der Grund liegt darin, dass er, aufgrund des Verbots der privaten Nutzung, davon ausgehen darf, lediglich Informationen über dienstliche Belange, nicht aber über private, zu erhalten.[109]

bb. Vollständige Zielrufnummernerfassung

Besonderheiten ergeben sich, wenn der Arbeitgeber die vollständige Zielrufnummer erfasst. Mit ihrer Hilfe kann der jeweilige Gesprächspartner identifiziert werden, was zu einer erhöhten Persönlichkeitsrelevanz dieses Datums und daher zu einer stärkeren Gewichtung der Rechte des Arbeitnehmers führt.[110] Beispielsweise kann die Information, dass der Arbeitnehmer die Nummer eines Arztes angerufen hat, Anlass zu Zweifeln über seinen Gesundheitszustand geben. Dennoch ist auch in diesem Fall davon auszugehen, dass der Arbeitgeber lediglich Informationen über dienstliche Kommunikationspartner, nicht aber über private erhält. Außerdem würde sich der Arbeitnehmer vertragsbrüchig verhalten, sollte er, entgegen des Verbotes, die Telefone privat nutzen und wäre daher weniger schutzwürdig.[111] Demzufolge geht die Rechtsprechung, trotz der erhöhten Persönlichkeitsrelevanz, davon aus, dass die komplette Zielrufnummer erhoben werden darf.[112]

cc. Inhaltsdaten

Hört der Arbeitgeber Gespräche mit, kann er vertrauliche Informationen erlangen, wenn der Arbeitnehmer etwa mit seinem Partner über sein erkranktes Kind spricht. Inhaltsdaten können

[107] *BAG*, Beschl. v. 27.5.1986 - 1 ABR 48/84, BAGE 52, 88; vgl. auch Art. 2 lit. b RL 2002/58.
[108] *ArbG Frankfurt a.M.*, Urt. v. 2.1.2002 – 2 Ca 5340/01, NZA 2002, 1093; Thüsing*/Traut*, § 10, Rn. 2; Moll/*Dendorfer*, § 35, Rn. 189; *Mengel*, Kapitel 7, Rn. 16.
[109] *ArbG Frankfurt a.M.*, Urt. v. 2.1.2002 – 2 Ca 5340/01, NZA 2002, 1093.
[110] *BAG*, Beschl. v. 27.5.1986 – 1 ABR 48/84, NZA 1986, 643; *BAG*, Urt. v. 13.1.1987 – 1 AZR 267/85, BAGE 54, 67; *LAG Niedersachsen*, Urt. v. 13.1.1998 – 13 Sa 1235/98, NZA-RR 1998, 259.
[111] *Hanau/Hoeren*, S. 61.
[112] *BAG*, Beschl. v. 27.5.1986 - 1 ABR 48/84, NZA 1986, 643; *LAG Niedersachsen*, Urt. v. 13.1.1998 – 13 Sa 1235/97, NZA-RR 1998, 259; andere Bewertungen können sich ergeben, wenn ein berechtigtes Interesse Dritter an der Geheimhaltung besteht, z.B. bei einem angestellten Psychologen: *BAG*, Urt. v. 13.1.1987 – 1 AZR 267/85, BAGE 54, 67; bei Telefonaten des Betriebsrats: *BVerwG*, Beschl. v. 28.7.1989 - 6 P 1/88, NVwZ 1990, 71; *BAG*, Urt. v. 18.1.1989 – 7 ABR 38/87, BeckRS 1989, 30729516.

also intime Umstände der persönlichen Lebensführung offenbaren. Das hat zur Folge, dass der Arbeitnehmer nochmals schutzbedürftiger ist und sein Interesse überwiegen könnte.[113]

Selbst beim Mithören dienstlicher Gespräche kann der Arbeitgeber Informationen erlangen, die Rückschlüsse auf private Angelegenheiten des Arbeitnehmers ermöglichen. Beispielsweise könnte sich ein Arbeitnehmer in einem dienstlichen Telefonat mit einem langjährigen und gut bekannten Geschäftspartner einleitend über seine Familie unterhalten. Daher kann auch bei dienstlichen Telefonaten nicht bloß die betriebliche Sphäre sondern auch die Privatsphäre des Arbeitnehmers betroffen sein.[114]

Außerdem werden Worte häufig in dem Bewusstsein geäußert, dass sie flüchtig und jederzeit korrigierbar sind.[115] Deshalb darf der Betroffene auch im Betrieb selbst bestimmen, wem er seine Worte zugänglich machen will.[116] Er kann darauf vertrauen, dass außer diesen Personen, niemand sonst die Gespräche mithört oder aufzeichnet. Demzufolge ist bereits eine Überwachung der „nur" dienstlichen Telefongespräche eines Mitarbeiters durch den Arbeitgeber grundsätzlich unzulässig.[117] Ausnahmsweise kann von einem überwiegenden Interesse des Arbeitgebers ausgegangen werden, sofern die Kontrolle dem Aufdecken von Straftaten dient, die Auswirkungen auf das Arbeitsverhältnis haben.[118] Allerdings darf der Arbeitgeber nicht anlasslos kontrollieren; er benötigt vielmehr einen konkreten und begründeten Verdacht.[119]

b. Private Nutzung erlaubt

In einem zweiten Schritt soll nun auf das Szenario eingegangen werden, in dem der Arbeitgeber die private Nutzung gestattet. In dem Fall ist davon auszugehen, dass bei einer Überwachung auch private Telefonate erfasst werden und so Informationen gewonnen werden, die Rückschlüsse auf Umstände der privaten Lebensführung zulassen. Das ist besonders vor dem Hintergrund kritisch zu betrachten, dass der Arbeitgeber durch die

[113] *Mengel*, BB 2004, 1445 (1449); *Weißberger*, NZA 2003, 1005 (1006).
[114] *BVerfG*, Beschl. v. 19.12.1991 – 1 BvR 382/85, NJW 1992, 815 (816).
[115] *BAG*, Urt. v. 29.10.1997 – 5 AZR 508/96, NZA 1998, 307; *BGH*, Urt. v. 13.10.1987 – VI ZR 83/87, NJW 1988, 1016 (1017); *Mengel*, BB 2004, 2014 (2017); *Lindemann/Simon*, BB 2001, 1950 (1952); *Gola*, MMR 1999, 322 (326); zur generellen Schutzbedürftigkeit des gesprochenen Wortes: *BVerfG* Beschl. v. 19.12.1991 – 1 BvR 382/85, NJW 1992, 815; *BVerfG*, Beschl. v. 31.01.73 – 2 BvR 454/71, BVerfGE 34, 238.
[116] *BVerfG*, Beschl. v. 19.12.1991 – 1 BvR 382/85, NJW 1992, 815 (816); *Däubler*, Rn. 347; *Mengel*, BB 2004, 1445 (1449).
[117] *Vietmeyer/Byers*, MMR 2010, 807 (809); *Oberwetter*, NZA 2008, 609 (611); *Mengel*, BB 2004, 1445 (1449); *Weißgerber*, NZA 2003, 1005 (1006).
[118] Moll/*Dendorfer*, § 35, Rn. 192; *Vietmeyer/Byers*, MMR 2010, 807 (809); *Wellhöner/Byers*, BB 2009, 2310 (2312); *Oberwetter*, NZA 2008, 609 (611); *Mengel*, BB 2004, 1445 (1449); *Lindemann/Simon*, BB 2001, 1950 (1951).
[119] Moll/*Dendorfer*, § 35, Rn. 192; *Mengel*, BB 2004, 1445 (1449).

Erlaubnis der privaten Nutzung ein schützenswertes Vertrauen bei den Arbeitnehmern dahingehend schafft, dass ihre Angelegenheiten auch privat bleiben.[120] Er eröffnet ihnen also eine Art privaten Raum.

aa. Einfache Verkehrsdaten

Aufgrund dieses privaten Raums ist, im Gegensatz zu dem Szenario in dem die private Nutzung verboten ist, bei einer Überwachung der einfachen Verkehrsdaten das Interesse des Arbeitnehmers höher zu bewerten. Darüber hinaus erscheint das Verhalten des Arbeitgebers rechtsmissbräuchlich, wenn er das selbst geschaffene, schützenswerte Vertrauen nicht hinreichend berücksichtigen würde. Daher dürfen einfache Verkehrsdaten nicht überwacht werden, wenn die private Nutzung erlaubt ist.[121] Nur bei einem begründeten Missbrauchsverdacht kann ein überwiegendes Interesse des Arbeitgebers angenommen werden, da ihm beispielsweise nicht zugemutet werden kann eine exzessive Privatnutzung des betrieblichen Telefons zu dulden.[122]

bb. Vollständige Zielrufnummer

Wenn schon die Erhebung der einfachen Verkehrsdaten bei einer verbotenen Privatnutzung unzulässig ist, muss dies erst recht für die persönlichkeitsrelevantere vollständige Zielrufnummer gelten. In der Regel überwiegt daher das Interesse des Arbeitnehmers gegenüber dem des Arbeitgebers.[123] Erst wenn ein Missbrauchsverdacht vorliegt, der nicht bereits durch eine Auswertung der einfachen Verkehrsdaten aufgeklärt werden kann, erscheint es im Einzelfall angemessen, die Zielrufnummer zu erfassen und aufzudecken.[124]

cc. Inhaltsdaten

Aufgrund der hohen Persönlichkeitsrelevanz von Inhaltsdaten, darf der Arbeitgeber schon bei einer verbotenen privaten Nutzung die dienstlichen Gespräche seiner Arbeitnehmer nicht mithören bzw. aufzeichnen. Dies muss erst recht für den Fall gelten, in dem aufgrund der erlaubten Privatnutzung die Wahrscheinlichkeit für das Mithören privater Gespräche steigt

[120] *BAG*, Urt. v. 29.10.1997 – 5 AZR 508/96, BAGE 87, 31; *Mengel*, Kapitel 7, Rn. 22.
[121] Moll/*Dendorfer*, § 35, Rn. 193; *Klengel/Mückenberger*, CCZ 2009, 81 (84); *Altenburg/v. Reinersdorff/Leister*, MMR 2005, 135; *Mengel*, BB 2004, 1445 (1451).
[122] *BAG*, Beschl. v. 27.5.1986 - 1 ABR 48/84, NZA 1986, 643; Moll/*Dendorfer*, § 35, Rn. 193; *Vietmeyer/Byers*, MMR 2010, 807 (809); *Mengel*, BB 2004, 1445 (1451).
[123] Moll/*Dendorfer*, § 35, Rn. 193; *Vietmeyer/Byers*, MMR 2010, 807 (809); Richardi/Wlotzke/Wißmann/Oetker/*Reichold*, § 86, Rn. 11; *Wellhöner/Byers*, BB 2009, 2310 (2312); *Mengel*, BB 2004, 1445 (1451); *Raffler/Hellich*, NZA 1997, 862 (863).
[124] *Panzer*, S. 246; *Wellhöner/Byers*, BB 2009, 2310 (2312).

und der Arbeitnehmer dadurch nochmals schutzwürdiger ist.[125] Ausnahmen bestehen nur dann, wenn der Arbeitgeber sich in einer Notstands- oder Notwehrlage befindet.[126] Hat er etwa den begründeten Verdacht, dass einer seiner Angestellten Straftaten begeht, überwiegt sein Interesse an der Aufklärung, sodass er in diesem Fall Gespräche mithören bzw. sogar aufzeichnen darf.[127]

2. Überwachung des betrieblichen E-Mail Kontos

In einem zweiten Schritt soll nun auf die Überwachung des betrieblichen E-Mail Kontos eingegangen werden. Wie die Telefonüberwachung, findet sie elektronisch und heimlich statt und ist daher mit den Tests im Projektszenario vergleichbar.

Außerdem stehen sich bei der E-Mail-Überwachung dieselben Interessen gegenüber wie bei der Telefonüberwachung. Auf der einen Seite verfolgt der Arbeitgeber das Ziel herauszufinden, womit seine Angestellten beschäftigt sind, auf der anderen Seite hat der Arbeitnehmer ein Interesse an einer geschützten Privatsphäre. Daher müssen auch in diesem Fall die gegenläufigen Interessen im Wege praktischer Konkordanz ausgeglichen werden.[128] Dabei wird, wie schon bei der Telefonüberwachung, zwischen erlaubter und verbotener Privatnutzung bzw. zwischen den einzelnen Daten unterschieden.[129]

a. Verbot der privaten Nutzung

aa. Verkehrsdaten

E-Mail-Verkehrsdaten, wie Sendezeit, Datengröße, oder Absender- und Empfängeradresse lassen zwar Rückschlüsse auf persönliche oder vertrauliche Umstände der privaten Lebensführung zu.[130] Der Arbeitgeber kann aber, wie bei der Überwachung der Telefonverbindungsdaten, davon ausgehen, dass er aufgrund des Verbots der privaten

[125] *BVerfG*, Beschl. v. 19.12.1991 – 1 BvR 382/85, NJW 1992, 815; Richardi/Wlotzke/Wißmann/Oetker/*Reichold*, § 86, Rn. 10; *Mengel*, BB 2004, 1445 (1451); *Weißgerber*, NZA 2003, 1005 (1006); Moll/*Dendorfer*, § 35, Rn. 194.

[126] *Wronka/Gola*, S. 8 f.; Moll/*Dendorfer*, § 35, Rn. 185; *Vietmeyer/Byers*, MMR 2010, 807 (809); *Klengel/Mückenberger*, CCZ 2009, 81 (85); *Mengel*, BB 2004, 1445 (1451).

[127] Moll/*Dendorfer*, § 35, Rn. 194; *Panzer*,S. 238.

[128] *BVerfG*, Beschl. v. 7.3.1990 – 1 BvR 266/86, BvR 913/87, BVerfGE 81, 278; *BVerfG*, Kammerbeschl. v. 6.10.2009 – 2 BvR 693/09, BVerfGK 16, 267; *Hesse*, § 72, Rn. 318; *Thüsing/Traut*, § 9, Rn. 63; *Wybitul*, NJW 2014, 3605 (3607); auf EU-Ebene ergibt sich praktisch das gleiche Verfahren, vgl. *EGMR*, Urt. v. 24.6.2004 – 59320/00 (von Hannover/Germany), Rn. 57; Urt. v. 12.1.2016 – 61496/08 (Barbulescu/Romania), Rn. 52.

[129] *Thüsing/Traut*, § 9, Rn. 42; *Mengel*, BB 2004, 2014 (2015); *Lindemann/Simon*, BB 2001, 1950 (1951); *EGMR*, Urt. v. 12.1.2016 – 61496/08 (Barbulescu/Romania); *BAG*, Urt. v. 7.7.2005 – 2 AZR 581/04, NJW 2006, 540; *LAG Niedersachsen*, Urt. v. 31.5.2010 – 12 Sa 875/09, NZA-RR 2010, 406.

[130] *EuGH*, Urt. v. 8.4.2014 – C-293/12, C495-12 (Digital Rights Ireland); Urt. v. 6.10.2015 – C362/14 (Schrems), *Korn*, HRRS 2009, 112 (112); *Ernst*, NZA 2002, 585 (590); *Vehslage*, AnwBl 2001, 145 (147).

Nutzung nur Informationen aus der dienstlichen Sphäre gewinnt.[131] Schreibt der Arbeitnehmer außerdem verbotswidrig private E-Mails, verhält er sich vertragsbrüchig und ist daher weniger schutzwürdig.[132] Demzufolge ist die Überwachung der Verkehrsdaten zulässig.[133]

bb. Inhaltsdaten

Wie bei der Telefonüberwachung dargestellt, ist die Persönlichkeitsrelevanz von Inhaltsdaten besonders hoch.[134] Daher könnte es auch in diesem Fall unzulässig sein, den Inhalt der Kommunikation zu überwachen.[135] Allerdings lag der Grund für das dortige Verbot in der sog. Flüchtigkeit des gesprochenen Wortes, die bei schriftlicher Kommunikation wegen ihrer Fixierung nicht vorliegt.[136] E-Mails sind vielmehr mit herkömmlicher Geschäftspost vergleichbar.[137] Bei dieser ist anerkannt, dass der Arbeitgeber sie lesen darf, so lange sie nicht durch Vermerke wie „vertraulich" oder „persönlich" besonders gekennzeichnet und daher offensichtlich nur für den Arbeitnehmer bestimmt ist.[138]

Außerdem sprechen die bereits bei den Verkehrsdaten angeführten Argumente für den Arbeitgeber. Er darf aufgrund des Verbots der Privatnutzung davon ausgehen, nur auf E-Mails mit geschäftlichem Inhalt zu stoßen, nicht aber auf solche mit privatem.[139] Die Möglichkeit dennoch auf private E-Mails zu stoßen, ändert nichts an der grundsätzlichen Erlaubnis, da sich der Mitarbeiter in dem Fall dem Verbot der privaten Nutzung widersetzt und sich somit vertragsbrüchig verhält. Die Überwachung von E-Mail-Inhaltsdaten ist daher bei einer verbotenen Privatnutzung erlaubt.[140]

---

[131] Siehe dazu bereits oben zur Telefonüberwachung S. 21; in Bezug auf E-Mails vgl. auch: *Thüsing/Traut*, § 9, Rn. 42; *Lindemann/Simon*, BB 2001, 1950 (1952); *EGMR*, 12.01.16 – 61496/08 (Barbulescu/Romania), Rn. 57.

[132] *ArbG Frankfurt a.M.*, Urt. v. 2.1.2002 – 2 Ca 5340/01, NZA 2002, 1093; *Thüsing/Traut*, § 9, Rn. 42; *Hanau/Hoeren*, S. 61.

[133] *Thüsing/Traut*, § 9, Rn. 42; *Thoma*, S. 139 f.; *Däubler*, Rn. 354; *Meng*el, BB 2004, 2014 (2016); *Beckschulze*, DB 2003, 2777 (2780); *Hanau/Hoeren*, S. 64 f.; *Lindemann/Simon*, BB 2001, 1950 (1952); *EGMR*, Urt. v.12.1.2016 – 61496/08 (Barbulescu/Romania).

[134] Vgl. dazu oben S.22; in Bezug auf E-Mail Inhaltsdaten vgl. auch: *Wolf/Mulert*, BB 2008, 442 (443).

[135] So im Ergebnis: *Däubler*, Rn. 351; *Ernst*, NZA 2002, 585 (589f.) – allerdings gehen sie unzutreffend von einer Vergleichbarkeit von E-Mails und mündlicher Kommunikation aus.

[136] *Thüsing/Traut*, § 9, Rn. 50; *Beckschulze*, DB 2003, 2777 (2779); *Mengel*, „Kontrolle der Email- und Internet-Kommunikation am Arbeitsplatz", BB 2004, 2014 (2017); *Mattl*, S. 140f.; *Wybitul*, NJW 2014, 3605 (3607); a.A.: *Däubler*, Rn. 351; *Ernst*, NZA 2002, 585 (589); *Raffler/Hellich*, NZA 1997, 862 (863).

[137] *Thüsing/Traut*, § 9, Rn. 50; *Wybitul*, NJW 2014, 3605 (3607); Moll/*Dendorfer*, § 35, Rn. 201; *Mengel*, BB 2004, 2014 (2016); *Beckschulze*, DB 2003, 2777 (2779); *Lindemann/Simon*, BB 2001, 1950 (1952).

[138] *LAG Hamm*, Urt. v. 19.2.2003 – Sa 1972/02, NZA-RR 2003, 346 (347); *Thüsing/Traut*, § 9, Rn. 50 f.; *Ernst*, NZA 2002, 585 (588).

[139] Vgl. oben, Fn. 131.

[140] Gola/Schomerus/*Klug*/*Körffer*, § 32, Rn. 23; *Thüsing/Traut*, § 9, Rn. 50; *Weißnicht*, MMR 2003, 448 (451); *Kömpf/Kunz*, NZA 2007, 1341 (1344); *Beckschulze*, DB 2003, 2777 (2779); *Hanau/Hoeren*, S. 54; *Gola*, MMR 1999, 322 (326); *EGMR*, Urt. v. 12.1.2016 – 61496/08 (Barbulescu/Romania).

Einschränkungen sind jedoch vorzunehmen, wenn die Ziele des Arbeitgebers bereits durch mildere und gleich effektive Maßnahmen erreicht werden können.[141] Ist der private Charakter einer E-Mail etwa schon aufgrund des Betreffs oder der E-Mail Adresse erkennbar, ist es für eine Missbrauchskontrolle nicht mehr erforderlich, die E-Mail zu lesen.[142] Aus den gleichen Erwägungen muss der Arbeitgeber vom Lesen Abstand nehmen, wenn er währenddessen bemerkt, dass er auf eine private E-Mail gestoßen ist.[143]

b. Erlaubnis der privaten Nutzung

Erlaubt der Arbeitgeber die private Nutzung des betrieblichen E-Mail Kontos, schafft er, wie bei der Erlaubnis der privaten Telefonnutzung, einen privaten Raum für den Arbeitnehmer, in dem dieser auf den Schutz seiner persönlichen Informationen vertrauen darf.[144] Gleichzeitig muss der Arbeitgeber die selbst geschaffene Privatsphäre berücksichtigen, da er sich andernfalls rechtsmissbräuchlich verhalten würde. Daher ist auch in diesem Fall die Überwachung des betrieblichen E-Mail Kontos unabhängig von der Art des Datums unzulässig.[145]

Ausnahmen gelten nur dann, wenn der Arbeitgeber den Verdacht hegt, dass der Arbeitnehmer den E-Mail-Dienst exzessiv oder zum Schaden des Arbeitgebers einsetzt.[146] Dabei gilt, dass die Verkehrsdaten wegen ihrer geringeren Persönlichkeitsrelevanz bereits bei einem einfachen Missbrauchsverdacht ausgewertet werden dürfen; Inhaltsdaten nur bei Verdacht einer Straftat oder ähnlich schwerwiegenden Vergehen.[147]

3. Testkäufe

Eine weitere, wenn auch nicht elektronische Form der heimlichen Überwachung am Arbeitsplatz, sind sog. Testkäufe, bei denen Arbeitsleistung oder -verhalten eines oder mehrerer Mitarbeiter überprüft wird. Dazu gibt sich beispielsweise ein professioneller Testkäufer als Kunde aus, um die Beratungsqualität der Mitarbeiter zu kontrollieren oder mittels inkorrekter Kassenbestände die Ehrlichkeit der Mitarbeiter bei der

---

[141] *Thüsing/Traut*, § 9, Rn. 75.
[142] *Thüsing/Traut*, § 9 Rn. 75; Moll/*Dendorfer*, § 35, Rn. 202; *Beckschulze*, DB 2003, 2777 (2780).
[143] *Hanau/Hoeren*, S. 54; *Weißnicht*, MMR 2003, 448 (451).
[144] Vgl. dazu auch oben S. 23; in Bezug auf E-Mails im Ergebnis gleich: *Joussen*, NZA-Beilage 2011, 35 (39); *Thoma*, S. 147.
[145] Simitis/*Seifert*, § 32, Rn. 92; *Thüsing/Traut*, § 9, Rn. 42; Moll/*Dendorfer*, § 35, Rn. 205; *Wolf/Mulert*, BB 2008, 442 (443); *Kömpf/Kunz*, NZA 2007, 1341 (1345); *Mengel*, 2004, 2014 (2018f.); *Gola*, MMR 1999, 322 (329).
[146] *ArbG Frankfurt a.M.*, Urt. v. 2.1.2002 – 2 Ca 5340/01, NZA 2002, 1093; *Mengel*, 2004, 2014 (2019).
[147] *ArbG Hannover*, Urt. v. 28.4.2005 – 10 Ca 791/04, NZA-RR 2005, 420; *ArbG Frankfurt a.M.*, Urt. v. 2.1.2002 – 2 Ca 5340/01, NZA 2002, 1093; Moll/*Dendorfer*, § 35, Rn. 205; *Mengel*, 2004, 2014 (2019).

Wechselgelderfassung zu prüfen.[148] Rechtlich ist das dabei verfolgte Interesse des Arbeitgebers an einem effizienten Betriebsablauf von Art. 12 GG und 14 GG geschützt.[149] Auf der anderen Seite ist die, aufgrund der Überwachung betroffene Persönlichkeit des Arbeitnehmers grundrechtlich durch sein Allgemeines Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG geschützt.[150] Für die Beurteilung der rechtlichen Zulässigkeit sind daher abermals die gegenseitigen Interessen im Wege praktischer Konkordanz in Einklang zu bringen.[151] Dazu haben Rechtsprechung und Literatur bestimmte Vorgaben entwickelt.

Zunächst ist aus Verhältnismäßigkeitsgründen eine offene Kontrolle einer heimlichen vorzuziehen.[152] Erst wenn konkrete Verdachtsmomente vorliegen oder die offene Kontrolle zwecklos bzw. nicht möglich wäre, darf sie auch heimlich erfolgen.[153] Letzteres ist regelmäßig der Fall, wenn Mitarbeiter die kontrollierte Tätigkeit alleine durchführen und eine offene Kontrolle somit wegen ihres Ausnahmecharakters sinnlos wäre,[154] beispielsweise bei einem Kassierer, der alleine Waren abkassiert.[155]

Außerdem ist es relevant, in welcher Art und in welchem Umfang die Testkäufe angekündigt wurden. Sind Kontrollen in dem Unternehmen üblich und fehlt eine Zeitangabe, lebt der Arbeitnehmer stets in der Angst, dass er sich in einer Testsituation befindet. Das kann zu einem permanenten Überwachungsdruck führen, der gravierende Auswirkungen auf die Persönlichkeit des Einzelnen hat.[156]

Weiterhin ist es unzulässig allgemeine Charaktereigenschaften oder persönliche Fertigkeiten zu überprüfen, sofern diese keinen Bezug zur vertraglich geschuldeten Arbeitsleistung haben.[157] Auch sonstige private Informationen, beispielsweise privat geführte Gespräche, dürfen nicht protokolliert werden.[158] Gegenstand der Überprüfung kann immer nur die Kontrolle der vertraglich geschuldeten Leistung sein, wobei es unerheblich ist, ob sich diese direkt aus dem Arbeitsvertrag, eventuellen Nebenbestimmungen oder individuellen

[148] *Zange*, AuA 2013, 150; *Decker/Deckers*, NZA 2004, 139; *Maschmann*, NZA 2002, 13 (16f.).
[149] *ArbG Gelsenkirchen*, Urt. v. 9.4.2009 – 5 Ca 2327/08, 5 Ca 2327/08.
[150] *BAG*, Urt. v. 18.11.1999 - 2 AZR 743/98, BAGE 93, 1, NJW 2000, 1211; *Joussen*, NZA-Beil. 2011, 35 (36); *Maschmann*, NZA 2002, 13 (14); *Ricken*, RdA 2001, 52.
[151] Richardi/Wlotzke/Wißmann/Oetker/*Wank*, § 97, Rn. 42.
[152] Zu diesem Grundsatz: *BVerfG*, Urt. v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274; bzgl. Testkäufen: *Zange*, AuA 2013, 150; *Maschmann*, NZA 2002, 13 (14f.).
[153] *Zange*, AuA 2013, 150 (151); *Maschmann*, NZA 2002, 13 (15).
[154] *BAG*, Urt. v. 18.11.1999 - 2 AZR 743/98, BAGE 93, 1, NJW 2000, 1211; *LAG Hamm*, Urt. v. 8.3.2007 – 17 Sa 1604/06; *Maschmann*, NZA 2002, 13 (14).
[155] *BAG*, Urt. v. 18.11.1999 - 2 AZR 743/98, BAGE 93, 1, NJW 2000, 1211.
[156] *ArbG Gelsenkirchen*, Urt. v. 9.4.2009 – 5 Ca 2327/08, BeckRS 2010, 74340.
[157] *Ricken*, RdA 2001, 52 (53).
[158] *Freckmann/Wahl*, BB 2008, 1904 (1907).

Arbeitsanweisungen ergibt.[159] Wird beispielsweise mittels inkorrekter Wechselgeldbestände in der Kasse die Ehrlichkeit der Mitarbeiter bei der Erfassung kontrolliert, ist Gegenstand der Untersuchung nicht die Ehrlichkeit als allgemeine Charaktereigenschaft, sondern die konkrete Arbeitsleistung, d.h. ob die Mitarbeiter ihrer vertraglich geschuldeten Pflicht, die Wechselgeldbestände richtig zu erfassen, nachgekommen sind.[160]

Schließlich gilt es zu berücksichtigen, ob mittels der Tests der Arbeitnehmer dazu verführt wird, sich vertragsbrüchig zu verhalten, beispielsweise indem ihm vom Arbeitgeber absichtlich zu viel Wechselgeld in die Kasse gelegt wird. In diesen Fällen wird dem Arbeitnehmer eine Falle gestellt, da er künstlich dazu verleitet werden soll, sich vertragsbrüchig zu verhalten.[161]. Der Arbeitgeber hätte die Pflichtverletzung dann zu einem gewissen Grad selbst mit verursacht.[162] Entscheidend für eine Rechtmäßigkeit solcher Tests ist allerdings, dass auch im regulären Arbeitsalltag Verführungssituationen entstehen können, beispielsweise weil versehentlich zu viel Wechselgeld in die Kasse gerät. Um die Verlässlichkeit seiner Mitarbeiter in solchen Fällen testen zu können, muss der Arbeitgeber zwangläufig eine vergleichbare Situation simulieren. Dass er dazu eine Falle stellt, ist unvermeidbar.[163] Für die Rechtmäßigkeit solcher Tests spricht außerdem, dass der von einem redlichen Arbeitnehmer ausgehen darf, der einer derartigen Verführung widerstehen würde.[164] Erst wenn eine Situation geschaffen wird, in der auch ein durchschnittlich rechtstreuer Arbeitnehmer vertragsbrüchig handeln würde, können solche Tests demzufolge unzulässig sein.[165]

Beachtet der Arbeitgeber diese Vorgaben, ist sein Interesse an einer Leistungskontrolle zur Verbesserung der Betriebsführung gegenüber dem Interesse des Arbeitnehmers an einem weitergehenden Schutz seiner Persönlichkeit höher zu gewichten. Testkäufe sind dann zulässig.[166]

---

[159] *BAG*, Beschl. v. 26.3.1991 - 1 ABR 26/90, NZA 1991,729; *Trappehl/Schmidl*, NZA 2009, 985 (987).
[160] *BAG*, Urt. v. 18.11.1999 - 2 AZR 743/98, BAGE 93, 1, NJW 2000, 1211; *Grobys*, NJW-Spezial 2005, 273 (274).
[161] *BAG*, Urt. v. 18.11.1999 - 2 AZR 743/98, BAGE 93, 1, NJW 2000, 1211; *Arnold*, S. 85f.
[162] *Maschmann*, NZA 2002, 13 (15); *BAG*, Urt. v. 18.11.1999 - 2 AZR 743/98, BAGE 93, 1, NJW 2000, 1211, Rn. 24.
[163] *BAG*, Beschl. v. 26.3.1991 - 1 ABR 26/90, NZA 1991, 729; *BAG*, Urt. v. 18.11.1999 - 2 AZR 743/98, BAGE 93, 1, NJW 2000, 1211; *Maschmann*, NZA 2002, 13 (16); *Ricken*, RdA 2001, 52 (53).
[164] *LAG Hamm*, Urt. v. 9.5.2005 – 8 Sa 118/04, BeckRS 2005, 42867.
[165] *Arnold*, S. 84.
[166] *BAG*, Urt. v. 18.11.1999 - 2 AZR 743/98, BAGE 93, 1, NJW 2000, 1211; *Zange*, AuA 2013, 150 (151); Moll/*Dendorfer*, § 35, Rn. 111; *Joussen*, NZA-Beil. 2011, 35 (39f.); *Ricken*, RdA 2001, 52f.; *Maschmann*, NZA 2002, 13 (21).

II. Übertragung auf das Testszenario

Nachdem die Vorgaben für die Zulässigkeit einer heimlichen und elektronischen Überwachung des Arbeitnehmers am Arbeitsplatz dargestellt wurden, sollen die dort erarbeiteten Wertungen nun auf das Testszenario übertragen werden. Ziel ist es, auf diese Weise die rechtlichen Anforderungen an die Konzeption der Tests herauszuarbeiten und so eine rechtssichere Umsetzung der ITS.APT-Lösung im UKSH zu gewährleisten. Dazu wird im Folgenden auf drei rechtliche Hürden eingegangen. Zunächst soll die heimliche Vorgehensweise problematisiert werden, gefolgt von einer Betrachtung möglicher arbeitsrechtlicher Konsequenzen für den Arbeitnehmer, falls dessen Testergebnis nicht den Erwartungen des Arbeitgebers entspricht und schließlich einer Analyse der Persönlichkeitsrelevanz der bei den Tests erhobenen Daten. Dabei werden jeweils Vorgaben für eine rechtskonforme Gestaltung der Tests gemacht, um das Persönlichkeitsrecht der Arbeitnehmer ausreichend zu berücksichtigen.

1. Heimliche Vorgehensweise

Als rechtlich herausfordernd erweist sich die heimliche Vorgehensweise. Die getesteten Arbeitnehmer wissen nicht, dass sie Testobjekt eines vermeintlichen IT Angriffs sind und ihre Reaktionen auf den Angriff erfasst werden. Dadurch sind ihre Möglichkeiten, rechtlichen Schutz zu ersuchen, stark eingeschränkt. Das führt zu einem intensiveren Eingriff, der nur durch wichtige Gründe zu rechtfertigen ist.[167]

Durch die Tests soll die Sicherheit informationstechnischer Systeme verbessert werden. Diese ermöglichen es, persönliche oder geschäftliche Angelegenheiten zu verwalten, zu bearbeiten oder zu archivieren. Außerdem bieten sie, über ihre Vernetzung, vielfältige Möglichkeiten des geschäftlichen oder persönlichen, auch intimen, Austauschs. Sie sind daher zu einem zentralen Element für die persönliche Lebensführung geworden.[168] Werden diese Systeme angegriffen, besteht die Gefahr, dass Dritte geschäftliche oder persönliche Informationen erlangen und somit die Persönlichkeitsentfaltung des Einzelnen oder die freie Unternehmensführung erheblich beeinträchtigen. Der Schutz informationstechnischer Systeme ist daher für die Freiheit und Persönlichkeit des Einzelnen unabdingbar und deshalb sogar grundrechtlich geboten.[169]

---

[167] *BVerfG*, Beschl. v. 27.2.2008, 1 BvR 370/07, 1 BvR 595, Rn. 238 ff.; ähnlich BAG, *Urt.* v. 20.6.2013 – 2 AZR 546/12 Rn. 30 ff. = NZA 2014, 143.

[168] *BVerfG*, Beschl. v. 27.2.2008 1 BvR 370/07, 1 BvR 595/07, Rn. 170 ff.; siehe auch: *Hornung*, CR 2008, 299 (302).

[169] *BVerfG*, Beschl. v. 27.2.2008 1 BvR 370/07, 1 BvR 595/07, Rn. 181, 186; Paal/*Gersdorf*, Art. 2 GG, Rn. 22.

Von besonderer Bedeutung ist der Schutz informationstechnischer Systeme in kritischen Infrastrukturen, wie beispielsweise dem UKSH.[170] Denn diese nehmen elementare Aufgaben wahr, die für ein funktionierendes und wohlfahrtförderndes soziales Zusammenleben vorausgesetzt werden.[171] Eine Schädigung ihrer IT Infrastruktur kann daher besonders gravierende Folgen haben. Dies zeigte sich beispielsweise Anfang 2016, als mehrere Krankenhäuser in Nordrhein-Westfalen aus Sicherheitsgründen ihre Systeme abschalten mussten.[172] Mit Ausnahme der Aufnahme von Notfällen, konnten diese Einrichtungen keine Personen mehr behandeln und somit ihrer Aufgabe, der Gesundheitssorge der Bevölkerung, nicht nachkommen. Um das staatliche Gemeinwesen aufrechterhalten zu können, müssen somit besonders die informationstechnischen Systeme kritischer Infrastrukturen vor Störungen durch IT Angriffe geschützt werden.[173] Eben diesem wichtigen Ziel dienen die Tests, die im UKSH durchgeführt werden sollen.

Die heimliche Vorgehensweise wäre allerdings unverhältnismäßig, wenn sie nicht notwendig wäre, ihr Zweck also auch mit milderen und gleich effektiven Mitteln erreicht werden könnte.[174] Das heimliche Vorgehen ist jedoch erforderlich, um aussagekräftige Testergebnisse zu erhalten. Wüsste der überprüfte Mitarbeiter von den anstehenden Tests, wäre seine Aufmerksamkeit bezüglich potentieller IT Angriffe um ein Vielfaches erhöht und würde nicht mehr die Realsituation widerspiegeln. Außerdem besteht dann die Gefahr, nicht bloß IT Sicherheitsbewusstsein zu testen, sondern auch, ob der Arbeitnehmer die betriebsinterne IT Arbeitsanweisung befolgt, wonach IT Angriffe in der Regel zu melden wären.[175]

---

[170] Vgl. zur Eigenschaft des UKSH als Betreiber einer Kritischen Infrastruktur TAP 2.3.

[171] Vgl. § 2 Abs. 10 BSIG, wonach Kritische Infrastrukturen Einrichtungen sind, die „den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden."; siehe auch die Gesetzesbegründung zur NIS-RL, COM (2013) 48 final, abrufbar unter http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf (zuletzt abgerufen am 17.03.16).

[172] www.computerwoche.de/a/kliniken-vs-hacker,3223442 (zuletzt abegrufen am 15.3.2016); www.spiegel.de/netzwelt/web/it-probleme-in-nrw-computervirus-legt-mehrere-krankenhaeuser-lahm-a-1077469.html (zuletzt abgerufen am 15.3.2015); www.klinikum-arnsberg.de/aktuelles-termine/meldungen-nachrichten/?no_cache=1&uid=150 (zuletzt abgerufen am 15.3.2016).

[173] www.bmi.bund.de/DE/Themen/Bevoelkerungsschutz/Schutz-Kritischer-Infrastrukturen/schutz-kritischer-infrastrukturen_node.html (zuletzt abgerufen am 15.3.2016); die Gesetzesbegründung zur NIS-RL (siehe Fn. 171) spricht von Systemen, „die für das Funktionieren unserer Gesellschaften und Volkswirtschaften unverzichtbar sind".

[174] *BVerfG*, Beschl. v. 27.2.2008, 1 BvR 370/07, 1 BvR 595/07, Rn. 225; siehe auch *BAG, Urt.* v. 21. 6.2012 − 2 AZR 153/11, NJW 2012, 3594.

[175] Vgl. hierzu auch die entsprechende Arbeitsanweisung des UKSH, die eine solche Mitteilungspflicht vorsieht.

Um dennoch einen angemessenen Interessenausgleich zu erzielen, müssen die Belange der Arbeitnehmer bei der Testdurchführung einbezogen werden. Das soll unter Berücksichtigung folgender Vorgaben geschehen: Erstens müssen die Arbeitnehmer soweit informiert werden, sodass keine bzw. nur solche Auswirkungen auf das Testergebnis zu erwarten sind, die empirisch vernachlässigbar sind. Beispielsweise könnten die Arbeitnehmer allgemein darüber informiert werden, dass die IT Sicherheit des Unternehmens demnächst getestet wird, ohne zu erwähnen, dass dabei das IT Sicherheitsbewusstsein der Arbeitnehmer gemessen wird. Zweitens müssen die Arbeitnehmervertretungen schon in der Konzeptionsphase und unabhängig von einer verpflichtenden Beteiligung nach den gesetzlichen Vorgaben des BetrVG bzw. des MBG S-H einbezogen werden.[176] Dabei müssen sie umfassend über das Vorhaben informiert werden, um auch auf kollektiver Ebene Arbeitnehmerinteressen zu berücksichtigen. Drittens müssen alle getesteten Personen transparent und umfassend aufgeklärt werden, nachdem die Tests durchgeführt wurden.[177] Ihnen muss mitgeteilt werden welche Daten erhoben wurden, zu welchem Zweck dies geschah und wer die verarbeitende Stelle ist.[178] Außerdem sind die Betroffenen über ihre Rechte zu informieren, insbesondere solche auf Zugang oder Löschen der Daten und auf ihr Recht die weitergehende Verarbeitung zu verbieten.[179]

Ebenfalls rechtlich problematisch ist in diesem Zusammenhang, dass den Arbeitnehmern durch die simulierten IT Angriffe eine Art Falle gestellt wird. Wie bei den Testkäufen wird dadurch eine künstliche Situation geschaffen, in der der Betroffene dazu verführt werden soll, sich vertragsbrüchig zu verhalten. Diese Testweise ist jedoch zulässig, wenn sie dem Arbeitgeber die einzige Möglichkeit bietet, eine Arbeitsleistung zu kontrollieren.[180] IT Sicherheitsbewusstsein lässt sich nur mit Hilfe simulierter IT Angriffe, also künstlich geschaffener Situationen, testen. Dem Arbeitnehmer muss also auch in diesem Fall eine Falle gestellt werden.

Die heimliche Vorgehensweise greift daher, unter den oben genannten Voraussetzungen, nicht unverhältnismäßig in die Rechte der Arbeitnehmer ein.

---

[176] vgl. dazu schon oben Beteiligung des Betriebs- und Personalrates, S. 7 ff.
[177] Unter anderem, um dem Arbeitnehmer die Möglichkeit zu geben, sich zu äußern, siehe: *Röckl/Fahl*, NZA 1998, 1035 (1037).
[178] Diese Pflicht des Arbeitgebers ergibt sich bereits aus § 33 BDSG, siehe dazu ausführlich: Thüsing/Pötters, § 18, Rn. 9-32.
[179] Siehe zu den Löschungspflichten: *Thüsing/Pötters*, § 11, Rn. 54 f.
[180] vgl. S. 27 ff.

2. Arbeitsrechtliche Konsequenzen

Ein wichtiger Unterschied zwischen der Überwachung der betrieblichen Telekommunikation oder der Durchführung von Testkäufen und dem Testszenario besteht in ihren unterschiedlichen Zwecken und den damit einhergehenden rechtlichen Folgen für den Arbeitnehmer. Mit Hilfe der herkömmlichen Überwachung am Arbeitsplatz soll ausschließlich die Arbeitsleistung überprüft werden.[181] Erfüllt der Arbeitnehmer dabei die Erwartungen des Arbeitgebers nicht, können arbeitsrechtliche Konsequenzen, wie negative Personalakteneinträge oder, im schlimmsten Fall, Kündigungen, folgen.[182] Mit Hilfe der Tests soll zwar mit dem IT Sicherheitsbewusstsein eine Arbeitsleistung gemessen werden, allerdings ohne dass die Option einer Sanktionierung besteht. Dem Arbeitnehmer sollen aus einem negativen Testergebnis keine arbeitsrechtlichen Konsequenzen drohen.

Um das zu gewährleisten und um generell zu verhindern, dass die erhobenen Daten missbraucht werden, müssen Zugriffe des Arbeitgebers oder Dritter unterbunden werden. Eine dabei in Betracht kommende Anonymisierung der Testergebnisse, als effektivste Form der Zugriffsbeschränkung, scheidet aber aus Gründen der Erforderlichkeit aus. Schließlich müssen die Ergebnisse des zweiten Tests denen des ersten Tests zugeordnet werden können, um aufzuklären welche Schulungsmaßnahme am effektivsten war und somit die besten Auswirkungen auf das IT Sicherheitsbewusstsein der Getesteten hatte. Eine andere Möglichkeit, dem Arbeitgeber zu verwehren die erhobenen Daten auf einzelne Person zu beziehen, ist die Daten zu pseudonymisieren. Selbstverständlich muss sich dafür der Schlüssel für die Klarnamen außerhalb des Zugriffsbereichs des Arbeitgebers befinden.[183] Dieser sollte bei einer vertrauenswürdigen und unabhängigen Stelle, wie einer Datenschutzbehörde, gespeichert werden.

3. Persönlichkeitsrelevanz

Die Darstellung bei der Telefon- und E-Mail Überwachung zeigt, dass es für die Zulässigkeit einer Überwachungsmaßnahme am Arbeitsplatz entscheidend darauf ankommt, welche Persönlichkeitsrelevanz die erhobenen Daten haben. Dabei muss sowohl zwischen den Rückschlussmöglichkeiten der gewonnen Information unterschieden werden als auch zwischen den äußeren Umständen, in dem die Information erlangt wird, mithin ob die private Nutzung erlaubt ist oder nicht.

[181] vgl. dazu ausführlich S. 20, 25 ff.
[182] Zu den möglichen Konsequenzen siehe: *Herfs-Röttgen*, NZA 2013, 478 zu Einträgen in der Personalakte; Glögem/Preis/Schmidt/*Oetker*, § 1, Rn. 188 ff. zur verhaltensbedingten Kündigung.
[183] vgl. zur Pseudonymisierung auch ausführlich oben S. 18 ff.

a. Rückschlussmöglichkeiten der gewonnen Information

Bei der Überwachung der betrieblichen Telekommunikation wurde nach Verkehrsdaten, der Zielrufnummer und Inhaltsdaten differenziert, da diese unterschiedliche Rückschlussmöglichkeiten auf Umstände der privaten Lebensführung bieten. Während die Inhaltsdaten eines Telefongesprächs selbst bei einer verbotenen privaten Nutzung nicht erhoben werden dürfen, weil dort sehr sensible persönliche Informationen gewonnen werden können, ist die Erhebung der Verkehrsdaten hingegen zulässig, weil dort die Rückschlussmöglichkeiten begrenzt sind.[184] Eine entscheidende Frage ist daher, welche Aussagekraft die bei den Tests erhobenen Daten über die Persönlichkeit der Getesteten haben. Dabei lassen sich zwei Arten von Informationen unterscheiden, die bei den Tests gewonnen werden können.

Erstens die mit Hilfe der Tests gewonnene Information, welches IT Sicherheitsbewusstsein eine Person hat. Diese Information lässt nur bedingt Rückschlüsse auf Umstände der persönlichen Lebensführung zu. Gleichwohl könnte es gegen die Zulässigkeit einer Erhebung dieser Information sprechen, wenn dadurch eine persönliche Fertigkeit überprüft wird, die nicht im Zusammenhang mit einer geschuldeten Arbeitsleistung steht. Wie bei den Testkäufen herausgestellt, kann sich das Kontrollinteresse des Arbeitgebers nur auf die vertragliche Arbeitsleistung beziehen.[185] Teil der arbeitsvertraglich geschuldeten Pflichten ist der ordnungsgemäße Umgang mit den Betriebsmitteln,[186] hier mit den informationstechnischen Systemen des Krankenhauses.[187] Zum ordnungsgemäßen Umgang mit solchen Systemen zählt insbesondere Angriffe auf sie abzuwehren bzw. nicht zu fördern.[188] Daher darf der Arbeitgeber auch kontrollieren wie die getesteten Personen auf simulierte IT Angriffe reagieren. Gegenstand der Tests ist mit anderen Worten nicht das IT Sicherheitsbewusstsein als rein persönliche Fertigkeit, sondern als Teil der Arbeitsleistung. Damit sind die Tests mit den Ehrlichkeitskontrollen bei Testkäufen vergleichbar, in denen die Ehrlichkeit der Mitarbeiter bei der Erfassung inkorrekter Wechselgeldbestände in der Kasse kontrolliert wird. Diese werden allgemein als zulässig angesehen.[189] Nichts anderes kann dementsprechend für die in diesem Fall zu beurteilenden Tests gelten.

---

[184] siehe dazu oben: S. 21 ff.
[185] siehe dazu oben S. 27 ff.
[186] Folgt aus § 241 Abs. 2 BGB, siehe Glögem/Schmidt/*Preis*, § 611, Rn. 707; siehe weiter Nachweise bei Düwell/*Kreuder*, § 96, Rn. 5; zur Arbeitnehmerhaftung i.A. Rolfs/Kreikebohm/Giesen/Udsching/*Joussen*, § 611, Rn. 366 ff.
[187] Vgl. dazu auch die Dienstanweisung des UKSH zum Internetgebrauch.
[188] Zur Schadensabwendungspflicht des Arbeitnehmers: Glögem/Schmidt/*Preis*, § 611, Rn. 744 ff.
[189] siehe dazu oben: S. 27 ff.

Zweitens können, je nach inhaltlicher Ausgestaltung der Tests, Informationen gewonnen werden, die erhebliche Rückschlüsse auf private Lebensumstände zulassen. Das zeigt sich besonders deutlich anhand des Phishing Mail Angriffsszenarios. Die bloße Information, dass ein Arbeitnehmer eine Phishing Mail mit einem bestimmten Inhalt liest, auf den Link in der Mail klickt oder sie sofort löscht, lässt Rückschlüsse auf dessen persönlichen Interessen zu. Beispielsweise kann die Reaktion einer jungen weiblichen Arbeitnehmern auf eine Phishing Mail über Familienplanung, Rückschlüsse eben darüber zulassen Ist eine Phishing Email so gestaltet, dass sie einen Link enthält, der auf Fußball, Kleidung oder Musik verweist, so lässt ein Anklicken des Links Rückschlüsse auf die Freizeitgestaltung des Arbeitnehmers zu. Insgesamt können damit sogar intimste Details aus dem Privatleben offenbart werden.

Der Vergleich zur Überwachung der betrieblichen Telekommunikation und zu Testkäufen verdeutlicht, dass der Arbeitgeber in diesem Zusammenhang keine privaten Informationen erheben darf. Sofern ihm Überwachungsbefugnisse bezüglich der Telekommunikation eingeräumt werden, basiert dies lediglich auf der Annahme, dass er in den Situationen keine privaten Informationen erlangen kann, weil ein redlicher Arbeitnehmer das Verbot der privaten Nutzung beachtet. Stößt der Arbeitgeber bei seinen erlaubten Kontrollen doch auf private Informationen, muss er die Kontrolle unverzüglich abbrechen.[190] Ähnliches gilt bei Testkäufen. Erlangt der Testkäufer private Informationen, darf er sie nicht protokollieren und an den Arbeitgeber weitergeben.[191]

Als Konsequenz muss in dem Projekt sichergestellt werden, dass die simulierten IT Angriffe keine Rückschlüsse auf Umstände der privaten Lebensführung der getesteten Personen ermöglichen. Eine Umsetzungsmöglichkeit in dem Phishing-Mail Angriffsszenario besteht in der Konstruktion inhaltlich neutraler E-Mails, beispielsweise einer Anfrage eines Systemadministrators eines Web-Mail Anbieters ein neues Passwort für den Dienst zu wählen. In dem Fall sind, neben Rückschlüssen auf das IT Sicherheitsbewusstsein, nur Rückschlüsse auf den Umstand möglich, dass die Person bei dem simulierten Anbieter ein Konto hat; nicht aber auf sensible persönliche Informationen. Eine weitere Möglichkeit die Phishing-Mails so zu konstruieren, dass sie keine dementsprechenden Rückschlüsse ermöglichen, besteht darin, unverständlichen oder sinnlosen Inhalt zu verschicken, indem beispielsweise Mails mit chinesischen oder fiktiven Schriftzeichen konstruiert werden.

[190] siehe dazu oben: S. 21 ff., 25 f.
[191] siehe dazu oben: S. 27 ff.

b. Äußere Umstände des Informationsgewinns

Die Darstellung der Überwachung der betrieblichen Telekommunikation zeigt außerdem, dass die äußeren Umstände, unter denen die Informationen gewonnen werden, also ob die private Nutzung erlaubt oder verboten ist, für die Beurteilung der Zulässigkeit maßgeblich ist. Im Projektszenario ist demzufolge zu untersuchen, ob die Unterscheidung auch in diesem Fall zu unterschiedlichen Ergebnissen führt und ob eine verbotene bzw. erlaubte Privatnutzung Einfluss auf die Testgestaltung hat.

Ist die private Nutzung verboten, hat der Arbeitgeber ein generelles Kontrollrecht. Allerdings dürfen auch in diesem Fall keine persönlichen Informationen erhoben werden. Werden die Tests so wie oben dargestellt konzipiert, können keine persönlichen Informationen erlangt werden, so dass nichts gegen dessen Zulässigkeit spricht.

Wenn die private Nutzung erlaubt ist, darf der Arbeitgeber nur im Einzelfall und bei einem begründeten Missbrauchsverdacht den Arbeitnehmer überwachen.[192] Keiner dieser Fälle liegt dem Testszenario zugrunde. Es könnte daher rechtlich unzulässig sein, das IT Sicherheitsbewusstseins bei einer erlaubten Privatnutzung zu überprüfen. Im Falle der Telekommunikationsüberwachung beruht die Restriktion des Arbeitgebers maßgeblich auf der Erwägung, dass er seinen Arbeitnehmern einen privaten Raum öffnet. Dort können sie davon ausgehen, dass ihre Privatsphäre geschützt bleibt. Überwacht der Arbeitgeber diesen Raum und erlangt dadurch private Informationen, verstieße das gegen den eigentlichen Schutzgedanken dieses Raums.[193] Demzufolge ist es dem Arbeitgeber untersagt, im Falle der erlaubten Privatnutzung, seine Mitarbeiter zu überwachen. Kann hingegen ausgeschlossen werden, dass der Arbeitgeber bei der Überwachung des privaten Raums private Information erlangt, ist eine Restriktion seiner Überwachungsbefugnisse nicht mehr notwendig. Der Schutz des Arbeitnehmers erstreckt sich schließlich nur auf seine Privatsphäre, die in dem Fall gar nicht betroffen ist. Auf die Zulässigkeit der Tests hat die Erlaubnis der privaten Nutzung also keine Auswirkungen, sofern durch die Tests keine persönlichen Informationen erhoben werden. Sind die simulierten IT Angriffe so wie oben vorgeschlagenen konzipiert, ist die Zulässigkeit der Tests nicht davon abhängig, ob die private Nutzung erlaubt oder verboten ist. Damit sind die Voraussetzungen an die Testgestaltung in dem Szenario der erlaubten Privatnutzung identisch mit denen der verbotenen Privatnutzung. Das ist ein entscheidender Unterschied zur Überwachung der betrieblichen Telekommunikation und erleichtert die

[192] siehe dazu: S. 23 ff., 27 f.
[193] vgl. dazu ausführlich S. 23.

Realisierung der Tests am UKSH, da es irrelevant ist, ob dort die private Nutzung verboten ist oder nicht.

4. Zusammenfassung

Werden die Tests somit wie hier vorgeschlagenen konzipiert, wird dadurch der erforderliche Schutz der Privatsphäre garantiert. Dies wird u.a. dadurch sichergestellt, dass die Interessen der Betroffenen frühzeitig, auch auf kollektiver Ebene, beachtet werden. Weiterhin werden mit Hilfe der Pseudonymisierung arbeitsrechtliche Konsequenzen effektiv vermieden. Schließlich lassen die Tests auch keine bedeutenden Rückschlüsse auf Umstände der persönlichen Lebensführung zu. Dadurch sind die berechtigten Interessen der getesteten Arbeitnehmer berücksichtigt. Gleichzeitig dienen die Tests auch dem berechtigten Interesse an einer verbesserten Sicherheit informationstechnischer Systeme, das gerade in kritischen Infrastrukturen besteht. Diese sind für ein funktionierendes staatliches Gemeinwesen von überragender Bedeutung. Das hier vorgeschlagene Testdesign berücksichtigt beide Interessen angemessen, so dass die Tests unter den genannten Voraussetzungen zulässig sind.

G. Literaturverzeichnis

Altenburg, Stephan / v. Reinersdorff, Wolfgang / Leister, Thomas	Telekommunikation am Arbeitsplatz, -139 (Zitiert als: *Altenburg/v. Reinersdorff/Leister*, MMR 2005, 135)
Arnold, Iris	Die Zuverlässigkeit der Überwachung von mobilen Arbeitnehmern, Berlin 2010 (Zitiert als: *Arnold*, S.)
Beckschulze, Martin	Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz – Rechte der Beteiligten und Rechtsfolgen bei Pflichtverletzungen, -2786 (Zitiert als: *Beckschulze*, DB 2003, 2777)
Borges, Georg	Rechtsfragen des Phishing – Ein Überblick, NJW 2005, 3313-3315 (Zitiert als: *Borges*, NJW 2005, 3313)
Dannhorn, Melanie / Mohnke, Lars	Arbeitnehmer-Monitoring, AuA 2006, 210-213 (Zitiert als: *Dannhorn/Mohnke*, AuA 2006, 210)
Däubler, Wolfgang	Gläserne Belegschaften?, 6. Auflage, Frankfurt a.M. 2015 (Zitiert als: *Däubler*, S.)
Däubler, Wolfgang / Klebe, Thomas / Wedde, Peter / Weichert, Thilo	Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG, 4. Auflage, Frankfurt 2013 (Zitiert als: Däubler/Klebe/Wedde/Weichert/*Bearbeiter*, BDSG, Rn. zu §)
Decker, Ralf / Deckers, Stefan	Die Beteiligungsrechte des Betriebsrats beim Testkauf, NZA 2004, 139-142 (Zitiert als: *Decker/Deckers*, NZA 2004, 139)

Donalies, Manfred (Begr.) / Hübner-Berger, Malte
Praxis der Kommunalverwaltung – Gesetz über die Mitbestimmung der Personalräte (Mitbestimmungsgesetz Schleswig-Holstein – MGB Schl.-H.), Wiesbaden 2015
(Zitiert als: *Donalies/Hübner-Berger*, Rn. zu §)

Düwell, Franz Josef (Hrsg.)
Betriebsverfassungsgesetz – Handkommentar, 4. Auflage, Baden-Baden 2014
(Zitiert als: Düwell/*Bearbeiter*, Rn. zu §)

Ernst, Stefan
Der Arbeitgeber, die E-Mail und das Internet, NZA 2002, 585-591
(Zitiert als: *Ernst,* NZA 2002, 585)

Freckmann, Anke / Wahl, Sabine
Überwachung am Arbeitsplatz – Was ist legitim? Wo setzt das Recht Grenzen?, BB 2008, 1904-1908
(Zitiert als: *Freckmann/Wahl,* BB 2008, 1904)

Gebhardt, Immaunel / Umnuß, Karsten
Anonymisierung als Weg aus der Mitbestimmung bei elektronischer Datenverarbeitung gemäß § 87 I Nr. 6 BetrVG?, NZA 2995, 103-111
(Zitiert als: *Gebhardt/Umnuß,* NZA 2995, 103)

Gersdorf, Hubertus / Paal, Boris P. (Hrsg.)
Beck'scher Online-Kommentar Informations- und Medienrecht, 11. Auflage, München 2016
(Zitiert als: Gersdorf/Paal*/Bearbeiter*, Rn. zu Art.)

Geppert, Martin / Schütz, Raimund (Hrsg.)
Beck'scher TKG-Kommentar, 4. Auflage, München 2013
(Zitiert als: Geppert/Schütz/*Bearbeiter*, TKG, Rn. zu §)

Glögem Rudi-Müller / Preis, Ulrich / Schmidt, Ingrid (Hrsg.)
Erfurter Kommentar zum Arbeitsrecht, 16. Auflage, München 2016
(Zitiert als: Glögem/Preis/Schmidt/*Bearbeiter*, Rn. zu §)

Gola, Peter / Klug, Christoph
Die Entwicklung des Datenschutzrechts im zweiten Halbjahr 2015, NJW 2016, 691-694
(Zitiert als: *Gola/Klug*, NJW 2016, 691)

Gola, Peter / Schomerus, Rudolf — BDSG – Bundesdatenschutzgesetz – Kommentar, 12. Auflage, München 2015
(Zitiert als: Gola/Klug/*Bearbeiter*, BDSG, Rn. zu §)

Gola, Peter — Neuer Tele-Datenschutz für Arbeitnehmer? – Die Anwendung von TKG und TDDSG im Arbeitsverhältnis, MMR 1999, 322-330
(Zitiert als: *Gola*, MMR 1999, 322)

Grobys, Marcel — Zuverlässigkeitstests im Arbeitsrecht, NJW-Spezial 2005, 273-274
(Zitiert als: *Grobys*, NJW-Spezial 2005, 273)

Hanau, Peter / Hoeren, Thomas — Private Internetnutzung durch Arbeitnehmer, München 2003
(Zitiert als: *Hanau/Hoeren*, S.)

Herfs-Röttgen, Ebba — Rechtsfragen rund um die Personalakte, NZA 2013, 478-482
(Zitiert als *Herfs-Röttgen*, NZA 2013, 478)

Hesse, Konrad — Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Auflage, Heidelberg 1999
(Zitiert als: *Hesse*, S.)

Hoeren, Thomas / Sieber, Ulrich / Holznagel, Bernd (Hrsg.) — Handbuch Multimedia-Recht, 42. Auflage, München 2015
(Zitiert als: Hoeren/Sieber/Holznagel/*Bearbeiter*, Rn. zu §)

Hornung, Gerrit — Ein neues Grundrecht – Der verfassungsrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme, CR 2008, 299-306

Stürner, Rolf (Hrsg.) — Jauernig – Bürgerliches Gesetzbuch – mit Rom-I-, Rom-II-, Rom-III-VO, EG-UntVO/HUntProt und EuErbVO – Kommentar, 16. Auflage, München 2015
(Zitiert als: Jauernig/*Bearbeiter*, Rn. zu §)

Joussen, Jacob — Mitarbeiterkontrolle: Was muss, was darf das Unternehmen wissen?, NZA-Beil. 2011, 35-42
(Zitiert als: *Joussen*, NZA-Beil. 2011, 35)

Kersten, Jens — Legitimationsgrenzen im Personalvertretungsrecht – Die Noelle des schleswig-holsteinischen Mitbestimmungsgesetzes: ein Vorbild?, RdA 2001, 23-27
(Zitiert als: *Kersten*, RdA 2001, 23)

Klengel, Jürgen Detlef W. / Mückenberger, Ole — Internal Investigations – typische Rechts- und Praxisprobleme unternehmensinterner Ermittlungen, CCZ 2009, 81-87
(Zitiert als: *Klengel/Mückenberger*, CCZ 2009, 81)

Kömpf, Nicola / Kunz, Holger — Kontrolle der Nutzung von Internet und E-Mail am Arbeitsplatz in Frankreich und in Deutschland, NZA 2007, 1341-1346
(Zitiert als: *Kömpf/Kunz*, NZA 2007, 1341)

Korn, Jana — Der strafprozessuale Zugriff auf Verkehrsdaten nach § 100g StPO, HRRS 2009, 112-124
(Zitiert als: *Korn*, HRRS 2009, 112)

Kratz, Felix / Gubbels, Achim — Beweisverwertungsverbote bei privater Internetnutzung am Arbeitsplatz, NZA 2009, 652-656
(Zitiert als: *Kratz/Gubbels*, NZA 2009, 652)

Lindemann, Achim / Simon, Oliver — Betriebsvereinbarungen zur E-Mail-, Internet- und Intranet-Nutzung, BB 2001, 1950-1956
(Zitiert als: *Lindemann/Simon*, BB 2001, 1950)

Linsenmaier, Wolfgang — Normsetzung der Betriebsparteien und Individualrechte der Arbeitnehmer, RdA 2008, 1-13
(Zitiert als: *Linsenmaier*, RdA 2008, 1)

Maschmann, Frank — Zuverlässigkeitstests durch Verführung illoyaler Mitarbeiter?, NZA 2002, 13-22
(Zitiert als: *Maschmann*, NZA 2002, 13)

Mattl, Tina — Die Kontrolle der Internet- und E-Mail-Nutzung am Arbeitsplatz – unter besonderer Berücksichtigung der Vorgaben des Telekommunikationsgesetzes, Hamburg 2008 (Zitiert als: *Mattl*, S.)

Maunz, Theodor / Dürig, Günter (Begr.) — Grundgesetz – Kommentar, Band II – Art. 6-15, 75. Ergänzungslieferung, München 2015 (Zitiert als: Maunz/Dürig/*Bearbeiter*, Rn. zu Art.)

Mengel, Anja — Compliance und Arbeitsrecht – Implementierung, Durchsetzung, Organisation, München 2009 (Zitiert als: *Mengel*, S.)

Mengel, Anja — Kontrolle der E-Mail- und Internetkommunikation am Arbeitsplatz – Wege durch einen juristischen Irrgarten, BB 2004, 2014-2021 (Zitiert als: *Mengel*, BB 2004, 2014)

Mengel, Anja — Kontrolle der Telefonkommunikation am Arbeitsplatz, BB 2004, 1445-1453 (Zitiert als: *Mengel*, BB 2004, 1445)

Moll, Wilhelm (Hrsg.) — Münchener Anwaltshandbuch Arbeitsrecht, 3. Auflage, München 2012 (Zitiert als: Moll/*Bearbeiter*, Rn. zu §)

Müllner, Wolfgang — Verhalten und Leistung gemäß § 87 Abs. 1 Nr. 6 BetrVG, DB 1984, 1677-1680 (Zitiert als: *Müllner*, DB 1984, 1677)

Oberwetter, Christian — Arbeitnehmerrechte bei Lidl, Aldi & Co., NZA 2008, 609-613 (Zitiert als: *Oberwetter*, NZA 2008, 609)

Panzer, Andrea — Mitarbeiterkontrolle und neue Medien, Frankfurt a.M. 2004 (Zitiert als: *Panzer*, S.)

Popp, Andreas „Phishing“, „Pharming“ und das Strafrecht, MMR 2006, 84-86
(Zitiert als: *Popp*, MMR 2006, 84)

Puschke, Jens / Singelnstein, Tobias Verfassungsrechtliche Vorgaben für heimliche Informationsbeschaffungsmaßnahmen, NJW 2005, 3534-3538
(Zitiert als: *Puschke*/*Singelnstein*, NJW 2005, 3534)

Raab, Thomas Betriebliche und außerbetriebliche Bildungsmaßnahmen, NZA 2008, 270-275
(Zitiert als: *Raab*, NZA 2008, 270)

Raffler, Andrea / Hellich, Peter Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer-e-Mails zulässig?, NZA 1997, 862-868
(Zitiert als: *Raffler/Hellich*, NZA 1997, 862)

Richardi, Reinhard / Wlotzke, Otfried / Wißmann, Hellmut / Oetker, Hartmut Münchener Handbuch zum Arbeitsrecht, 3. Auflage, München 2009
(Zitiert als: Richardi/Wlotzke/Wißmann/Oetker/*Bearbeiter*, Rn. zu §)

Richardi, Reinhard (Hrsg.) Betriebsverfassungsgesetz mit Wahlordnung – Kommentar, 15. Auflage, München 2016
(Zitiert als: Richardi/*Bearbeiter*, Rn. zu §)

Ricken, Oliver Außerordentliche Kündigung, RdA 2001, 52-55
(Zitiert als: *Ricken*, RdA 2001, 52)

Röckl, Johannes / Fahl, Christian Kündigung nach heimlicher Videoüberwachung, NZA 1998, 1035-1041
(Zitiert als: *Röckl/Fahl*, NZA 1998, 1035)

Rolfs, Christian / Kreikebohm, Ralf / Giesen, Richard / Udsching, Peter (Hrsg.) Beck’scher Online-Kommentar Arbeitsrecht, 38. Auflage, München 2015
(Zitiert als: Rolfs/Kreikebohm/Giesen/Udsching/*Bearbeiter*, Rn. zu §)

Schaub, Günter (Hrsg.) Arbeitsrechts-Handbuch, 16. Auflage, München 2015
(Zitiert *als: Schaub/Bearbeiter*, Rn. zu §)

Schierbaum, Bruno Technische Maßnahmen für den Arbeitnehmerdatenschutz, CuA 2015, 33-37

(Zitiert als: Schierbaum, CuA 2015, 33)

Schmitt, Jochen Anmerkung zum Beschluss des BAG v. 10.11.87 - 1 ABR 55/86, AP BetrVG 1972 § 77 Nr. 24
(Zitiert als: *Schmitt*, AP BetrVG 1972 § 77 Nr. 24)

Simitis, Spiros (Hrsg.) Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden 2014
(Zitiert als*: Simitis/Bearbeiter*, BDSG, Rn. zu §)

Thoma, Oliver Das Spannungsverhältnis zwischen Arbeitnehmerndatenschutz und IT gestützter Compliance : Die Gefahren der Internet- und E-Mail-Kontrolle sowie des Datenscreenings für das informationelle Selbstbestimmungsrecht der Arbeitnehmern, Hamburg 2013
(Zitiert als: *Thoma*, S.)

Thüsing, Gregor (Hrsg.) Arbeitnehmerndatenschutz und Compliance – Effektive Compliance im Spannungsfeld vin BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, 2. Auflage, München 2014
(Zitiert als: Thüsing/*Bearbeiter*, Rn. zu §)

Trappehl, Bernhard / Schmidl, Michael Arbeitsrechtliche Konsequenzen von IT Sicherheitsverstößen, NZA 2009, 985-990
(Zitiert als: *Trappehl/Schmidl*, NZA 2009, 985)

Vehslage, Thorsten Privates Surfen am Arbeitsplatz, AnwBl 2001, 145-149
(Zitiert als: *Vehslage*, AnwBl 2001, 145)

Versteyl, Ludger-Anselm Telefondatenerfassung im Betrieb – Kein Grund zur Orwell'scher Beschwörung, NZA 1987, 7-10
(Zitiert als: *Versteyl*, NZA 1987, 7)

Vietmeyer, Katja / Byers, Philipp
Der Arbeitgeber als TK-Anbieter im Arbeitsverhältnis – Geplante BDSG-Novelle lässt Anwendbarkeit des TKG im Arbeitsverhältnis unangetastet, MMR 2010, 807-811
(Zitiert als: *Vietmeyer/Byers*, MMR 2010, 807)

Wabnitz, Heinz-Bernd / Janovsky, Thomas (Hrsg.)
Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl., München 2014
(Zitiert als: Wabnitz/Janovsky/*Bearbeiter*, Kapitel, Rn.)

Weißgerber, Michael
Das Einsehen kennwortgeschützter Privatdaten des Arbeitnehmers durch den Arbeitgeber, NZA 2003, 1005-1009
(Zitiert als: *Weißgerber*, NZA 2003, 1005)

Weißnicht, Elmar
Die Nutzung des Internet am Arbeitsplatz, MMR 2003, 448-453
(Zitiert als: *Weißnicht*, MMR 2003, 448)

Wellhörner, Astrid / Byers, Philipp
Datenschutz im Betrieb – Alltägliche Herausforderung für den Arbeitgeber?!, BB 2009, 2310-2316
(Zitiert als: *Wellhörner/Byers*, BB 2009, 2310)

Wolf, Thomas / Mulert, Gerrit
Die Zulässigkeit der Überwachung von E-Mail-Korrespondenz am Arbeitsplatz, BB 2008, 442-447
(Zitiert als: *Wolf/Mulert*, BB 2008, 442)

Wolff, Heinrich Amadeus / Brink, Stefan (Hrsg.)
Beck'scher Online-Kommentar Datenschutzrecht, 15. Edition, München 2015 (Stand: 01.08.2015)
(Zitiert als: *Wolff/Brink*, Syst. Rn.)

Wronka, Georg / Gola, Peter
Handbuch Arbeitnehmerdatenschutz – Rechtsfragen und Handlungshilfen, 6. Auflage, Heidelberg 2013
(Zitiert als: *Wronka/Gola*, S.)

Wybitul, Tim / Pötters, Stephan
Der neue Datenschutz am Arbeitsplatz, RDV 2016, 10-16
(Zitiert als: *Wybitul/Pötters*, RDV 2016, 10)

Wybitul, Tim / Sörup, Thorsten / Pötters, Stephan — Betriebsvereinbarungen und § 32 BDSG: Wie geht es nach der DS-GVO weiter?, ZD 2015, 559-564
(Zitiert als: *Wybitul/Sörup/Pötters*, ZD 2015, 559)

Wybitul, Tim — E-Mail-Auswertung in der betrieblichen Praxis – Handlungsempfehlungen für Unternehmen, NJW 2014, 3605-3611
(Zitiert als: *Wybitul*, NJW 2014, 3605)

Zange, Julia — Kontrolle am Arbeitsplatz – Mystery Shopping, Detektive, Videoüberwachung, AuA 2013, 150-152
(Zitiert als: *Zange*, AuA 2013, 150)

Zimmer, Mark / Heymann, Robert C.J. — Beteiligungsrechte des Betriebsrats bei unternehmensinternen Ermittlungen, BB 2010, 1853-1856
(Zitiert als: *Zimmer*/*Heymann*, BB 2010, 1853)