



SCHRIFTEN ZUM DEUTSCHEN UND  
EUROPÄISCHEN ARBEITS- UND SOZIALRECHT

Herausgegeben von Ulrich Preis

Band 26

David Kruchen

---

# Telekommunikationskontrolle zur Prävention und Aufdeckung von Straftaten im Arbeitsverhältnis

Private Arbeitgeber im Spannungsverhältnis zwischen  
Datenschutz und Compliance

## Teil 1: Einleitung

Das 21. Jahrhundert steht unter dem Stern der informationstechnischen Entwicklung. Speziell im Bereich der Telekommunikation sind nahezu wöchentlich Neuentwicklungen zu bestaunen. Telefon- und Internetnetze werden immer leistungsfähiger und schneller, die hierfür notwendigen Kommunikationseinrichtungen immer komplexer. Die Flut neuer Anwendungen und Funktionen im IT-Bereich ist kaum noch zu überblicken. Informationen verbreiten sich in Sekunden um die ganze Welt und sind für jedermann jederzeit problemlos erreichbar. Gleiches gilt auch für jeden einzelnen Menschen; die umfassende Verweigerung der Teilnahme an der globalen Vernetzung ist kaum noch möglich. Auch das moderne Arbeitsleben wird heute bestimmt von diesen Entwicklungen. Der überwiegenden Mehrheit der Arbeitnehmer in Deutschland steht am Arbeitsplatz bereits ein Internetzugang zur Verfügung, die Tendenz ist weiter steigend.<sup>1</sup>

Die jüngere Vergangenheit lehrt uns jedoch, dass der unaufhaltsame informationstechnische Fortschritt unserer Gesellschaft auch seine Schattenseiten hat. Wer darauf vertraut, sich im virtuellen Umfeld anonym bewegen zu können, erliegt einem Irrglauben. Jede Nutzung technischer Kommunikationsmedien, die für den Einzelnen in ihrer Komplexität kaum noch wirklich verstanden werden können, hinterlässt Spuren. Wer die Gerätschaften zu nutzen weiß und über entsprechendes technisches Know-how verfügt, dem gewähren sie eine Fülle von Informationen über den jeweiligen Nutzer, wobei jener sich über deren Preisgabe häufig gar nicht bewusst ist. Der Nutzer läuft Gefahr, zu einem „Überwachungsobjekt“ zu werden.<sup>2</sup>

Die Bevölkerung und auch die Politik wurde spätestens durch die gehäuft in Presse und Rechtsprechung auftretende „Datenskandale“ für das Thema des Datenschutzes sensibilisiert. Speziell im Verhältnis zwischen Arbeitnehmer und Arbeitgeber spielt dieses eine immer bedeutendere Rolle. Das Interesse des Arbeitgebers an Informationen über seine Beschäftigten ist hoch: Je umfangreicher seine Datengrundlage ist, desto präziser und leichter können immer wieder notwendige personalpolitische und unternehmerische Entscheidungen getroffen

---

1 Nach Angaben des Statistischen Bundesamtes waren im Januar 2011 54 % der Erwerbstätigen über den Arbeitsplatzcomputer mit dem Internet verbunden. Im Januar 2003 waren es nur 31 %.

Informationen abrufbar unter:

„<https://www.destatis.de/DE/Publikationen/Thematisch/Informationsgesellschaft/Unternehmen/InformationstechnologieUnternehmen.html>“. Letzter Abruf am 01.07.2012.

2 Hiervor warnt insbesondere *Däubler*, Rn. 23. Er prägt den Begriff der „Gläsernen Belegschaft“.

werden. Für die systematische Überwachung und Kontrolle der Belegschaft bieten sich ihm immer neue Mittel und Wege, denen sich der einzelne Mitarbeiter aufgrund seiner Dienstverpflichtung kaum entziehen kann. Hier reiht sich auch die Überwachung der Telekommunikation der Beschäftigten ein. Zu Recht stellt sich der Arbeitnehmer die Frage, was er sich eigentlich alles gefallen lassen muss.

Andererseits handeln Arbeitgeber bei der Durchführung von Kontrollen aus nachvollziehbaren Motiven. Die technische Entwicklung bietet zahlreiche Möglichkeiten, gegen Betriebsstörungen durch Mitarbeiter effektiv vorgehen zu können. Dabei stehen häufig die Fälle im Fokus, in denen Mitarbeiter durch kriminelle Aktivität das Unternehmen oder Dritte direkt oder mittelbar schädigen. Die technischen Errungenschaften sind schließlich inhaltsneutral und begünstigen die Kommunikation redlicher wie unredlicher Nutzer gleichermaßen. Inhalte und Umstände von Kommunikationsvorgängen sind dazu geeignet, Hinweise auf oder gar Beweise für kriminelle Vorgänge gewinnen zu können. Den Arbeitgeber im Falle von gegen ihn verübten oder aus seinem betrieblichen Umfeld entspringenden Straftaten zum tatenlosen Zuseher zu verdammen, obwohl effiziente Maßnahmen im Bereich des technisch Machbaren liegen, kann nicht Ziel der Rechtsordnung sein. Allerdings werden in aller Regel nicht nur potentielle Straftäter sondern auch die weitaus größere Zahl der redlich handelnden Mitarbeiter von einer Überwachungsmaßnahme erfasst. Erneut muss die Frage gestellt werden, ob ein unbescholtener Mitarbeiter sich gegen ein entsprechendes Vorgehen des Arbeitgebers zur Wehr setzen kann.

Doch nicht nur aus ureigenen Interessen des Arbeitgebers greift dieser zu Überwachungs- und Kontrollmaßnahmen. Die Rechtsordnung selbst verlangt von ihm, durch geeignete präventive und repressive Maßnahmen dafür Sorge zu tragen, dass sich seine Beschäftigten rechtskonform verhalten. Für den Fall einer Zuwiderhandlung gegen die Compliance-Verpflichtung, auf die hier angespielt wird, drohen empfindliche Schadenersatzforderungen und hohe Bußgelder.<sup>3</sup> Insbesondere für den Fall strafbaren Handelns durch Arbeitnehmer, dem wohl eindeutigsten und schwerwiegendsten aller möglichen Gesetzesverstöße, ist der Arbeitgeber zu datenschutzrechtlich brisanten Kontrollmaßnahmen gezwungen, will er negative Auswirkungen auf sich und sein Unternehmen verhindern. Gesetzgeber bzw. Gerichte verleihen dem hier umrissenen Konflikt somit eine zusätzliche Dimension. Gerade vor dem Hintergrund der Compliance-Verpflichtung ist die Kenntnis über die Zulässigkeitsgrenzen für Kontrollmaßnahmen für den Arbeitgeber nicht zuletzt auch finanziell von höchster Relevanz.

---

3 Die Siemens AG wurde im Jahre 2008 zu einer Zahlung von 395 Mio. € wegen unterlassener Aufsichtsmaßnahmen verurteilt. Vgl. hierzu den Bußgeldbescheid der Staatsanwaltschaft München vom 15.12.2008, abrufbar unter „[www.siemens.com/sec-einigung](http://www.siemens.com/sec-einigung)“ (Letzter Abruf am 01.07.2012).

In diesem sensiblen Umfeld ist der Gesetzgeber gefragt, effiziente und handhabbare Normen zu statuieren, um den Bereich des Arbeitnehmerdatenschutzes insgesamt und den Bereich der Überwachung der Telekommunikation der Beschäftigten im Speziellen zu reglementieren. Verfährt der Gesetzgeber zu streng oder zu unbedacht mit einschränkenden Verboten oder erschwerenden Anforderungen, so stellt er den Arbeitgeber im Extremfall hinsichtlich der Verhinderung von Rechtsverstößen durch die Belegschaft vor unlösbare Aufgaben.<sup>4</sup> Auch für die Arbeitnehmerseite ist es von allerhöchstem Interesse, die Grenzen der arbeitgeberseitigen Kontrollmaßnahmen klarzustellen. Hierdurch können datenschutzrechtliche Verstöße der Arbeitgeber effizient aufgedeckt und die Gerichte durch Verhinderung unnötiger Gerichtsverfahren entlastet werden.

Konkrete parlamentarische Ansätze zur Schaffung eines eigenen Beschäftigtendatenschutzgesetzes gibt es bereits seit dem Jahre 2008. Diese verkörpern den ursprünglichen Anstoß für die vorliegende Arbeit. Ein im Jahre 2010 eingeleitetes Gesetzgebungsverfahren verzögerte sich jedoch aufgrund schwer überbrückbarer politischer Diskrepanzen und umfangreichem Widerstand von Gewerkschaften, Arbeitgeberverbänden und aus der Rechtswissenschaft erheblich. Eine Verabschiedung in naher Zukunft erscheint zum Zeitpunkt der Fertigstellung dieser Arbeit unwahrscheinlich. Anstelle einer Untersuchung der in einem Gesetzgebungsverfahren mit unmöglich absehbarem Ausgang befindlichen Regelungen konzentriert sich der Verfasser auf die ausführliche Erörterung der geltenden Rechtslage. Ziel dieser Arbeit ist es, zu untersuchen, welche konkreten Befugnisse die geltende Rechtsordnung dem privaten Arbeitgeber hinsichtlich der Kontrolle der Telekommunikation zur Aufdeckung und Prävention von Straftaten durch Beschäftigte zuspricht. Auf dieser Basis können die verschiedenen Handlungsoptionen einander gegenübergestellt und bewertet werden. Zudem wird veranschaulicht, an welchen Stellen aus Sicht des Verfassers noch gesetzgeberischer Handlungsbedarf besteht.

Der Verfasser beschränkt sich dabei auf den speziellen Kontrollzweck der Aufdeckung und Prävention von Straftaten durch Mitarbeiter. Diese Beschränkung dient nicht allein der Verhinderung einer ausufernden Darstellung. Sie ermöglicht gleichzeitig wesentlich konkretere Ausführungen, sofern die Zulässigkeit einer konkreten Überwachungsmaßnahme von einer Interessenabwägung oder die Anwendbarkeit gesetzlicher Grundlagen von der Zwecksetzung abhängt. Allein der Begrenzung des Umfangs der Arbeit geschuldet ist die Beschränkung auf Kontrollmaßnahmen durch private Arbeitgeber.

Zur Heranführung an das Kernthema dient nachfolgende Kurzübersicht der Ereignisse, die das Thema „Arbeitnehmerdatenschutz“ erst ins öffentliche Bewusstsein riefen.

---

4 Zugespitzt betitelt ist der Aufsatz von *Wybitul*, BB 2009, 1582: „Vertrauen ist gut, Kontrolle verboten?“

## A. Beispiele für „Datenskandale“ in Deutschland

Der Stellenwert des Themas „Datenschutz“ in der gesellschaftlichen Diskussion nimmt stetig zu. Die Aufdeckung von Rechtsverstößen eines Arbeitgebers im Umgang mit sensiblen, personenbezogenen Mitarbeiterdaten liegt mittlerweile an der journalistischen und politischen Tagesordnung. In jüngerer Vergangenheit, verstärkt seit dem Jahre 2008, erschüttern immer wieder so genannte „Datenskandale“ beachtlicher Dimensionen das Vertrauen der Beschäftigten in ihre jeweilige Unternehmensleitung. Nachfolgend sollen einige Beispiele systematischer Mitarbeiterüberwachung aufgeführt werden, die zu erheblichen gesellschaftlichen Eklats geführt haben und die Notwendigkeit von Datenschutz im Arbeitsverhältnis verdeutlichen.

Im Frühjahr 2008 wurde bekannt, dass der Discounter LIDL Privatdetekteien dazu einsetzte, seine Mitarbeiter mit Hilfe von Miniaturkameras systematisch zu bespitzeln.<sup>5</sup> Die Kameras wurden von den Detektiven in den einzelnen Filialen vor Dienstbeginn der Mitarbeiter installiert. Angeblich sollte die Maßnahme der Überführung von Ladendieben aus dem Kundenkreis dienen, was jedoch einzig dem Filialleiter kommuniziert wurde.<sup>6</sup> Tatsächlich wurde das gewonnene Bildmaterial aber auch zur Einschätzung des Verhaltens der Beschäftigten gegenüber Kunden, Kollegen und in den Pausen ausgewertet. Darüber hinaus wurden die persönlichen Verhältnisse der Beschäftigten und deren Familien ausgeforscht, etwa hinsichtlich deren finanzieller Situation, Gesundheitszustand oder eventuell bevorstehender Schwangerschaften. Zu diesem Zweck wurden dienstliche und persönliche Telefonate abgehört.<sup>7</sup>

Ähnliche Vorwürfe wurden im April 2008 gegenüber den Unternehmen IKEA und Burger King erhoben. Beide sollen Mitarbeiter mittels Videokameras heimlich und ohne Zustimmung des Betriebsrates überwacht haben, Burger King filmte sogar die Gründung eines Betriebsrates.<sup>8</sup> Ebenso in die Kritik gerie-

---

5 Dieser Fall verursachte unmittelbare Reaktionen in der Rechtswissenschaft, was bereits der Titel des Aufsatzes von *Oberwetter*, NZA 2008, 609 andeutet.

6 Über den Vorgang berichtete die Zeitschrift Stern unter: <http://www.stern.de/wirtschaft/news/unternehmen/ueberwachungsskandal-lidl-gibt-bespitzelung-zu-615031.html>. Letzter Abruf am 01.07.2012.

7 Die Aufsichtsbehörden für den Datenschutz veröffentlichten im September 2008 einen Bericht zum Fall vor, wiedergegeben in RDV 2008, 216; vgl. auch *Däubler*, Rn. 2b.

8 Vgl. dazu einen Bericht der Süddeutschen Zeitung unter: <http://www.sueddeutsche.de/wirtschaft/mitarbeiter-bespitzelung-auch-ikea-und-burger-king-ueberwachten-personal-1.211812>. Letzter Abruf am 01.07.2012.

ten die Unternehmen Edeka und Plus.<sup>9</sup> Bei der Firma Tönnies, einem Unternehmen aus der Fleischindustrie, wurden sogar Videoaufnahmen von Mitarbeitern in Kantinen und Umkleidekabinen gemacht.<sup>10</sup>

Im Mai 2008 wurde bekannt, dass die Deutsche Telekom das Telefonverhalten zahlreicher Beschäftigten überwachte und auswertete. Das Unternehmen litt zu dieser Zeit unter dem Bekanntwerden unternehmensschädlicher interner Informationen. Systematische Telefonkontrollen erfolgten daher maßgeblich zum Zweck, Pressekontakte einzelner Mitarbeiter in Erfahrung zu bringen und Beweismaterial zur Nutzung für interne Ermittlungen zu erlangen. Darüber hinaus wurden Daten zur finanziellen Situation der Mitarbeiter erhoben.<sup>11</sup>

Der Versicherungskonzern Gerling überwachte aus ähnlichem Anlass nicht nur die Telefonverkehrsdaten sondern auch die Verkehrsdaten der E-Mail-Kommunikation der Mitarbeiter, was im Juli 2008 aufgedeckt wurde. Wie im Falle der Telekom diene das Vorgehen zur Identifikation von Mitarbeitern, die betriebsinterne Informationen zum Abbau der betrieblichen Altersversorgung an die Presse herausgegeben hatten.<sup>12</sup>

Verwickelt in zweifelhafte Überwachungsmethoden war auch die Deutsche Bahn, was im April 2009 an die Öffentlichkeit drang.<sup>13</sup> Schwerpunkt der Vorwürfe waren hier umfangreiche, von Privatdetekteien mehrfach durchgeführte Abgleiche von privaten Bankverbindungen der Beschäftigten mit denen von Dienstleistern und Zulieferern (so genannte „Sreenings“) zur Aufdeckung möglicher Korruptionsfälle, ohne dabei allerdings konkreten Verdachtsmomenten nachzugehen.<sup>14</sup> In diesem Zusammenhang sollen sowohl E-Mail-Inhalte als auch Kontodaten ausgelesen worden sein.<sup>15</sup>

---

9 Nachzulesen bei der Süddeutschen Zeitung unter: <http://www.sueddeutsche.de/wirtschaft/mitarbeiterueberwachung-spitzel-skandal-auch-bei-edeka-und-plus-1.286584>. Letzter Abruf am 01.07.2012.

10 Hierzu ebenfalls die Süddeutsche Zeitung unter: <http://www.sueddeutsche.de/wirtschaft/bussgeld-fuer-fleischverarbeiter-toennies-kameras-im-umkleideraum-1.698260>. Letzter Abruf am 01.07.2012.

11 Vgl. einen Bericht des Spiegel unter: <http://www.spiegel.de/wirtschaft/0,1518,586516,00.html>. Letzter Abruf am 01.07.2012. Dazu auch *Däubler*, Rn. 2f.

12 Hierüber berichtete Focus Online unter: [http://www.focus.de/finanzen/news/mitarbeiterueberwachung-auch-gerling-hat-bespitzelt\\_aid\\_320701.html](http://www.focus.de/finanzen/news/mitarbeiterueberwachung-auch-gerling-hat-bespitzelt_aid_320701.html). Letzter Abruf am 01.07.2012.

13 Vgl. den Bericht der Süddeutschen Zeitung unter: <http://www.sueddeutsche.de/wirtschaft/bahn-datenskandal-pfeif-aufs-recht-1.391890>. Letzter Abruf am 01.07.2012.

14 Zur Verdeutlichung der unterschiedlichen Bewertung der Vorgänge in der Rechtswissenschaft: *Diller*, BB 2009, 438 (438 ff.) sah keinerlei Rechtsverstoß; diese Ansicht harsch kritisierend *Steinkühler*, DB 2009, 1294 (1294 f.).

15 Vgl. zum Fall insgesamt *Däubler*, Rn. 2g; *Ehleben/Schirge/Seipel*, AiB 2009, 192 (192 f.).

Insgesamt wird deutlich, dass datenschutzrechtlich zumindest bedenkliche Vorgänge im Umgang mit Beschäftigtendaten kein Einzelfall sind und unabhängig von Betriebsgröße und Branchenzugehörigkeit auftreten können. Dabei beschränkt sich die vorstehende Darstellung sogar ausschließlich auf von größeren Unternehmen durchgeführte Überwachungsmaßnahmen mit einem Bezug zu technischen Medien und erhebt keinen Anspruch auf Vollständigkeit. Die Häufung der Beispiele zeigt aber, dass die Beschäftigten vor einer uferlosen Erhebung und Nutzung ihrer persönlichen Daten durch die Arbeitgeber geschützt werden müssen.<sup>16</sup> Allerdings sind die Beweggründe, die Unternehmen zu solchen Kontrollen bewegen, nicht selten gut nachvollziehbar: Insbesondere Überwachungsmaßnahmen zur Abwehr und Verhinderung von Straftaten gegen sich oder gegen betriebsfremde Dritte, welche Kerngegenstand dieser Arbeit sein sollen, lassen sich auf ein billigenswertes Motiv zurückführen.<sup>17</sup> Es wird ersichtlich, dass effiziente gesetzliche Regelungen zum Umgang mit Beschäftigtendaten vor dem Hintergrund der widerstreitenden Interessen der Arbeitsvertragsparteien nicht nur praktisch notwendig sondern sogar unerlässlich für ein funktionierendes Zusammenwirken der Arbeitsvertragsparteien sind.

---

16 Exemplarisch *Kock/Francke*, NZA 2009, 646 (651); *Viotto*, AuR 2010, 422 (422 ff.).

17 Exemplarisch *Wybitul*, BB 2009, 1582 (1582 ff.); *Heinson*, BB 2010, 3084 (3084 ff.); *Freckmann/Wahl*, BB 2008, 1904 (1904 ff.).

## B. Gang der Untersuchung

Um die Rechtswidrigkeitsgrenzen für arbeitgeberseitige Überwachungsmaßnahmen im Sinne dieser Arbeit genau ausloten zu können, müssen im nachfolgenden zweiten Teil zunächst die rechtlichen Rahmenbedingungen dargestellt werden. Als Ausgangspunkt der weiteren Ausführungen soll eine Gegenüberstellung der grundrechtlich gestützten Interessen der Arbeitsvertragsparteien an der Durchführung oder Verhinderung einer Mitarbeiterkontrolle dienen.<sup>18</sup> Im Anschluss folgt eine Darstellung der einfachgesetzlichen Grundlagen, über die der Gesetzgeber eben jenes verfassungsrechtliche Spannungsverhältnis des Arbeitnehmerdatenschutzes zu kanalisieren versucht.<sup>19</sup> Diese Darstellung darf und wird sich nicht ausschließlich auf datenschutzrechtliche Grundlagen beschränken, sondern nimmt auch diejenigen einfachgesetzlichen und europarechtlichen Regelungen und Prinzipien in den Blick, die potentiell Einfluss auf die Entscheidung des Arbeitgebers für oder gegen die Überwachung der Telekommunikation der Beschäftigten haben. Insbesondere die genaue Bedeutung der bereits angerissenen Compliance-Pflicht bedarf näherer Ausführungen.<sup>20</sup>

Auf dieser Basis werden im dritten Teil dieser Arbeit die dem Arbeitgeber unmittelbar durch die Rechtsordnung zugesprochenen Kontrollbefugnisse erarbeitet.<sup>21</sup> Die Anwendungsbereiche der datenschutz- und telekommunikationsrechtlichen Vorschriften müssen hierfür trennscharf voneinander abgegrenzt werden. Eine wesentliche Zäsur bildet in diesem Zusammenhang das Vorliegen oder Nichtvorliegen der arbeitgeberseitigen Erlaubnis der Privatnutzung der betrieblichen Kommunikationseinrichtungen durch die Beschäftigten.<sup>22</sup> Erst nach der Präzisierung sämtlicher Anwendbarkeitsvoraussetzungen können Fallgruppen gebildet und die jeweils einschlägigen Rechtsgrundlagen ermittelt werden. Insbesondere ist zur Ermittlung der konkreten Kontrollbefugnisse zwischen den im Arbeitsleben wesentlichen Kommunikationsformen Telefon<sup>23</sup>, Internet<sup>24</sup> und E-Mail<sup>25</sup> zu differenzieren. Unter Rückgriff auf die gewonnenen Erkenntnisse kann schließlich die Frage beantwortet werden, ob die Gesetzeskonzeption den

---

18 Zum jeder Mitarbeiterkontrolle zugrunde liegenden Interessenkonflikt siehe S. 10 ff.

19 Zu den einfachgesetzlichen Grundlagen siehe S. 18 ff.

20 Zur Compliance-Verpflichtung des Arbeitgebers siehe S. 25 ff.

21 Zu den einfachgesetzlich zugesprochenen Kontrollbefugnissen siehe S. 52 ff.

22 Die Erlaubnis der Privatnutzung der betrieblichen Kommunikationsmittel wird auf S. 76 ff. erörtert.

23 Kontrollbefugnisse bei erlaubter Privatnutzung: S. 97 ff.; Kontrollbefugnisse ohne Erlaubnis einer Privatnutzung: S. 187 ff.

24 Bei erlaubter Privatnutzung S. 113 ff.; ohne Erlaubnis einer Privatnutzung S. 195 ff.

25 Bei erlaubter Privatnutzung S. 125 ff.; ohne Erlaubnis einer Privatnutzung S. 211 ff.



einfachgesetzlichen, verfassungsrechtlichen und europarechtlichen Anforderungen genügt.<sup>26</sup>

Der vierte Teil der Arbeit befasst sich mit der Frage, inwieweit der Arbeitgeber Telekommunikationskontrollen ohne Rückgriff auf einfachgesetzliche Rechtfertigungsvorschriften legitimieren kann. Insbesondere soll hinterfragt werden, ob über Betriebsvereinbarungen, Tarifverträge<sup>27</sup> oder Einwilligungen der von einer Maßnahme betroffenen Beschäftigten<sup>28</sup> eine Erweiterung der einfachgesetzlich zugesprochenen Kontrollbefugnisse erreicht werden kann. Anschließend wird die Eignung der jeweiligen Vorgehensweise als Alternative zu einer strikten Orientierung an den gesetzlichen Rechtfertigungstatbeständen einer Bewertung unterzogen.<sup>29</sup>

Im fünften Teil werden die wesentlichen Ergebnisse der Arbeit in Thesen zusammengefasst.<sup>30</sup> Auf dieser Grundlage können im abschließenden sechsten Teil Handlungsempfehlungen für den kontrollierenden Arbeitgeber ausgesprochen werden.<sup>31</sup> Der Autor erstellt auf Basis der erarbeiteten Erkenntnisse Musterkonzeptionen für die drei untersuchten Kommunikationsmedien betreffende Kontrollmaßnahmen, die einen gerechten Interessenausgleich schaffen und sämtlichen Anforderungen der Rechtsordnung entsprechen.<sup>32</sup> Zuletzt wird der aus Sicht des Verfassers bestehende gesetzgeberische Handlungsbedarf veranschaulicht.<sup>33</sup>

---

26 Siehe dazu S. 139 ff. und S. 279 ff.

27 Zur Möglichkeit der Rechtfertigung einer Kontrollmaßnahme über Betriebsvereinbarungen und Tarifverträge siehe S. 254 ff.

28 Zur Möglichkeit der Rechtfertigung einer Kontrollmaßnahme über Einwilligungen der Betroffenen siehe S. 234 ff.

29 Zur Eignung von Einwilligungen zur Rechtfertigung von Kontrollmaßnahmen siehe S. 250 ff., zur Eignung von Betriebsvereinbarungen und Tarifverträgen siehe S. 262 f. und S. 267 ff.

30 Die Arbeit wird auf S. 273 ff. in Thesen zusammengefasst.

31 Zu den Handlungsempfehlungen für den Arbeitgeber siehe S. 279 ff.

32 Musterkonzeption Telefon: S. 284 ff.; Musterkonzeption Internet: 286 ff.; Musterkonzeption E-Mail: 288 ff.

33 Siehe hierzu S. 289 ff.