

Kramer
IT-Arbeitsrecht

IT-Arbeitsrecht

Handbuch
Digitalisierung · Homeoffice · KI
Virtuelle Betriebsratsarbeit

Herausgegeben von

Dr. Stefan Kramer

Rechtsanwalt und Fachanwalt für Arbeitsrecht, Hannover/Hamburg

Bearbeitet von

RA, FAArbR *Dr. Anton Barrein*; RA, FAArbR *Dr. Frank Bongers*;
RA, FAArbR *Dr. Philipp Byers*; RA, FAArbR Prof. *Dr. Michael Fuhlrott*;
RA, FAArbR *Karl Geißler*; RA, FAArbR *Dr. Christian Hoppe*;
RA, FAArbR *Dr. Stefan Kramer*; RAin, FAinArbR *Dr. Judith Neu*;
RA, FAStrR, FAStrR *Dirk Petri*; RA, FAArbR *Dr. Alexander Raif*; RAin *Dr. Janine Schleper*;
RAin, FAinArbR *Dr. Kathrin Schulze Zumkley*; RA Prof. *Christian Solmecke*;
Direktor d. ArbG *Dr. Jens Tiedemann*; RAin, FAinArbR *Stephanie Törkel*;
Stellv. Direktor d. ArbG, RiArbG *Dr. Axel von der Straten*;
RAin, FAinArbR *Kathrin Wenzel*

4. Auflage 2026



Zitiervorschlag
Kramer IT-ArbR/Solmecke § 1 Rn. 1

beck.de

ISBN PRINT 978 3 406 83314 4

© 2026 Verlag C.H.Beck GmbH & Co. KG
Wilhelmstraße 9, 80801 München
info@beck.de

Druck und Bindung: Beltz Grafische Betriebe GmbH
Am Fliegerhorst 8, 99947 Bad Langensalza

Satz: Druckerei C.H.Beck, Nördlingen
Umschlag: Druckerei C.H.Beck, Nördlingen

chbeck.de/nachhaltig
produktsicherheit.beck.de

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Alle urheberrechtlichen Nutzungsrechte bleiben vorbehalten.
Der Verlag behält sich auch das Recht vor, Vervielfältigungen dieses Werkes
zum Zwecke des Text and Data Mining vorzunehmen.

Vorwort

Die Megatrends im IT-Arbeitsrecht seit der ersten Auflage dieses Handbuches im Jahr 2017 waren die Digitalisierung von analogen Arbeitsvorgängen, die Ausbreitung mobiler Arbeit (vor allem im Homeoffice) und der Einsatz sprachbasierter KI in Gestalt von Chatbots, deren Anwendung insbesondere durch die Anfang August 2024 in Kraft getretene KI-VO europarechtlich reglementiert wurde. Neben die Chatbot-KI tritt aktuell in immer stärkerem Maße die „physical ai“ oder „Industrie-KI“, bei der die KI die Maschinensteuerung und die Bewegung von Robotern übernimmt und damit die Arbeitsvorgänge in Fabrikhallen rasanter und grundlegender verändert als bisher. Zielsetzung dieses Trends ist es, dass industrielle Maschinen und Roboter nicht mehr aufwendig programmiert werden müssen, sondern durch die KI erkennen, lernen, sich selbst dynamisch optimieren und damit viel effizienter Aufgaben erledigen können. Finale ökonomische Ziele sind die Steigerung der Produktivität, der Wirtschaftlichkeit und des Gewinns.

IT-Arbeitsrecht als ein Teilgebiet des Arbeitsrechts, das sich mit der Beurteilung arbeitsrechtlicher Fragen befasst, die beim IT-Einsatz entstehen, thematisiert insoweit die Zulässigkeit des KI-Einsatzes bei der Aufgabenerledigung. In dem neuen Kapitel § 2 X werden insbesondere die praxisrelevanten Fragen in Bezug auf den (eigenmächtigen) Einsatz von KI durch den Arbeitnehmer und die Tauglichkeit einer autonomen KI als weisungsbefugter Vorgesetzter gegenüber dem Arbeitnehmer beleuchtet und bewertet. Auch in den übrigen Kapiteln wurde die besondere Bedeutung des KI-Einsatzes bei den vorgenommenen Textaktualisierungen berücksichtigt. Weitere neue oder vertiefte Themen der Neuauflage sind Workation, Beendigung und Einschränkung von Homeoffice, Cybercrime und Mitbestimmung des Betriebsrats beim Einsatz von KI. Das datenschutzrechtliche Kapitel (§ 4) nimmt nunmehr auch die KI-VO in den Blick. Für eine vertiefende Lektüre der datenschutzrechtlichen Aspekte bietet sich das von den Herausgebern Weth/Herberger/Wächter/Sorge in diesem Verlag in der dritten Auflage im Januar 2026 erschienene Praxishandbuch zum Arbeitnehmerdatenschutz „Daten- und Persönlichkeitsschutz im Arbeitsverhältnis“ an.

Im Rahmen der Neuauflage hat es Veränderungen im Autorenteam gegeben. Aufgrund mehrerer laufender eigener Buchprojekte ist die dankenswerterweise seit der ersten Auflage des Handbuches mitwirkende Kollegin Dr. Nathalie Oberthür aus dem Team ausgeschieden; die von ihr betreuten Kapitel wurden von Dr. Janine Schleper übernommen. Ende Juni 2024 verstarb leider unser Mitautor RiBAG aD Dr. Mario Eylert, dem wir auch in diesem Autorenkreis ein ehrendes Andenken bewahren. Das von ihm betreute Kapitel führt Dr. Anton Barrein fort.

Das im Buch verwendete generische Maskulinum dient ausschließlich der besseren Lesbarkeit des Textes; es sollen sich alle lesenden Menschen – unabhängig von ihrem Geschlecht – angesprochen und einbezogen fühlen.

Dr. Peter Glanz, Lektoratsleiter Arbeitsrecht, und Renate Tobin, Lektorin, sei herzlich für die umsichtige verlagsseitige Betreuung der Neuauflage gedankt. Mein Buchbeitrag ist Birgitt Kramer, Felix Kramer, Annika Kramer und George Fischer gewidmet.

Hannover/Hamburg, im Mai 2026

Stefan Kramer

Vorwort zur ersten Auflage

Titel und Struktur dieses Buches sind seit der Jahrtausendwende gewachsen und haben sich nach gut 15 Jahren konkretisiert. Ausgangspunkt war die um das Jahr 2000 herum in meiner anwaltlichen Praxis erstmals aufgetretene Thematik der privaten Internetnutzung am Arbeitsplatz als Kündigungsgrund. Von diesem Punkt aus ergaben sich infolge der fortschreitenden Entwicklung und Verbreitung der IT im Arbeits- und Wirtschaftsleben regelmäßig neue arbeitsrechtliche Herausforderungen. Aus der literarischen und anwaltlichen Bearbeitung einzelner Aspekte dieses Prozesses wie Telearbeit, Kündigungsrelevanz von Internetnutzung, Inanspruchnahme betrieblicher IT-Ressourcen und eines Facebook-Postings sowie IT-bezogener kollektivrechtlicher Fragestellungen entstand letztendlich der Gedanke einer umfassenden Darstellung der wesentlichen Themenbereiche des IT-Arbeitsrechts. Dieser wurde dankenswerterweise vom Lektor Thomas Wilting und vom Verlag positiv aufgenommen. Mein Buchbeitrag ist in memoriam Johannes Kramer gewidmet.

Der Untertitel des Werkes lehnt sich in abgewandelter Form bewusst an das Thema der arbeitsrechtlichen Abteilung des 71. Deutschen Juristentages („Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf“), der Anfang September 2016 in Essen stattfand, an. Während jedoch dort – entsprechend der Zielsetzung des djt – die Benennung von gesetzlichen Defiziten und der daraus folgende Reformbedarf im Mittelpunkt standen, sind Gegenstand dieses Buches die Darstellung der wesentlichen IT-bezogenen Herausforderungen aus der Sicht eines digitalisierten Unternehmens und deren praxisgerechte Lösung. Dabei werden bei den verschiedenen Problemstellungen sowohl die Arbeitnehmer- als auch die Arbeitgeberseite berücksichtigt.

Das Buch soll allen in Theorie und Praxis auf dem Gebiet des IT-Arbeitsrechts tätigen Lesern eine Hilfestellung zur Bewältigung der individual- und kollektivrechtlichen Herausforderungen geben. Für diese Zielsetzung haben sich dankenswerterweise zahlreiche renommierte Mitautoren aus der Anwalt- und Richterschaft begeistern lassen, die sich bereits in der Vergangenheit in Gestalt von anwaltlichen Praxisfällen, Gerichtsurteilen, Aufsätzen oder Dissertationen eingehend mit unterschiedlichen Aspekten des IT-Arbeitsrechts befasst haben. Ohne sie hätte das umfangreiche Vorhaben nicht realisiert werden können. Angesichts der für die Entwicklung der IT typischen Dynamik ist bereits jetzt absehbar, dass es sich bei dem Inhalt des Werkes um eine aktuelle Momentaufnahme wesentlicher Auswirkungen der IT auf das Arbeitsrecht handelt, die einer Fortschreibung zur Bewältigung neuer Herausforderungen bedarf. Die IT- und Arbeitswelt wird 2025 völlig anders aussehen als heute. Da der Schwerpunkt der Darstellung im Arbeitsrecht liegt, werden zwar datenschutzrechtliche Auswirkungen und Begrenzungen berücksichtigt; für eine vertiefende Lektüre bietet sich insoweit allerdings das von Weth/Herberger/Wächter in diesem Verlag herausgegebene Praxishandbuch zum Arbeitnehmerdatenschutz „Daten- und Persönlichkeitsschutz im Arbeitsverhältnis“ an. Wie Franz Gamillscheg in seinem Vorwort zur 7. Auflage des ersten Bandes der legendären PdW-Reihe unter Bezugnahme auf ein Wort von Otto Kahn-Freund schrieb, ist im Arbeitsrecht „eine Woche eine lange Zeit“. Dies gilt erst recht für das IT-Arbeitsrecht.

Hannover, im April 2017

Stefan Kramer

Autorinnen und Autoren des Handbuchs

Dr. Anton Barrein	Rechtsanwalt und Fachanwalt für Arbeitsrecht, activelaw Offenhausen.Wolter, Hannover
Dr. Frank Bongers	Rechtsanwalt und Fachanwalt für Arbeitsrecht, Esche Schümann Commichau, Hamburg
Dr. Philipp Byers	Rechtsanwalt und Fachanwalt für Arbeitsrecht, Dentons, München
Prof. Dr. Michael Fuhlrott	Rechtsanwalt und Fachanwalt für Arbeitsrecht, Daten- schutzbeauftragter (TÜV) FUHLROTT Arbeitsrecht, Hamburg
Karl Geißler	Rechtsanwalt und Fachanwalt für Arbeitsrecht, T/S/C, Gütersloh
Dr. Christian Hoppe	Rechtsanwalt und Fachanwalt für Arbeitsrecht, Esche Schümann Commichau, Hamburg
Dr. Stefan Kramer	Rechtsanwalt und Fachanwalt für Arbeitsrecht, kramer arbeitsrecht, Hannover/Hamburg
Dr. Judith Neu	Rechtsanwältin und Fachanwältin für Arbeitsrecht sowie Syndikusrechtsanwältin bei der Knorr-Bremse Systeme für Schienenfahrzeuge GmbH, München
Dirk Petri	Rechtsanwalt und Fachanwalt für Strafrecht und Steuer- recht, Datenschutzbeauftragter (TÜV), verte/rechts- anwälte, Köln
Dr. Alexander Raif	Rechtsanwalt und Fachanwalt für Arbeitsrecht, GreenGate Partners, Berlin
Dr. Janine Schleper	Rechtsanwältin, Bird & Bird LLP, Hamburg
Dr. Kathrin Schulze Zumkley	Rechtsanwältin und Fachanwältin für Arbeitsrecht, T/S/C, Gütersloh
Prof. Christian Solmecke	Rechtsanwalt, WBS.LEGAL, Köln
Dr. Jens Tiedemann	Direktor des Arbeitsgerichts Bonn, Lehrbeauftragter an der Rheinischen Friedrich-Wilhelms-Universität, Bonn
Stephanie Törkel	Rechtsanwältin und Fachanwältin für Arbeitsrecht, BGHP, Berlin
Dr. Axel von der Straten	Richter am Arbeitsgericht, Stellv. Direktor des Arbeits- gerichts Hannover
Kathrin Wenzel	Rechtsanwältin und Fachanwältin für Arbeitsrecht sowie Syndikusrechtsanwältin bei MAN Truck & Bus Deutsch- land GmbH, München

Inhaltsübersicht

Autorinnen und Autoren des Handbuchs	V
Vorwort	VII
Vorwort zur ersten Auflage	VIII
Inhaltsverzeichnis	XI
Abkürzungsverzeichnis	XXXI
Literaturverzeichnis	XXXIX

§ 1 Digitalisierte Arbeitswelt

I. Bisherige Entwicklung	1
II. Arbeitsplatz und neue Arbeitsformen	4
III. Internet und Social Media	16
IV. Künstliche Intelligenz	19
V. Cybercrime und Prävention	25

§ 2 Individualarbeitsrecht

I. Betriebsstruktur und moderne Arbeitsformen	37
II. IT-Erklärungen im Arbeitsverhältnis	52
III. IT-Nutzung als Pflichtverletzung: Abmahnung und Kündigung	78
IV. Haftung des Arbeitnehmers im Rahmen der IT-Nutzung	182
V. Kontrolle der IT-Nutzung	188
VI. Prozessuale Verwertbarkeit von Kontrollergebnissen	211
VII. IT-Nutzung als Regelung im Arbeitsverhältnis	245
VIII. Mobile Arbeit: im Homeoffice und unterwegs	255
IX. Bring your own device (BYOD)	283
X. Einsatz von KI bei der Aufgabenerledigung	293
XI. Ständige Erreichbarkeit durch IT-Mittel und Arbeitsschutz	297
XII. Elektronische Personalakte	310
XIII. Einsatz von KI als Auswahlinstrument bei Personalmaßnahmen	322
XIV. IT-Einsatz und Compliance	342
XV. IT-Fortbildung im Arbeitsverhältnis	374
XVI. Digitalisierung von Krankmeldung und Krankschreibung	387
XVII. Cybercrime und Auswirkungen auf das Arbeitsverhältnis	393
XVIII. Robotereinsatz im Arbeitsverhältnis	405

§ 3 Kollektives Arbeitsrecht

I. Betriebsrat und Datenschutz	414
II. Betriebsverfassungsrechtliche Besonderheiten moderner Arbeitsformen	439
III. Einsatz von IT im Bereich des Betriebsverfassungsrechts	450
IV. Gestaltung des IT-Einsatzes durch Betriebsvereinbarungen	468
V. IT-Infrastruktur für die Betriebsratsarbeit	505
VI. IT-Fortbildung des Betriebsrats	519
VII. Digitaler Zugang der Gewerkschaft zum Betrieb	536

§ 4 Anwendung von IT und DS-GVO/KI-VO

I. Videoüberwachung	554
II. Ortungssysteme	603

Inhaltsübersicht

III. Biometrische Verfahren	632
IV. Einsatz von Kommunikations- und Kollaborationstools	659
§ 5 IT-Arbeitsstrafrecht	
I. Einleitung	680
II. Videoüberwachung am Arbeitsplatz	683
III. Überwachung der Kommunikation am Arbeitsplatz	699
IV. E-Mail und Internetüberwachung	710
V. Mitarbeiterüberwachung und Internal Investigations	718
VI. Strafbarkeit des Arbeitnehmers bei IT-Pflichtverletzungen	732
§ 6 Sozialversicherungs- und steuerrechtliche Behandlung der IT-Nutzung	
I. Sozialversicherungsrechtliche Behandlung der IT-Nutzung	739
II. Steuerrecht	742
Stichwortverzeichnis	747

Inhaltsverzeichnis

Autorinnen und Autoren des Handbuchs	V
Vorwort	VII
Vorwort zur ersten Auflage	VIII
Abkürzungsverzeichnis	XXXI
Literaturverzeichnis	XXXIX

§ 1 Digitalisierte Arbeitswelt (Solmecke)

I. Bisherige Entwicklung	1
II. Arbeitsplatz und neue Arbeitsformen	4
1. IT-Nutzung	4
2. Entgrenztes Arbeiten	5
a) Home- und Mobile-Office	6
b) Vertrauensarbeit	8
3. BYOD	8
4. Crowdfunding/Crowdsourcing	9
5. Job Sharing	12
6. Desk Sharing	13
7. Cloud Computing	13
8. Economy on Demand	15
9. Scrum	16
III. Internet und Social Media	16
IV. Künstliche Intelligenz	19
1. Heutiger Einsatz von KI in der Arbeitswelt	20
2. Herausforderungen im Umgang mit KI	22
3. Perspektive: Wie könnte KI zukünftig die Arbeitswelt verändern?	24
V. Cybercrime und Prävention	25

§ 2 Individualarbeitsrecht

I. Betriebsstruktur und moderne Arbeitsformen (Fuhlrott)	37
1. Einleitung	37
2. Herkömmlicher Betriebsbegriff	38
a) Betriebsverfassungsrechtlicher Betriebsbegriff	39
aa) Konstitutive Voraussetzungen	39
bb) Weitere Indizien	40
cc) Fiktionen des BetrVG	40
b) Kündigungsschutzrechtlicher Betriebsbegriff	41
c) Betriebsbegriff bei anzeigepflichtigen Entlassungen	41
d) Betriebsübergangsrechtlicher Betriebsbegriff	41
e) Gemeinschaftsbetriebe	42
3. Bedeutung des Betriebsbegriffs im Individualarbeitsrecht	42
a) Shop-in-shop-Konzepte	43
b) Homeoffice und mobiles Arbeiten	43
c) Matrixstrukturen	44
d) Desk-Sharing	45
e) Co-Working-Spaces	46

f) Crowdfunding und Plattformökonomie	48
g) Virtuelle Unternehmen und Betriebe	52
II. IT-Erklärungen im Arbeitsverhältnis (<i>von der Straten</i>)	52
1. Zweck von Formerfordernissen	53
2. Formenkatalog	53
a) Notarielle Urkunde	54
b) Schriftform	54
c) Elektronische Form	55
aa) Funktionsweise	55
bb) Verhältnis zur Schriftform	57
d) Textform	59
e) Formfreie Erklärungen	60
3. Folgen eines Formverstößes	60
a) Formvorgabe aufgrund gesetzlicher Regelung	60
b) Vertraglich vereinbarte Formvorschrift	61
c) Vereinbarte Formvorschrift in einem Tarifvertrag	61
d) Treuwidrigkeit	62
4. Zugang	62
5. Situationen, in denen die Formeinhaltung relevant ist	64
a) Abmahnung	64
b) Änderungskündigung	65
c) Arbeitnehmerüberlassung	65
d) Arbeitsvertrag, Änderungsvereinbarungen	65
e) Arbeitsvertragsnachweis	65
f) Aufhebungsvertrag	66
g) Ausbildungsvertrag	66
h) Ausschlussfristen: Geltendmachung von Ansprüchen	66
i) Befristung	67
j) Betriebsübergang	67
k) Diskriminierung: Geltendmachung von Ansprüchen	68
l) Elternzeit	69
m) Entgelttransparenzgesetz	70
n) Familienpflegezeit	71
o) Kündigung, Änderungskündigung	71
p) Pflegezeit	72
q) Sonderlösungsrecht	72
r) Exkurs: Tarifvertrag	73
s) Teilzeit	73
t) Nachvertragliches Wettbewerbsverbot	74
u) Zeugnis	76
v) Zweckbefristung	76
6. Überblick: Wichtige formbedürftige Erklärungen im Arbeitsverhältnis ...	77
III. IT-Nutzung als Pflichtverletzung: Abmahnung und Kündigung	78
1. IT als Betriebsmittel (<i>Wenzel</i>)	78
a) Arten von IT-Betriebsmitteln	78
b) Anspruch auf IT-Betriebsmittel	78
aa) Individualvertraglicher Anspruch	79
bb) Betriebliche Übung	79
cc) Kollektiver Anspruch: Betriebsvereinbarung	80
c) Herausgabeansprüche des Arbeitgebers und Widerruf der Nutzungserlaubnis	80
aa) Beendigung des Arbeitsverhältnisses	80

bb) Freistellung	81
cc) Entfallen der dienstlichen Notwendigkeit der Betriebsmittel	82
dd) Pflichtverstöße im Zusammenhang mit der IT-Nutzung	83
2. Privatnutzung und betriebliche Übung (<i>Wenzel</i>)	83
a) Abgrenzung berufliche und private Nutzung	83
b) Erlaubnis der Privatnutzung	84
aa) Anspruch auf Privatnutzung	84
bb) Ausdrückliche Gestattung	85
cc) Duldung und Betriebliche Übung	86
c) Nachträgliche Untersagung der Privatnutzung	88
aa) Freiwilligkeitsvorbehalt	88
bb) Widerrufsvorbehalte	89
3. Passwortmissbrauch (<i>Wenzel</i>)	90
a) Hintergrund des Passwortschutzes	90
b) Vertragliche Regelung zur Verwendung von Passwörtern	91
c) Pflichtverstöße bei der Passwortnutzung	92
d) Arbeitsrechtliche Sanktionsmöglichkeiten	92
aa) Abmahnung	93
bb) Kündigung	93
4. Weitergabe sensibler IT-Daten (<i>Wenzel</i>)	95
a) Begriff der sensiblen IT-Daten	95
aa) Begriff der personenbezogenen Daten	95
bb) Begriff der unternehmensbezogenen Daten	96
b) Geheimhaltungspflichten des Mitarbeiters	96
c) Arbeitsrechtliche Sanktionsmöglichkeiten	97
aa) Bewusste Weitergabe von sensiblen IT-Daten	97
bb) Unbewusste Weitergabe von Daten und Vorbereitungshandlungen	98
5. Private Telefon- und Handy-Nutzung (<i>Neu</i>)	99
a) Zulässigkeit der privaten Telefon- und Handy-Nutzung	99
aa) Ausdrücklich verbotene Privatnutzung	99
bb) Konkludentes Verbot	99
cc) Fehlen einer Nutzungsregel	100
dd) Erlaubte Privatnutzung	100
ee) Konkludente Nutzungserlaubnis	102
ff) Betriebliche Übung	103
gg) Betriebsvereinbarung	103
b) Rechtsfolgen einer unzulässigen privaten Telefon- und Handynutzung	105
aa) Ermahnung	105
bb) Abmahnung	105
cc) Ordentliche Kündigung	107
dd) Außerordentliche Kündigung	108
ee) Schadensersatzansprüche des Arbeitgebers	111
ff) Rücknahme der privaten Nutzungserlaubnis	111
6. Private Internetnutzung am Arbeitsplatz (<i>Hoppe</i>)	111
a) Private Internetnutzung als Chance und Risiko für den Arbeitgeber	111
aa) Steigerung von Arbeitsmotivation und -effizienz der Belegschaft	112
bb) Gewährleistung der Funktionsfähigkeit betrieblicher Abläufe	112
b) Nutzungserlaubnis und -verbot als Maßstab für die Beurteilung der Schwere der Pflichtverletzung	113
aa) Gestattung der Privatnutzung	113
bb) Ausdrückliches Verbot	114
cc) Fehlen einer Nutzungsregelung	115

c) Kündigungsrelevanz privater Internetnutzung am Arbeitsplatz: Maßstäbe höchstrichterlicher Rechtsprechung	115
d) Fallgruppen in der Instanzrechtsprechung	119
aa) Verletzung der Hauptleistungspflicht	119
bb) Nutzung trotz entgegenstehenden ausdrücklichen Nutzungsverbots	121
cc) „Ausschweifende“ Nutzung bei Fehlen eines Privatnutzungsverbots	123
dd) Problematische Nutzungsinhalte: Gefährdung der Unternehmensreputation	125
e) Rücknahme der privaten Nutzungserlaubnis	128
f) Zusammenfassung	129
7. Private E-Mail-Nutzung (<i>Byers</i>)	131
a) Kontrollmöglichkeiten	131
b) Arbeitsrechtliche Sanktionsmöglichkeiten bei unzulässiger Nutzung von E-Mail	133
aa) Einzelfälle möglicher Pflichtverstöße	135
bb) Schadensersatzansprüche des Arbeitgebers	139
cc) Rücknahme der Erlaubnis zur Privatnutzung	140
8. Private Nutzung betrieblicher Hard- und Software (<i>Byers</i>)	140
a) Hard- und Softwarenutzung am Arbeitsplatz zu privaten Zwecken	140
b) Verbot der Speicherung privater Dateien	141
c) Kontrollmöglichkeiten	141
d) Pflichtverstöße	142
aa) „Privatarchiv“ auf der Festplatte des dienstlichen PC	143
bb) Private Software auf dem dienstlichen PC	143
cc) Privatnutzung von Speichermedien	144
dd) Anfertigung von Raubkopien	145
9. Posting in sozialen Netzwerken (<i>Kramer</i>)	145
a) Formen von Postings	146
b) Verletzung einer arbeitsvertraglichen Pflicht	146
c) Pflichtverletzungsrelevante Schnittstellen zum Arbeitsverhältnis	146
aa) Privates Posting am Arbeitsplatz	146
bb) Geheimhaltungsrelevante Postings	147
cc) Arbeitsrechtliche Fernwirkung von Statusmeldungen	147
dd) Den Arbeitgeber, Vorgesetzte oder Kollegen beleidigende und kritisierende Postings	147
ee) Kundenbezogene geschäftsschädigende und allgemein rufschädigende Postings	150
ff) Nutzung des „Gefällt mir“-Buttons	151
gg) Zugehörigkeit zu einer gegen den Arbeitgeber gerichteten Facebook-Gruppe	151
d) Reaktionsmöglichkeiten des Arbeitgebers	151
aa) Rüge	151
bb) Abmahnung	152
cc) Ordentliche Kündigung	153
dd) Außerordentliche Kündigung	154
e) Verwertung von Postings im Prozess	155
10. Vorgehen bei IT-Tat- und Verdachtskündigung (<i>Eylert/Barrein</i>)	156
a) Einleitung	156
b) Grundlagen von Tat- und Verdachtskündigung	157
aa) Die Verdachtskündigung	158
bb) Zum Verhältnis von Verdachts- und Tatkündigung einerseits und von außerordentlicher und ordentlicher Verdachtskündigung andererseits	159

cc) Die Voraussetzungen einer Verdachtskündigung	161
dd) Die Kündigungserklärungsfrist (§ 626 Abs. 2 BGB)	168
c) Tatsachenfeststellungen als Basis für einen möglichen Kündigungsgrund	169
aa) Die Aufklärung des kündigungsrelevanten Sachverhalts	170
bb) Die Beteiligung der Interessenvertretung	176
d) Mögliche Reaktionsmöglichkeiten des Arbeitnehmers	176
e) Weitere Besonderheiten einer IT-Verdachtskündigung im Kündigungsschutzprozess	177
aa) Übergehen von Verdachts- zur Tatsachenkündigung während des Kündigungsschutzprozesses	177
bb) Ausspruch einer weiteren Kündigung und Nachschieben von Kündigungsgründen im Kündigungsschutzprozess	178
cc) Beweis- und Sachverhaltsverwertungsverbote	179
dd) Aussetzung des arbeitsgerichtlichen Verfahrens bis zum Abschluss des Strafverfahrens?	181
IV. Haftung des Arbeitnehmers im Rahmen der IT-Nutzung (<i>Hoppe</i>)	182
1. Grundlagen der Haftung im Arbeitsverhältnis	183
2. Anspruchsgrundlagen	183
3. Übertragung der Haftungsgrundsätze auf die IT-Nutzung	185
a) Haftung bei dienstlicher Nutzung sowie bei gestatteter Privatnutzung ..	185
b) Haftung bei Privatnutzung trotz Verbots	186
c) Berücksichtigung eines Mitverschuldens des Arbeitgebers	187
4. Schadensersatzanspruch des Arbeitgebers für vertragswidrig verwendete Arbeitszeit?	187
5. Zusammenfassung	188
V. Kontrolle der IT-Nutzung (<i>Oberthür/Schleper</i>)	188
1. Rechtliche Grundlagen	188
2. Personenbezug der Kontrolldaten	190
3. Kontrollmaßnahmen bei untersagter Privatnutzung	190
a) Gesetzliches Verbot mit Erlaubnisvorbehalt	191
b) Rechtsgrundlage: Einwilligung des Arbeitnehmers	191
aa) Freiwilligkeit der Einwilligungsentscheidung	191
bb) Schriftform und Inhalt der Einwilligung	192
cc) Widerruf der Einwilligung	192
c) Rechtsgrundlage: Kollektivvereinbarung	193
aa) Zulässigkeit eigenständiger Datenschutzregelungen	193
bb) Wahrung eines angemessenen Datenschutzniveaus	193
d) Gesetzliche Ermächtigungsnormen	194
aa) Präventive Kontrollmaßnahmen	195
bb) Repressive Kontrollmaßnahmen	197
e) Transparenz der Datenerhebung	198
f) Zulässigkeit einzelner Kontrollmaßnahmen	199
aa) Zugang zum Internet	199
bb) E-Mail-Dienste	199
cc) (Mobil-)Telefonie	200
dd) Social Media	201
4. Kontrollmaßnahmen bei erlaubter Privatnutzung	202
a) Anwendungsbereich des TDDDG	202
b) Arbeitgeber als Diensteanbieter	202
c) Wahrung des Fernmeldegeheimnisses	203
aa) Schutzgegenstand des Fernmeldegeheimnisses	203

bb) Zeitlicher Schutzbereich des Fernmeldegeheimnisses	204
cc) Auswirkungen des Fernmeldegeheimnisses	204
d) Datenschutzrechtliche Vorgaben	204
e) Einwilligung des Arbeitnehmers	205
f) Zulässigkeit einzelner Kontrollmaßnahmen	206
aa) Zugang zum Internet	206
bb) E-Mail-Dienste	206
cc) (Mobil-)Telefonie	207
dd) Soziale Netzwerke	207
5. Kontrollmaßnahmen gegenüber Betriebsratsmitgliedern	208
6. Folgen einer unzulässigen Kontrolle für den Arbeitgeber	208
a) Straf- und bußgeldrechtliche Folgen	208
aa) Verstoß gegen das Fernmeldegeheimnis	208
bb) Verstoß gegen datenschutzrechtliche Bestimmungen	209
b) Schmerzensgeldansprüche	209
c) Folgen für den Bestand des Arbeitsverhältnisses	210
aa) Unterlassungsansprüche	210
bb) Außerordentliche Arbeitnehmerkündigung	210
cc) Auflösungsantrag	211
VI. Prozessuale Verwertbarkeit von Kontrollergebnissen (<i>Tiedemann</i>)	211
1. Praktischer Problemaufriss im arbeitsgerichtlichen Verfahren	213
2. Verfassungs- und unionsrechtliche sowie weitere Aspekte eines prozessualen Verwertungsverbots	215
a) Mangelnde gesetzliche Regelung und prozessuales Verwertungsverbot als Ausnahmefall	215
b) Grundrechtsbindung der Gerichte und Eingriff in Grundrechte	216
c) Güter- und Interessenabwägung	217
d) Unionsrechtliche Aspekte und EMRK	219
e) Sachvortrags- und/oder Beweisverwertungsverbot	224
f) Umfang eines prozessualen Verwertungsverbots und Fernwirkung	225
3. Ausgewählte Sachgruppen und Einzelfälle	226
a) Verstoß gegen Mitbestimmungsrechte des Betriebsrates und Vereinbarung eines Verwertungsverbots	227
b) Verstoß gegen Bestimmungen der DS-GVO und des BDSG	229
c) Offene Videoüberwachung	231
d) Verdeckte bzw. heimliche Videoüberwachung	232
e) Mithören und Aufzeichnen von Telefonaten und Gesprächen	234
f) Heimliche Spind- bzw. Schrankdurchsuchung	235
g) Überwachung durch Keylogger 236	
h) Verwendung automatisiert erstellter digitaler Zeitstempel in Dateien/ Datenbanken	237
i) Verwendung von Chatprotokollen, E-Mails und WhatsApp- Nachrichten	237
j) Einblick in elektronischen Kalender	239
k) GPS-Daten und Bewegungsprofil	239
l) Einsicht in (kennwortgeschützte) Dateien/Ausspähen von Daten	240
m) Einsicht in Browser-Chronik bzw. Browser-Verlauf	241
n) Zufallsfunde	242
o) (Video- und Ton-)Aufzeichnungen einer Dashcam	243
p) Auswertung von Daten eines Zutrittskontrollsystems	244
4. Folgen eines prozessualen Verwertungsverbots	244

VII. IT-Nutzung als Regelung im Arbeitsverhältnis (<i>Byers</i>)	245
1. Erfordernis einer arbeitsvertraglichen Regelung	245
a) Betriebliche Übung	245
b) Eingeschränkte Kontrollmöglichkeiten der Privatnutzung	245
c) Erschwerte Sanktionsmöglichkeit bei fehlender IT-Nutzungsregelung	246
2. Gestaltungsmöglichkeiten der IT-Nutzung	247
a) Überlassungszweck	247
aa) Ausschließlich dienstliche Nutzung	247
bb) Erlaubte private Nutzung	248
b) Nutzungsvereinbarungen bei erlaubter Privatnutzung	249
aa) Zeitliche Beschränkungen	249
bb) Inhaltliche Beschränkungen	249
cc) Vertretungsregelungen beim E-Mail-Postfach	251
c) Sicherheitsbezogene Regelungen	252
aa) Verwendung von Passwörtern	252
bb) Verwendung von Spam- und Virenfiltern	252
d) Regelung zur Protokollierung und Kontrolle	253
VIII. Mobile Arbeit: im Homeoffice und unterwegs (<i>Hoppe</i>)	255
1. Umfang und Beendigungsmöglichkeiten („Back to the Office“)	257
2. Mobilarbeit im Homeoffice: Ausstattung und Haftungsfragen	261
3. Aufwendungsersatz und Fahrtkosten; Homeoffice-Pauschale	262
4. Arbeitszeit: Umfang und Grenzen	264
5. Datenschutzrechtliche Rahmenbedingungen	266
6. Arbeitsschutzrechtliche Vorgaben	268
7. Unfallversicherungsschutz im Homeoffice, Gerichtsstand bei Streitigkeiten	269
8. Mitbestimmung des Betriebsrats	271
9. Mobilarbeit und Workation im Ausland	274
10. Muster: Vereinbarung über Mobilarbeit	277
IX. Bring your own device (BYOD) (<i>Hoppe</i>)	283
1. Personalpolitische Dimension und Erscheinungsformen	283
2. Einführung von BYOD im Arbeitsverhältnis	284
3. Datenschutz und Informationssicherheit	286
4. Administration des IT-Endgerätes und Grenzen der Nutzungsüberwachung	288
5. Mitbestimmung des Betriebsrats	289
6. Haftungsfragen, Urheberrecht und arbeitszeitrechtliche Behandlung	290
7. Gestaltungshinweise für eine BYOD-Policy	291
X. Einsatz von KI bei der Aufgabenerledigung (<i>Kramer</i>)	293
1. Zulässigkeit des KI-Einsatzes durch den Arbeitnehmer	293
a) KI-Nutzungsvorgaben des Arbeitgebers	294
b) Regelungsloser Zustand	294
c) Arbeitsrechtliche Folgen einer unzulässigen KI-Nutzung für den Arbeitnehmer	295
d) Checkliste für eine Chatbot-Nutzungsregel	295
2. Zulässigkeit einer Aufgabenzuweisung durch KI an den Arbeitnehmer	296
XI. Ständige Erreichbarkeit durch IT-Mittel und Arbeitsschutz (<i>Kramer</i>)	297
1. IT-Einsatz und Arbeitszeit	298
a) Vollarbeit	298
b) Arbeitsbereitschaft	299
c) Bereitschaftsdienst	299
d) Rufbereitschaft	299

e) Zwingender öffentlich-rechtlicher Rechtsrahmen	300
f) Ruhezeit	301
g) Einordnung von Freizeittätigkeit	302
aa) Eigeninitiative freiwillige Freizeittätigkeit ohne Kenntnis des Arbeitgebers	302
bb) Freizeittätigkeit gegen den ausdrücklichen Willen des Arbeitgebers	303
cc) Freizeittätigkeit in Kenntnis oder mit Duldung des Arbeitgebers ...	303
dd) Freizeittätigkeit im eigenen Interesse und reine Gefälligkeiten	304
h) Einordnung der jederzeitigen Erreichbarkeit	304
aa) Weisung zur Erreichbarkeit per IT-Mittel	305
bb) Ausnahmefall: Bindung an Homeoffice	305
i) Freizeittätigkeit und Rechte des Betriebsrats	305
2. Beeinträchtigung des Urlaubsanspruchs durch IT-Einsatz	306
a) Urlaubsrechtliche Ausgangslage	306
b) Urlaubstätigkeit	307
aa) Eigeninitiative freiwillige Urlaubstätigkeit	307
bb) Angewiesene oder erwartete Urlaubstätigkeit	307
c) Ständige Erreichbarkeit und Urlaub	307
aa) Ausdrückliche Weisung zur Erreichbarkeit	308
bb) Nicht vereinbarte, freiwillige Erreichbarkeit im Urlaub	308
3. Konsequenzen für Arbeitgeber und Arbeitnehmer	309
a) Arbeitgeber	309
b) Arbeitnehmer	310
XII. Elektronische Personalakte (<i>Raif</i>)	310
1. Grundsätze der Aktenführung	311
a) Führungsbefugnis	311
b) Wahrheitspflicht	312
c) Vollständigkeit	312
d) Vertraulichkeit und Datenschutz	312
2. Inhalt der Personalakte	314
3. Rechte der Arbeitnehmer	316
a) Einsichtsrecht des Arbeitnehmers	316
b) Erklärungen des Arbeitnehmers zur Personalakte	317
4. Ansprüche des Arbeitnehmers	318
a) Entfernungsanspruch	318
b) Weitere Arbeitnehmeransprüche	320
5. Aufbewahrungspflichten und Rechtslage nach Ende des Arbeitsverhältnisses	320
6. Mitbestimmung des Betriebsrates bei Einführung der E-Akte	321
XIII. Einsatz von KI als Auswahlinstrument bei Personalmaßnahmen (<i>Geißler</i>)	322
1. KI als Auswahlhilfe	322
a) KI-Einsatz bei der Informationsbeschaffung – Chancen, Risiken und Notwendigkeiten	322
b) Nutzung entscheidender IT – als automatisierte Einzelentscheidung verboten?	324
c) Diskriminierungsrechtliche Bedenken	328
d) Implikationen der KI-VO	331
2. IT-Einsatz in konkreten Auswahlprozessen	332
a) IT-Einsatz bei Einstellungsentscheidungen	332
aa) „Einfache“ Bewerbermanagementsysteme	333
bb) Pre-Employment-Screening in Internet und Social Media	335
cc) Roborecruiting/Einsatz von Analysesoftware	336

dd) People Analytics	337
ee) Bewerberscoring	338
ff) Betriebsratsbeteiligung – unabdingbar aber unpraktikabel	339
b) Auswahlentscheidungen im ungekündigten Arbeitsverhältnis	339
aa) Schutz des Persönlichkeitsrechts	339
bb) Kollektiver Schutz	340
cc) Anwendungsfälle der KI-Nutzung	341
c) Einsatz bei Beendigungsentscheidungen	342
XIV. IT-Einsatz und Compliance (<i>Schulze Zumkley</i>)	342
1. Einführung	342
a) Compliance im Arbeitsrecht	342
b) Der Begriff „Compliance“	343
2. Compliance-Organisation	343
a) Rechtsgrundlagen und Pflichtenkanon	344
aa) Spezialgesetzliche Regelungen	344
bb) Mittelbare Pflichten	344
b) Ziele der Compliance(-Maßnahmen)	346
c) Ausrichtung und Anforderungen an Compliance-Systeme	347
aa) Adressatenkreis	347
bb) Anforderungen an ein Compliance-System	348
cc) Ausgestaltung eines Compliance-Systems	353
dd) Mitbestimmungsrechte	355
3. Compliance-Tools	356
a) Präventive Tools	356
aa) Code of Conduct	356
bb) Schulungen	358
cc) Bewerber-Kontrolle: Background-Check und Pre Employment Screening	361
b) Ermittlung von (möglichem) Fehlverhalten	363
aa) Einsatz von „Spyware“	363
bb) Analyse des Telefonverhaltens	364
cc) E-Mail-Screening	365
dd) Mitarbeiterbefragung	366
ee) Interne Meldesysteme	367
ff) KI-gestützte Prozesse in Meldestellen und internen Untersuchungen	371
XV. IT-Fortbildung im Arbeitsverhältnis (<i>von der Straten</i>)	374
1. Weiterbildungsanspruch des Arbeitnehmers?	375
a) Weiterbildung und Beschäftigungsanspruch	375
b) Besondere Beschäftigtengruppen	376
aa) Teilzeitbeschäftigte und befristet beschäftigte Arbeitnehmer	376
bb) Schwerbehinderte Menschen	376
c) Vereinbarungen zwischen Arbeitgeber und Arbeitnehmer	377
d) Art. 4 KI-VO: Besondere Verpflichtung des Arbeitgebers?	377
2. Pflicht des Arbeitnehmers zur Weiterbildung?	378
a) Fortbildung außerhalb der Arbeitszeit	379
b) Fortbildung während der Arbeitszeit	379
3. Schulungskostenvereinbarungen	380
a) Grundsätze	380
aa) Form	381
bb) Anlass: Anforderung an die Bildungsmaßnahme	381
cc) Transparenz bezüglich der Kosten und des Rückzahlungsbetrags ..	381

dd) Transparenz bezüglich des Beendigungsgrundes	382
ee) Bindungsdauer: angemessenes Verhältnis der beiderseitigen Interessen	383
ff) Checkliste	384
gg) Grenzüberschreitende Arbeitsverhältnisse	384
b) Folgen eines Verstoßes	384
c) Ausbildungsverhältnis	385
4. Auswirkung einer Fortbildung auf Kündigungen	385
a) Betriebsbedingte Kündigung	385
b) Kündigung wegen Leistungsmängeln	386
5. Möglichkeit der Inanspruchnahme von Fördermitteln	386
XVI. Digitalisierung von Krankmeldung und Krankschreibung (<i>Kramer</i>)	387
1. Mitteilungspflicht	387
a) Adressat, Inhalt und Zeitpunkt der Krankmeldung	387
b) Mitteilung per IT	388
2. Nachweispflicht	389
a) Grundsatz: eAU statt „gelber Schein“	389
b) Ausnahmen vom eAU-Verfahren	390
3. Virtuelle Krankschreibung	390
a) Per Video	390
b) Online	391
c) Per Telefon	392
4. Mitbestimmung des Betriebsrats	392
5. Muster-Regelung	393
XVII. Cybercrime und Auswirkungen auf das Arbeitsverhältnis (<i>Barrein</i>)	393
1. Prävention und Vorkehrungen zur Vermeidung von Cybervorfällen	394
2. Umgang mit Cybervorfällen aus Arbeitgeberpersicht	394
a) Neuausübung des Direktionsrechts	395
b) Erweiterung des Direktionsrechts aus dem Arbeitsvertrag	395
c) Direktionsrechtserweiterung aufgrund einer Notsituation	396
aa) Arbeitsort	397
bb) Arbeitszeitlage und Arbeitszeitvolumen (Verlängerung der Arbeitszeit/Anordnung von Kurzarbeit)	398
cc) Arbeitsinhalt	400
d) Vergütung	401
e) Schadensersatz	402
aa) Grundsätze innerbetrieblichen Schadensausgleichs	402
bb) Höhe des Schadensersatzanspruchs/Verschuldensgrad	402
cc) Versicherung	403
dd) Mitverschulden	404
f) Sanktionierung: Kündigung oder Abmahnung?	404
3. Mitbestimmungsrecht des Betriebsrates	404
XVIII. Robotereinsatz im Arbeitsverhältnis (<i>Tiedemann</i>)	405
1. Weisungsrecht	405
2. Arbeits- und Gesundheitsschutz	406
3. Haftung	407
4. Mitbestimmung	408

§ 3 Kollektives Arbeitsrecht

I. Betriebsrat und Datenschutz (<i>Raif</i>)	414
1. Kontroll- und Gestaltungsrechte des Betriebsrats	414
a) Funktion des Betriebsrats beim Arbeitnehmerdatenschutz	414
b) Schutz- und Förderungsgebot nach § 75 Abs. 2 BetrVG	414
c) Überwachungspflicht des Betriebsrats nach § 80 Abs. 1 BetrVG	415
d) Informationsrechte des Betriebsrats	416
aa) Allgemeiner Informationsanspruch nach § 80 Abs. 2 S. 1 BetrVG	416
bb) Besondere Informationsrechte des Betriebsrats	418
e) Beratungsrechte	419
aa) Beratungen über Änderungen der Arbeitsplatzumgebung	419
bb) Personalplanung	419
f) Zustimmungsrechte des Betriebsrats	420
aa) Personalfragebögen	420
bb) Auswahlrichtlinien	422
g) Zustimmungsverweigerungsrecht des Betriebsrats nach § 99 BetrVG	424
h) Erzwingbare Mitbestimmung	425
aa) Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb	425
bb) Mitbestimmung bei Technischen Einrichtungen (§ 87 Abs. 1 Nr. 6 BetrVG)	427
2. Betriebsrat als Datenschutzverpflichteter	430
a) Datenschutzverpflichtung des Betriebsrats	430
b) Kontrolle der datenschutzrechtlichen Pflichten des Betriebsrats	432
c) Schweigepflichten der Betriebsratsmitglieder	434
aa) Allgemeine Verschwiegenheitspflichten	434
bb) Spezielle Schweigepflichten	435
3. Willensbildung und Kommunikation des Betriebsrats	435
a) Kommunikation zwischen Arbeitgeber und Betriebsrat	436
b) Betriebsratsinterne Willensbildung und Kommunikation	436
c) Kommunikation zwischen Betriebsrat und Arbeitnehmern sowie Dritten	438
d) Praktische Umsetzung	438
II. Betriebsverfassungsrechtliche Besonderheiten moderner Arbeitsformen (<i>Fuhlrott</i>)	439
1. Betriebsbegriff: Veränderungen und Einflüsse moderner Arbeitsformen	439
a) Co-Working-Spaces	440
b) Crowdfunding	440
2. Beteiligungsrechte bei der Einführung moderner Arbeitsformen	442
a) Überwachungsauftrag und Informationsrecht, § 80 BetrVG bzw. § 106 BetrVG	442
b) Personelle Einzelmaßnahmen, insbesondere Versetzung, § 99 Abs. 1 BetrVG	443
c) Mitbestimmung in sozialen Angelegenheiten, § 87 Abs. 1 BetrVG	444
aa) Ordnung des Betriebs, § 87 Abs. 1 Nr. 1 BetrVG	444
bb) Arbeitszeitgestaltung, § 87 Abs. 1 Nr. 2 und 3 BetrVG	445
cc) Technische Einrichtung, § 87 Abs. 1 Nr. 6 BetrVG	445
dd) Verhütung von Arbeitsunfällen und Berufskrankheiten, § 87 Abs. 1 Nr. 7 BetrVG	446
ee) Ausgestaltung von mittels Informations- und Kommunikationstechnik erbrachter mobiler Arbeit, § 87 Abs. 1 Nr. 14 BetrVG	447

d) Unterrichtung und Verhandlung bei Betriebsänderungen, § 111 BetrVG	447
aa) Schwellenwerte und Arbeitnehmerbetroffenheit	448
bb) Vorliegen einer Betriebsänderung	448
cc) Rechtliche Folgen	449
e) Beratungs- und Mitbestimmungsrecht gemäß §§ 90 f. BetrVG	449
III. Einsatz von IT im Bereich des Betriebsverfassungsrechts (<i>Neu</i>)	450
1. Betriebsratswahl	450
a) Bestellung des Wahlvorstands	450
b) Beschlussfassung des Wahlvorstands	450
c) Erlass und Bekanntmachung des Wahlausschreibens	451
d) Bekanntmachung der Wählerliste und der Wahlordnung	452
e) Einspruch gegen die Wählerliste	453
f) Einreichung und Bekanntmachung von Vorschlagslisten und Wahlvorschlägen	454
g) Stimmabgabe	454
h) Benachrichtigung der Gewählten	455
i) Bekanntgabe des Wahlergebnisses	456
2. Betriebsratsbeschluss	456
a) Einladung zur Betriebsratssitzung	456
b) Durchführung der Betriebsratssitzung	457
c) Beschlussfassung des Betriebsrats	458
3. Mitwirkung und Mitbestimmung des Betriebsrats	459
a) Unterrichtung und Information	459
b) Abschluss von Betriebsvereinbarungen	460
c) Interessenausgleich	460
d) Sozialplan	461
e) Einigungsstelle	461
aa) Verhandlung vor der Einigungsstelle	461
bb) Beschlüsse der Einigungsstelle	461
f) Unterrichtung des Wirtschaftsausschusses	462
4. Personelle Einzelmaßnahmen	462
a) Beteiligung des Betriebsrats bei Einstellung, Versetzung, Eingruppierung oder Umgruppierung	462
b) Vorläufige personelle Maßnahme	463
c) Mitbestimmung des Betriebsrats bei Kündigungen	463
d) Kündigung von Betriebsratsmitgliedern und Mitgliedern besonderer Interessenvertretungen	464
e) Entfernung betriebsstörender Arbeitnehmer	465
f) Mitteilung des Arbeitgebers bei personellen Maßnahmen von leitenden Angestellten	465
5. Übersicht	466
IV. Gestaltung des IT-Einsatzes durch Betriebsvereinbarungen (<i>Raif</i>)	468
1. Betriebsvereinbarung als Gestaltungsinstrument	469
2. Gestaltungsgrenzen für IT-Betriebsvereinbarungen	470
a) Europarechtliche Vorgaben (DS-GVO)	470
b) Vorgaben aus Grundrechten	471
c) Vorgaben nach dem BDSG	471
d) Gestaltungsgrenzen aufgrund § 75 BetrVG	472
aa) Recht und Billigkeit	472
bb) Schutz- und Förderungsgebot	474

3. Gestaltung typischer IT-Betriebsvereinbarungen/Checklisten	475
a) IT-Nutzung im Betrieb und bei mobile Work	476
b) Videoüberwachung	478
c) GPS-Ortungssysteme	479
d) Biometrische Zugangskontrolle	481
e) Elektronische Personalakte	483
f) Künstliche Intelligenz in der Personalarbeit	484
g) Social Media Guidelines	485
h) Microsoft 365 (MS 365) (<i>Tiedemann</i>)	493
4. Mitbestimmung des BR beim Einsatz von KI (<i>Raif</i>)	498
a) Informationsanspruch nach § 80 Abs. 2 BetrVG	498
b) Informations- und Beratungsrecht nach § 90 BetrVG	499
c) Personelle Mitbestimmung bei KI	500
d) Soziale Mitbestimmung bei KI	501
(1) KI als mitbestimmungspflichtige technische Einrichtung (§ 87 Abs. 1 Nr. 6 BetrVG	501
(2) Zusätzliche Mitbestimmung nach § 87 BetrVG	503
e) Wirtschaftliche Mitbestimmung bei KI	504
f) KI-Anwendung als Sachmittel (§ 40 Abs. 2 BetrVG)	505
V. IT-Infrastruktur für die Betriebsratsarbeit (<i>Kramer</i>)	505
1. Sachmittelanpruch des Betriebsrats	506
a) IT als Sachmittel	506
b) Erforderlichkeit und Interessenabwägung	506
c) Beschlussfassung des Betriebsrats	507
d) Reaktionsmöglichkeiten des Arbeitgebers	508
e) Gerichtliche Auseinandersetzung	509
2. „IT-Grundausrüstung“ des Betriebsrats	510
a) Grundsätze	510
b) „Regelausrüstung“ im Einzelnen	510
3. Einzelfallbedingt beanspruchbare spezielle IT-Mittel	514
4. Regelungsbedarf für IT-Mittel des Betriebsrats in Betriebsvereinbarungen	516
a) Wege des Kommunikationsschutzes	516
b) Klauselbeispiele	517
5. Zulässiger Nutzungsumfang der IT-Mittel des Betriebsrats	517
6. Zukünftige Entwicklung des Anspruchs auf IT-Mittel	518
7. Schnellübersicht: Anspruch des Betriebsrats auf IT-Mittel	519
VI. IT-Fortbildung des Betriebsrats (<i>Tiedemann</i>)	519
1. Erforderlichkeit und IT-bezogener Gegenstand der Fortbildung	521
2. Teilnehmeranzahl und Mitteilung an den Arbeitgeber	524
3. Träger der Fortbildungsveranstaltung und Referenten	525
4. Zeitliche Lage und Dauer der Fortbildung sowie Mitteilung an den Arbeitgeber	525
5. Format der Schulung	526
6. Beurteilungsspielraum des Betriebsrats und gerichtlicher Prüfungsmaßstab	526
7. Kostentragung durch den Arbeitgeber	529
8. Anspruchsberechtigung bei § 37 Abs. 6 BetrVG	530
9. Entgeltfortzahlung	530
10. Freizeitausgleich	531
11. Streitigkeiten	532
a) Einigungsstellenverfahren	532
b) Streitigkeiten über das Arbeitsentgelt bzw. den Freizeitausgleich	532

c) Streitigkeiten über die Erforderlichkeit, die Freistellung oder die Kostenübernahme	532
aa) Hauptsacheverfahren	533
bb) Einstweiliger Rechtsschutz	534
cc) Kostenrechtliche Hinweise	535
VII. Digitaler Zugang der Gewerkschaft zum Betrieb (<i>Neu</i>)	536
1. Zulässigkeit von Gewerkschaftswerbung und -mitteilung im Betrieb	536
a) Das Grundrecht auf Koalitionsfreiheit	536
b) Das Recht auf Werbung und Mitgliederinformation im Betrieb	537
2. Gewerkschaftswerbung per E-Mail	538
a) Beeinträchtigung einzelner Arbeitnehmer	538
b) Beeinträchtigung des Arbeitgebers	539
aa) Rechtsprechung des Bundesarbeitsgerichts	539
bb) Kritik der Literatur	540
c) Grenzen der elektronischen gewerkschaftlichen Betätigung	541
aa) Unzulässige Inhalte	541
bb) Streikaufruf	541
cc) Intensität der Kommunikation	542
d) Weitergabe von E-Mail-Adressen der Mitarbeiter	542
aa) Keine Herausgabe bei fortlaufender Mitwirkungshandlung des Arbeitgebers	542
bb) Herausgabe bei punktueller Mitwirkungshandlung des Arbeitgebers	543
cc) Herausgabepflicht im virtuellen Betrieb	546
3. Zugang zu einer betriebsinternen Kommunikationsplattform	546
4. Gewerkschaftsseite im betrieblichen Intranet	547
5. Verlinkung auf die Homepage der Gewerkschaft	548
6. Nutzung der Intranetseite des Betriebsrats durch die Gewerkschaft	549
7. Abwehrrechte	549
a) Abwehrrechte des Arbeitgebers	549
b) Abwehrrechte des einzelnen Arbeitnehmers	550

§ 4 Anwendung von IT und DS-GVO/KI-VO

I. Videoüberwachung (<i>Bongers</i>)	554
1. Arten der Videoüberwachung	554
2. Rechtliche Grundlagen: Datenschutz- und Arbeitsrecht	555
a) Verbot mit Erlaubnisvorbehalt	556
b) Personenbezogene Daten im Rahmen der Videoüberwachung	556
c) Verarbeitung personenbezogener Daten	557
d) Einwilligung des Arbeitnehmers	558
e) Weitere Rechtsgrundlagen – Überblick	561
f) Besondere Kategorien personenbezogener Daten als Gegenstand der Videoüberwachung von Beschäftigten	565
g) Zweckbindung	567
3. Videoüberwachung an nicht öffentlich zugänglichen Arbeitsplätzen	567
a) Rechtliche Grundlage der Videoüberwachung an nicht öffentlich zugänglichen Arbeitsplätzen	567
b) Verhältnismäßigkeit	571
c) Einzelfälle der Videoüberwachung an nicht öffentlich zugänglichen Arbeitsplätzen	572
4. Besonderheiten bei öffentlich zugänglichen Räumen/Arbeitsplätzen	579
a) Definition des öffentlich zugänglichen Arbeitsplatzes	580
b) Offene Videoüberwachung an öffentlich zugänglichen Arbeitsplätzen	581

c) Verdeckte Videoüberwachung an öffentlich zugänglichen Arbeitsplätzen	584
5. Einsatz von Attrappen	584
6. Tonaufzeichnungen	585
7. Pflicht zur Löschung von Videodaten	585
8. Informationsansprüche des Arbeitnehmers nach Art. 13 und 14 DS-GVO	587
a) Art. 13 oder 14 DS-GVO	587
b) Zeitpunkt der Information	587
c) Ausschluss einer verdeckten Videoüberwachung wegen Informationspflichten?	588
9. Auskunftsansprüche des Arbeitnehmers	591
10. Betriebliche Mitbestimmung	592
11. Sachvortrags- und Beweisverwertungsverbote	592
12. Videoüberwachung und KI-VO	595
a) Inkrafttreten der KI-VO	595
b) Videotechnik als KI-System	595
c) Arbeitgeber als Betreiber (Anwender) von KI-Systemen	596
d) Relevante Regelungen der KI-VO	596
e) Videoüberwachung als verbotene Praktik im Sinne der KI-VO	596
aa) Verbot von KI-Systemen zur sozialen Bewertung	597
bb) Verbot von KI-Systemen zur Bewertung des Risikos der Begehung von Straftaten (Art. 5 Abs. 1 lit. d KI-VO)	598
cc) Verbot von KI-Systemen zur Erstellung und Erweiterung von Datenbanken zur Gesichtserkennung (Art. 5 Abs. 1 lit. e KI-VO)	598
dd) Verbot von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz (Art. 5 Abs. 1 lit. f KI-VO)	599
ee) Verbot von KI-Systemen zur biometrischen Kategorisierung (Art. 5 Abs. 1 lit. g KI-VO)	599
ff) Verbot zur biometrischen Echtzeit-Fernidentifikation in öffentlichen zugänglichen Räumen zu Strafverfolgungszwecken (Art. 5 Abs. 1 lit. h, Abs. 2 KI-VO)	599
f) Videoüberwachung als Hochrisikosystem im Sinne der KI-VO	600
g) Transparenzpflichten von Anbietern und Betreibern	602
h) Betriebliche Mitbestimmung beim Einsatz von KI (Videoüberwachung)	602
II. Ortungssysteme (<i>Bongers</i>)	603
1. Einleitung	603
2. Begriffsbestimmung und Beispiele	603
a) Satellitenortung	603
b) Ortung über ein Mobiltelefon und Telekommunikationsnetze	604
c) WLAN	604
d) RFID	604
e) Tachografen	605
3. Personenbezogene Daten beim Einsatz von Ortungssystemen	605
4. Datenschutz- und arbeitsrechtliche Grundlagen	605
5. Ortung des Arbeitnehmers während der Arbeitszeit	611
a) Aufklärung und Vermeidung von Straftaten und Pflichtverletzungen der Arbeitnehmer	611
b) Koordinierung von Einsätzen der Arbeitnehmer	612
c) Warenortung – mittelbare Ortung des Arbeitnehmers	613
d) Ortung zur Sicherheit des Arbeitnehmers	613
e) (Fern-)Ortung im Falle des Verlusts von Betriebsmitteln	614

6. Ortung des Arbeitnehmers in der Freizeit und in den Pausen	615
a) Grundsatz der Unzulässigkeit der Ortung außerhalb der Arbeitszeit	615
b) Erforderlichkeit der Abschaltbarkeit von Ortungssystemen zur Vermeidung der Ortung außerhalb der Arbeitszeit	615
c) Ortung des Arbeitnehmers während Pausen	616
7. Relevanz telekommunikationsrechtlicher oder telemedienrechtlicher Bestimmungen	616
a) Verkehrsdaten	618
b) Standortdaten iSd § 13 TDDDG	618
c) § 25 TDDDG (Schutz der Privatsphäre bei Endeinrichtungen)	622
8. Pflichten zur Löschung von Ortungsdaten, Pflicht zur Information und Auskunft	626
9. Betriebliche Mitbestimmung	626
10. Beweisverwertung	626
11. Ortungssysteme und KI-VO	626
a) Inkrafttreten der KI-VO	626
b) Ortungssysteme als KI-Systeme	626
c) Arbeitgeber als Betreiber (Anwender) von KI-Systemen	627
d) Relevante Regelungen der KI-VO	627
e) Ortung als verbotene Praktik im Sinne der KI-VO	627
aa) Verbot von KI-Systemen zur sozialen Bewertung	628
bb) Verbot von KI-Systemen zur Bewertung des Risikos der Begehung von Straftaten (Art. 5 Abs. 1 lit. d KI-VO)	628
f) Ortungssystem als Hochrisikosystem im Sinne der KI-VO	629
g) Transparenzpflichten von Anbietern und Betreibern	631
h) Betriebliche Mitbestimmung beim Einsatz von KI (Ortungssysteme) ..	632
III. Biometrische Verfahren (<i>Bongers</i>)	632
1. Begriff, Ziel, Funktionsweise und Beispiele	632
2. Personenbezug	635
3. Rechtliche Grundlagen: Datenschutz- und Arbeitsrecht	637
a) Einwilligung	637
b) Art. 6 Abs. 1 UAbs. 1 lit. b und f DS-GVO, § 26 BDSG	638
4. Anwendung der datenschutz- und arbeitsrechtlichen Grundsätze auf einzelne Fallgruppen	641
a) Zutrittskontrolle	641
b) Zeiterfassungssysteme	642
c) Fingerprint statt Passwort	643
d) Bezahlungssystem in Kantine	644
e) Auswahlentscheidungen mit unterstützender Verarbeitung biometrischer Daten	644
5. Löschung und datenschutzrechtliche Auskunfts- und Informationsrechte .	645
6. Mitbestimmung des Betriebsrats	645
7. Biometrische Verfahren und KI-VO	645
a) Inkrafttreten der KI-VO	645
b) Biometrische Daten im Sinne der KI-VO	645
c) Überblick über Regelungen zu biometrischen Verfahren in der KI-VO mit praktischer Relevanz für ein Arbeitsverhältnis	646
aa) KI-Systeme iSd KI-VO	646
bb) Arbeitgeber als Betreiber (Anwender) von KI-Systemen	646
cc) Überblick über die biometrischen Verfahren, die in der KI-VO geregelt sind	647

dd) Bei der Durchführung des Arbeitsverhältnisses denkbare Anwendungsfälle	648
ee) Biometrische Verfahren als verbotene Praktiken	650
ff) Biometrische Verfahren als Hochrisikosysteme im Arbeitsverhältnis	653
gg) Transparenzpflichten von Anbietern und Betreibern	659
hh) Betriebliche Mitbestimmung beim Einsatz von KI (Biometrische Verfahren)	659
IV. Einsatz von Kommunikations- und Kollaborationstools (<i>Törkel</i>)	659
1. Cloud-Tools	659
2. Datenschutzrechtliche Anforderungen	660
a) Wirksamer Auftragsverarbeitungsvertrag	660
b) Auftragsverarbeitung und KI	663
c) Verarbeitungsverzeichnis	663
d) Datenschutzfolgenabschätzung	664
e) Einhaltung der datenschutzrechtlichen Garantien bei Drittlandbezug ..	665
f) Umsetzung technischer und organisatorischer Maßnahmen	666
3. Probleme in der Praxis	667
a) Einsatz von Tracking-Tools	668
b) Aufzeichnung von Online-Meetings	669
c) Pflicht zur Kameraaktivierung im Online-Meeting	669
d) Übergang von Beschäftigtendaten beim Betriebsübergang gemäß § 613a BGB – „Asset Deal“	671
4. Empfehlungen zum rechtskonformen Einsatz	672
a) Empfehlungen für Arbeitgeber	672
aa) Auswahl eines datenschutzrechtlich geeigneten Cloud-Anbieters ..	672
bb) Abschluss und Prüfung des Auftragsvertrages	673
cc) Datenschutzhinweise	674
dd) Datenlöschung	674
ee) Datenschutzfolgenabschätzung	674
b) Empfehlungen für Arbeitnehmer	675
5. Betriebliche Mitbestimmung	676

§ 5 IT-Arbeitsstrafrecht (*Petri*)

I. Einleitung	680
II. Videoüberwachung am Arbeitsplatz	683
1. Strafbarkeit nach § 201a StGB	684
a) Kriminalpolitische Bedeutung	684
b) Tatgegenstand	684
c) Räumlicher Schutzbereich	685
d) Tathandlungen	685
e) Subjektiver Tatbestand	686
f) Rechtswidrigkeit	686
g) Rechtsfolgen und Strafantrag nach § 205 StGB	687
2. Strafbarkeit nach § 42 BDSG	688
a) Kriminalpolitische Bedeutung	688
b) Schutzbereich	688
c) Tatbestandliche Qualifizierung und subjektiver Tatbestand	689
d) Rechtswidrigkeit	691
e) Rechtsfolgen und Strafantrag	691
3. Ordnungswidrigkeit nach Art. 83 Abs. 5 lit. a DS-GVO	693
a) Kriminalpolitische Bedeutung	693

b) Tatbestand des Art. 83 Abs. 5 lit. a iVm Art. 6 Abs. 1 lit. f DS-GVO	694
c) Subjektiver Tatbestand	695
d) Rechtsfolgen	696
III. Überwachung der Kommunikation am Arbeitsplatz	699
1. Verletzung der Vertraulichkeit des Wortes § 201 StGB	700
a) Schutzbereich	700
b) Tathandlungen	701
c) Rechtfertigung	702
2. Verletzung des Briefgeheimnisses § 202 StGB	702
a) Kriminalpolitische Bedeutung	703
b) Rechtsgut	703
c) Subjektiver Tatbestand und Rechtswidrigkeit	703
d) Rechtsfolge und Strafantrag	704
3. Abfangen von Daten § 202b StGB	704
a) Rechtsgut	704
b) Tatobjekt	704
c) Subjektiver Tatbestand und Rechtswidrigkeit	705
d) Rechtsfolgen und Strafantrag	705
4. Abhören oder Mitteilen von Nachrichten nach § 27 TDDDG	706
a) Rechtsgut	706
b) Tatobjekt	706
c) Subjektiver Tatbestand und Rechtswidrigkeit	707
5. Speicherung und Auswertung entgegen § 42 BDSG, Art. 83 Abs. 4-6 DS-GVO	707
IV. E-Mail und Internetüberwachung	710
1. Strafbarkeit nach § 206 StGB	710
a) Täterkreis	711
b) Tathandlung nach Abs. 1	711
c) Tathandlung nach Abs. 2	713
d) Subjektiver Tatbestand und Rechtswidrigkeit	713
e) Rechtsfolgen	714
f) Verfahrensbesonderheiten	714
2. Strafbarkeit nach § 202a StGB	715
a) Kriminalpolitische Bedeutung	715
b) Tatgegenstand Daten	715
c) Nicht für den Täter bestimmt	716
d) Zugangsverschaffung	716
e) Subjektiver Tatbestand und Rechtswidrigkeit	716
f) Rechtsfolgen und Strafantrag	717
3. Strafbarkeit nach § 42 BDSG	717
4. Ordnungswidrigkeit nach Art. 83 DS-GVO	718
V. Mitarbeiterüberwachung und Internal Investigations	718
1. Arbeitsstrafrechtliche IT-Compliance	719
2. KI und Internal Investigation	719
a) Anwendungsbereiche	720
b) KI-Verordnung	721
c) Risiken	722
d) Zusammenfassung	722
3. Gang interner Ermittlungen	723
4. Verwertungsverbote	727
5. Zusammenarbeit mit staatlichen Organen	729

6. Behandlung der Unternehmenskommunikation	730
7. Zusammenfassung	731
VI. Strafbarkeit des Arbeitnehmers bei IT-Pflichtverletzungen	732
1. § 23 iVm § 4 GeschGehG: Verletzung von Geschäftsgeheimnissen	732
a) Einleitung/Überblick	732
b) Tatbestand	733
aa) Tathandlungen	733
bb) Tatobjekt	733
cc) Mögliche Täter	733
dd) Besondere Handlungsmotivation	734
ee) Vorsatz	734
c) Rechtswidrigkeit	734
d) Schuld	735
e) Antragsdelikt	735
f) Konkurrenzen	735
aa) Zivilrechtliche Konsequenzen	735
bb) Arbeitsrechtliche Folgen	735
cc) Weitere strafrechtliche Vorschriften	736
2. Zusammenfassung	737
 § 6 Sozialversicherungs- und steuerrechtliche Behandlung der IT-Nutzung	
I. Sozialversicherungsrechtliche Behandlung der IT-Nutzung (<i>Oberthür/Schleper</i>)	739
1. Nutzungsvorteile als Arbeitsentgelt iSv § 14 SGB IV	739
2. Ausnahmen von dem gesetzlichen Arbeitsentgeltbegriff	739
a) Lohnsteuerfreiheit des Nutzungsrechts	740
b) Erfordernis der „zusätzlichen Leistung“	740
3. Beitragsrechtliche Bewertung der IT-Nutzung	741
II. Steuerrecht (<i>Petri</i>)	742
1. Einleitung	742
2. Steuerfreie Überlassung	742
3. Umsatzsteuer	744
4. Schenkung	746
Stichwortverzeichnis	747