

Josephine Scharnberg

Illegale Internal Investigations

**Strafrechtliche Grenzen
unternehmensinterner
Ermittlungen**

Inhaltsverzeichnis

Abkürzungsverzeichnis	XXVII
-----------------------------	-------

Kapitel 1 – Rechtliche Einordnung der unternehmensinternen

Ermittlungen	1
A. Einleitung und Hinführung zum Thema	1
B. Compliance	4
I. Begriffserklärung, Ursprung und Entwicklung.....	4
II. Ursachen für den Wandel.....	8
1. Steigendes Strafbarkeitsrisiko	8
2. Internationale Gesetzgebung	10
III. Folgen von Non-Compliance.....	11
1. Überblick.....	11
2. § 30 OWiG – Verbandsgeldbuße.....	11
3. Ausschluss von öffentlichen Aufträgen	13
4. Korruptionsregister	13
IV. Vorteile.....	15
V. Rechtspflicht „Compliance“	17
1. Spezialgesetzliche Regelungen.....	17
2. Allgemeine Rechtspflicht?	18
VI. Compliancemaßnahmen	21
1. Compliance-Organisation.....	23
2. Verhaltenskodex	24
3. Compliance-Programm.....	25
4. Information und Beratung	26
C. Internal Investigations	27
I. Begriff.....	27
II. Ursprung und Entwicklung	28
III. Zielsetzung	30
IV. Auslöser für Internal Investigations.....	32
1. Hinweisgebersystem: Whistleblowing-Hotline.....	32
2. Hinweisgebersystem: Ombudsmann	34
3. Kronzeugenregelung und Co.	35

V.	Durchführung: intern vs. extern	36
VI.	Vor- und Nachteile einer internen Untersuchung	40
	1. Vorteile.....	40
	2. Nachteile.....	44
VII.	Rechtliche Gebotenheit	46
	1. Spezialgesetzliche Regelungen.....	46
	2. Allgemeine Rechtspflicht?	47
VIII.	Ablauf.....	49
	1. Untersuchungsmaßnahmen.....	49
	2. Verdeckte Untersuchung	50
	3. Beteiligung des Betriebsrates	51
	4. Einschaltung der Strafverfolgungsbehörden	52
	5. Verhältnis zu staatsanwaltschaftlichen Ermittlungen.....	53
IX.	Anwendbares Recht.....	55
D.	Zulässigkeit privater Ermittlungen	56
	I. Allgemeines.....	56
	II. Grundsätzliche Zulässigkeit privater Ermittlungen.....	57
	1. Keine Überschneidung mit staatlichen Ermittlungen.....	57
	2. Untersuchungen parallel zu staatlichen Ermittlungen	57
	3. Ergebnis	59
	III. Besondere Konstellation der internen Ermittlungen.....	59
Kapitel 2 – Beschäftigtendatenschutzrecht		63
A.	Aktuelle Gesetzeslage und geplante Gesetzesänderung	63
B.	Bundesdatenschutzgesetz – BDSG.....	65
	I. Anwendungsbereich	65
	1. Sachlicher Anwendungsbereich	65
	2. Persönlicher Anwendungsbereich.....	66
	3. Landesdatenschutzgesetze.....	67
	II. Grundsätze des BDSG	67
	1. § 3a BDSG – Grundsatz der Datenvermeidung und -sparsamkeit	67
	2. § 4 Abs. 2 S. 1 BDSG – Grundsatz der Direkterhebung.....	68
	3. § 4 Abs. 1 BDSG – Verbot mit Erlaubnisvorbehalt.....	70
	III. Erlaubnisnormen.....	70
	1. Einwilligung	70
	2. Betriebsvereinbarung.....	71
	3. § 32 BDSG – Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses	73

a.	Voraussetzungen des § 32 Abs. 1 S. 2 BDSG.....	73
aa.	Straftat.....	74
bb.	Im Beschäftigungsverhältnis.....	74
cc.	Tatsächliche Anhaltspunkte.....	75
dd.	Dokumentation.....	77
ee.	Maßnahme beim Betroffenen.....	77
ff.	Zur Aufdeckung der Tat erforderlich.....	78
gg.	Verhältnismäßigkeit der Kontrolle.....	78
(I)	Legitimer Zweck.....	79
(II)	Geeignetheit.....	79
(III)	Erforderlichkeit.....	79
(IV)	Angemessenheit.....	79
(1)	Interessen des Arbeitnehmers.....	79
(2)	Interessen des Arbeitgebers.....	81
(3)	Interessenabwägung.....	81
(4)	Einschränkung?.....	83
b.	Voraussetzungen des § 32 Abs. 1 S. 1 BDSG.....	84
4.	§ 28 BDSG – Datenerhebung und -speicherung für eigene Geschäftszwecke.....	84
5.	Zusammenfassung.....	86
IV.	Auftragsdatenverarbeitung – § 11 BDSG.....	86
1.	Allgemeines.....	86
2.	Abgrenzung zur Funktionsübertragung.....	87
3.	Einordnung der externen Ermittler.....	88
C.	Telekommunikationsgesetz – TKG.....	90
I.	Anwendungsbereich.....	90
1.	Anwendungsbereich des TKG.....	90
2.	Anwendungsbereich des Fernmeldegeheimnisses.....	91
II.	Arbeitgeber als Dienstanbieter: Abgrenzung BDSG – TKG.....	92
1.	Dienstliche Nutzung.....	92
2.	Verbotene private Nutzung.....	93
a.	Grundsatz.....	93
b.	Duldung trotz Verbotes.....	94
c.	Betriebliche Übung.....	95
aa.	Anspruch aus betrieblicher Übung.....	96
bb.	Argumente gegen die Entstehung einer betrieblichen Übung.....	96
cc.	Ergebnis.....	99
d.	Ergebnis für den Fall der verbotenen privaten Nutzung.....	99

3.	Gestattete private Nutzung.....	100
a.	Rechtsprechung	100
b.	Die bisher h.M.: Argumente für die Anwendbarkeit des TKG	101
aa.	Wortlaut	102
bb.	Arbeitnehmer als Dritter	103
cc.	Gesetzgebungsgeschichte	104
dd.	Zweck des TKG.....	105
ee.	Beschluss des OLG Karlsruhe vom 10.1.2005	105
c.	Argumente gegen die Anwendbarkeit des TKG.....	106
aa.	Wortlaut – üblicherweise gegen Entgelt erbracht	106
bb.	Rechtsfolgen der Anwendbarkeit	108
	(I) Strafbarkeitsrisiko nach § 206 StGB	108
	(II) Einsichtsrecht des Arbeitgebers	108
	(III) Interessenabwägung.....	109
	(IV) Fehlende Systematik der Gesetze – Dokumentationspflicht.....	109
cc.	Teleologie – Förderung des Wettbewerbs	110
dd.	Weitere Argumente	112
d.	Stellungnahme	112
e.	Ergebnis für den Fall der gestatteten privaten Nutzung.....	113
4.	Keine Regelung hinsichtlich der privaten Nutzung: Duldung und betriebliche Übung.....	114
a.	Sozialadäquanz	114
b.	Duldung	114
c.	Betriebliche Übung	115
5.	Zusammenfassung und Ergebnis	116
D.	Telemediengesetz – TMG.....	118
I.	Anwendungsbereich des TMG allgemein	118
	1. Sachlicher Anwendungsbereich	118
	2. Persönlicher Anwendungsbereich.....	119
II.	Anwendbarkeit der Datenschutzvorschriften des TMG	119
III.	Ergebnis	120
E.	Zusammenfassung.....	120
Kapitel 3 – Strafbarkeitsrisiken einzelner Ermittlungsmaßnahmen		123
A.	E-Mail-Screening.....	123
I.	Allgemeines.....	123
II.	Ablauf.....	125

	1. Durchführung.....	125
	2. Beteiligung des Betriebsrates	125
III.	Grundsätzliches zur Rechtmäßigkeit des E-Mail-Screenings	126
IV.	Kontrolle von E-Mail-Logfiles	127
	1. Begriff.....	127
	2. Rechtmäßigkeit nach § 32 Abs. 1 S. 2 BDSG	127
	a. Dienstliche E-Mail.....	128
	b. Private E-Mail	129
	3. Rechtmäßigkeit nach TKG.....	129
	a. Eingriff in das Fernmeldegeheimnis.....	129
	b. Rechtfertigungsgründe des TKG.....	130
	c. Zwischenergebnis	131
	d. Ausnahme: Straftatverdacht?	132
	4. Ergebnis	132
V.	Inhaltskontrolle – Rechtmäßigkeit nach BDSG	133
	1. Erforderlichkeit einer Rechtfertigung.....	133
	2. Rechtfertigung nach § 32 Abs. 1 S. 2 BDSG.....	134
	a. Voraussetzungen des § 32 Abs. 1 S. 2 BDSG.....	134
	b. Verhältnismäßigkeit	135
	aa. Geeignetheit	135
	bb. Erforderlichkeit.....	135
	cc. Angemessenheit.....	136
	(I) Interessen des Arbeitnehmers	136
	(II) Interessen des Arbeitgebers	137
	(III) Interessenabwägung.....	137
	(1) Dienstliche E-Mails.....	138
	(a) Vergleichbarkeit der E-Mail mit herkömmlichen Kommunikations- mitteln.....	138
	(aa) Vergleichbarkeit der E-Mail mit dem Telefonat.....	138
	(bb) Vergleichbarkeit der E-Mail mit dem Postverkehr	139
	(cc) Stellungnahme	141
	(b) Kontrollrechte des Arbeitgebers.....	141
	(2) Private E-Mails	143
	(a) Verbotene private Nutzung.....	144
	(aa) Charakter der E-Mail nicht erkennbar.....	145

	(bb) Charakter der E-Mail erkennbar.....	145
	(cc) Sonderfall: Straftatverdacht.....	146
	(dd) Ergebnis für den Fall der verbotenen privaten Nutzung.....	147
	(b) Erlaubte private Nutzung.....	148
	(aa) Grundsatz.....	148
	(bb) Mischnutzung.....	148
	(cc) Sonderfall: Straftatverdacht.....	149
	(dd) Ergebnis für den Fall der gestatteten privaten Nutzung.....	150
	(3) Ausnahme: Besondere Berufsgruppen.....	150
	3. Zusammenfassung.....	151
VI.	Inhaltskontrolle – Rechtmäßigkeit nach TKG.....	152
	1. Dienstliche E-Mails.....	152
	2. Private E-Mails.....	153
	a. Fernmeldegeheimnis.....	153
	aa. Schutzbereich.....	153
	(I) Persönlicher Schutzbereich.....	153
	(II) Sachlicher Schutzbereich.....	153
	bb. Reichweite des Fernmeldegeheimnisses.....	153
	(I) Während des Übertragungsvorganges.....	154
	(II) Speicherung auf lokalem Endgerät.....	154
	(III) Speicherung auf dem Server.....	154
	(1) BVerfGE 124, 43.....	155
	(2) Übertragbarkeit.....	156
	(a) Kein Schutz durch das Fernmeldegeheimnis.....	156
	(b) Schutz durch das Fernmeldegeheimnis.....	157
	(c) Stellungnahme.....	159
	(d) Fallgruppen.....	159
	(aa) POP3-Verfahren.....	159
	(bb) IMAP-Verfahren.....	160
	(cc) Sicherungskopien.....	161
	cc. Zwischenergebnis.....	161
	b. Eingriff.....	161
	c. Rechtfertigung.....	162
	aa. Besondere Rechtfertigungsgründe des TKG.....	162
	(I) § 88 Abs. 3 S. 3 TKG i.V.m. §§ 91 ff. TKG.....	162

(II) § 88 Abs. 3 S. 3 TKG i.V.m. § 32 Abs. 1 S. 2 BDSG.....	162
(III) § 88 Abs. 3 S. 4 TKG	163
(IV) Zwischenergebnis.....	163
bb. Allgemeine strafrechtliche Rechtfertigungsgründe.....	163
(I) Anwendbarkeit	163
(II) Hilfsweise: Bejahung der Anwendbarkeit.....	165
(III) Einwilligung.....	166
(1) Doppeltes Zustimmungserfordernis	166
(2) Kein doppeltes Zustimmungserfordernis	167
(3) Stellungnahme.....	168
(IV) Mutmaßliche Einwilligung	168
cc. Betriebsvereinbarung.....	168
dd. Ausnahme: Straftatverdacht?	169
d. Ergebnis	170
3. Mischnutzung	170
4. Ergebnis	172
VII. Strafbarkeitsrisiken.....	173
1. Strafbarkeitsrisiken nach StGB.....	173
a. § 206 StGB – Verletzung des Post- oder Fernmeldegeheimnisses.....	173
aa. Rechtsgut	174
bb. Tatbestand	174
(I) Tauglicher Täter.....	174
(II) Unternehmen, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt	175
(III) Tatsachen, die dem Post- oder Fernmeldegeheimnis unterliegen.....	176
(IV) Tathandlung.....	177
(1) Abs. 1: Weitergabe von geschützten Informationen.....	177
(a) Mitteilung an eine andere Person	177
(b) Dem Täter bekannt geworden.....	178
(c) Zwischenergebnis.....	179
(2) Abs. 2 Nr. 1: Ausforschung von Informationen.....	179
(3) Abs. 2 Nr. 2: Unterdrücken von Informationen.....	180
(4) Zwischenergebnis.....	180

(V)	Unbefugt.....	181
(1)	Hinweis auf Rechtswidrigkeit.....	181
(2)	Doppelfunktion.....	181
(3)	Einverständnis.....	182
(VI)	Subjektiver Tatbestand.....	182
cc.	Rechtswidrigkeit.....	183
(I)	Besondere Rechtfertigungsgründe des TKG.....	183
(II)	Allgemeine strafrechtliche Rechtfertigungsgründe.....	184
dd.	Schuld.....	184
ee.	Ergebnis.....	185
b.	§ 202 StGB – Verletzung des Briefgeheimnisses.....	187
c.	§ 202a StGB – Ausspähen von Daten.....	187
aa.	Geschütztes Rechtsgut.....	187
bb.	Objektiver Tatbestand.....	188
(I)	Daten.....	188
(II)	Nicht für den Täter bestimmt.....	189
(1)	Dienstliche E-Mails.....	189
(2)	Private E-Mails.....	191
(a)	Gestattete private Nutzung.....	191
(b)	Verbotene private Nutzung.....	191
(c)	Ergebnis.....	192
(III)	Zugangverschaffung.....	192
(IV)	Besondere Zugangssicherung.....	193
(1)	Grundsatz.....	193
(2)	Verschlüsselung.....	195
(3)	Zugangssicherung privater E-Mails.....	196
(a)	Einzelne Dateien.....	196
(b)	Personalisiertes Laufwerk.....	196
(c)	Ergebnis – besondere Zugangssicherung.....	197
cc.	Subjektiver Tatbestand.....	198
dd.	Rechtswidrigkeit.....	198
(I)	Rechtfertigungsgründe: Allgemein.....	199
(II)	Rechtfertigung nach § 32 Abs. 1 S. 2 BDSG.....	199
ee.	Ergebnis.....	200
d.	§ 202b StGB – Abfangen von Daten.....	201
aa.	Objektiver Tatbestand.....	201
(I)	Daten.....	201
(II)	Nicht für den Täter bestimmt.....	201

(III) Nichtöffentliche Datenübermittlung (Alt. 1).....	201
(1) Datenübermittlung	201
(2) Nichtöffentlichkeit	202
(IV) Verschaffen.....	203
(V) Technische Mittel	203
bb. Subjektiver Tatbestand.....	203
cc. Rechtswidrigkeit.....	204
dd. Ergebnis	204
e. § 202c StGB – Vorbereiten des Ausspähens und Abfangens von Daten.....	204
f. § 201 StGB – Verletzung der Vertraulichkeit des Wortes	205
g. § 303a StGB – Datenveränderung.....	205
2. Strafbarkeitsrisiken nach BDSG	206
a. § 43 BDSG - Bußgeldvorschriften	206
aa. Tatbestand	206
(I) Täter.....	206
(II) Tatobjekt	207
(III) Tathandlung.....	207
(IV) Subjektiver Tatbestand.....	208
bb. Rechtswidrigkeit.....	208
cc. Ergebnis	208
b. § 44 BDSG – Strafvorschriften	209
aa. Alt. 1: gegen Entgelt	209
bb. Alt. 2: Bereicherungsabsicht	210
cc. Alt. 3: Schädigungsabsicht	210
dd. Ergebnis	210
3. Strafbarkeitsrisiken nach TKG	211
4. Ergebnis	212
a. Kontrolle dienstlicher E-Mails.....	212
b. Kontrolle privater E-Mails.....	212
c. Strafbarkeit des privaten Ermittlers	213
VIII. Zusammenfassung.....	213
B. Auswertung von Dokumenten, Dateien und Personalakten	215
I. Verwertung von Unterlagen in Papierform	215
1. Zulässigkeit nach Datenschutzrecht	215
a. Dienstliche Dokumente.....	216
b. Private Dokumente	217

2.	Strafbarkeitsrisiken.....	218
a.	§ 202 StGB – Verletzung des Briefgeheimnisses	218
aa.	Objektiver Tatbestand.....	218
	(I) Tatobjekt.....	218
	(1) Verschlossenes Schriftstück – § 202 Abs. 1 Nr. 1 StGB	218
	(2) Verschlossenes Behältnis – § 202 Abs. 2 StGB.....	219
	(II) Nicht zu seiner Kenntnis bestimmt	219
	(1) Dienstliche Dokumente.....	220
	(2) Private Dokumente	220
	(III) Tathandlungen.....	220
	(1) Öffnen – § 202 Abs. 1 Nr. 1 StGB.....	220
	(2) Kenntnisverschaffen vom Inhalt nach Öffnen – § 202 Abs. 2 StGB.....	221
	bb. Subjektiver Tatbestand.....	221
	cc. Rechtswidrigkeit	221
	dd. Ergebnis	222
b)	§§ 43, 44 BDSG – Bußgeld- und Strafvorschriften.....	222
II.	Einsichtnahme in Dateien – Kontrolle von Akten und Unterlagen in elektronischer Form	223
1.	Zulässigkeit nach Datenschutzrecht	223
a)	Dienstliche Dateien.....	223
b)	Private Dateien.....	224
c)	Gemischte Dateien	225
d)	Ergebnis	226
2.	Strafbarkeitsrisiken.....	226
a)	§ 202a StGB – Ausspähen von Daten	226
aa)	Objektiver Tatbestand.....	226
	(I) Daten.....	226
	(II) Nicht für den Täter bestimmt.....	226
	(1) Dienstliche Dateien.....	227
	(2) Private Dateien	227
	(III) Zugangverschaffung.....	228
	(IV) Besondere Zugangssicherung.....	228
bb)	Subjektiver Tatbestand.....	229
cc)	Rechtswidrigkeit	229
dd)	Ergebnis	229
b)	§§ 43, 44 BDSG – Bußgeld- und Strafvorschriften.....	230

III.	Auswertung von Personalakten	230
1.	Zulässigkeit nach Datenschutzrecht	230
2.	Strafbarkeitsrisiken.....	231
IV.	Zusammenfassung.....	231
C.	Interviews	232
I.	Einleitung	232
II.	Beteiligung des Betriebsrates	234
III.	Anwendbares Recht.....	236
IV.	Amnestieprogramme.....	240
1.	Allgemeines.....	240
2.	Inhalt und typische Bestandteile einer Amnestie	242
a.	Absehen von arbeitsrechtlichen Sanktionen.....	243
b.	Schutz vor Schadenersatzansprüchen.....	244
c.	Schutz vor Strafverfolgung.....	244
d.	Zusicherung von Vertraulichkeit.....	245
e.	Übernahme von Verteidigerkosten und Geldstrafen	246
3.	Vergaberechtliche Grenzen der Amnestie	247
4.	Beseitigung von Amnestiezusagen.....	248
5.	Beteiligung des Betriebsrates	249
6.	Strafbarkeitsrisiken hinsichtlich der Gewährung von Amnestien.....	250
a.	§ 266 StGB – Untreue	250
aa.	Verpflichtungs- oder Verfügungsbefugnis.....	250
bb.	Vermögensbetreuungspflicht.....	251
cc.	Missbrauch der Befugnis.....	251
(I)	Unternehmerische Entscheidung.....	252
(II)	Auf Grundlage angemessener Informationen.....	253
(III)	Handeln zum Wohle der Gesellschaft	254
(IV)	Gutgläubigkeit	255
(V)	Zulässigkeit einzelner Amnestiezusagen	255
(1)	Verzicht auf Schadenersatzansprüche.....	255
(2)	Übernahme der Geldstrafe, -buße oder -auflage	257
(3)	Übernahme der Verteidigerkosten	258
dd.	Ergebnis	260
b.	§ 258 StGB – Strafvereitelung.....	260
c.	§ 138 StGB – Nichtanzeige geplanter Straftaten.....	261
V.	Teilnahmepflicht der Mitarbeiter	262
VI.	Aussagepflicht des verdächtigen Arbeitnehmers	262
1.	Vertraglich geschuldete Tätigkeit.....	264

2.	§§ 666, 675 Abs. 1 BGB – persönlicher Arbeitsbereich.....	264
a.	Anspruchsgrundlage.....	264
b.	Reichweite der Auskunftspflicht.....	266
c.	Pflicht zur selbstbelastenden Aussage?.....	267
aa.	Architekten-Fall.....	268
bb.	Übertragbarkeit auf das Arbeitsverhältnis.....	268
	(I) Übertragbarkeit.....	268
	(II) Fehlende Übertragbarkeit.....	270
	(III) Stellungnahme.....	271
3.	§§ 611, 241 Abs. 2 BGB – allgemeiner Auskunftsanspruch/ arbeitsvertragliche Nebenpflicht	273
a.	Allgemeines.....	273
b.	Voraussetzungen.....	274
aa.	Berechtigtes Interesse des Arbeitgebers	274
bb.	Zumutbarkeit / Interessenabwägung.....	275
	(I) Keine Pflicht zur Selbstbelastung.....	276
	(II) Pflicht zur Selbstbelastung.....	276
	(III) Vermittelnde Ansichten	277
	(IV) Stellungnahme.....	278
cc.	Beweislastumkehr.....	278
c.	Ergebnis.....	280
4.	§ 242 BGB – allgemeine Treuepflicht	280
5.	Zusammenfassung.....	281
VII.	Anwendbarkeit des nemo tenetur-Grundsatzes: Selbstbeziehungspflicht oder Aussageverweigerungsrecht?.....	282
1.	Allgemeines.....	282
2.	§ 136 StPO (analog)	284
3.	Geltung des nemo tenetur-Grundsatzes?.....	284
a.	Anwendbarkeit des nemo tenetur-Grundsatzes.....	285
b.	Keine Anwendbarkeit des nemo tenetur-Grundsatzes	286
aa.	Gemeinschuldner-Beschluss des BVerfG.....	287
bb.	Übertragbarkeit des Gemeinschuldner-Beschlusses ...	288
	(I) Übertragbarkeit.....	288
	(II) Fehlende Übertragbarkeit.....	289
	(III) Stellungnahme.....	290
cc.	Beweisverwertungsverbot?.....	290
	(I) Annahme eines Beweisverwertungsverbotes	290
	(1) § 97 Abs. 1 S. 3 InsO analog.....	290
	(2) Beweisverwertungsverbot im Hinblick auf nemo tenetur.....	291

	(3) Ausnahme: Freiwillige Aussage.....	293
	(II) Ablehnung eines Beweisverwertungsverbotes	293
	c. Stellungnahme	294
	4. Zusammenfassung.....	295
VIII.	Fair trial-Grundsatz	296
	1. Allgemeines.....	296
	2. Fair trial im Rahmen des Interviews	297
	3. Stellungnahme	298
IX.	Aussagepflicht hinsichtlich Fehlverhalten Dritter.....	298
X.	Rechte der Mitarbeiter im Rahmen einer Befragung	300
	1. Hinzuziehung eines Mitgliedes des Betriebsrates.....	300
	a. § 82 Abs. 2 S. 2 BetrVG.....	301
	b. § 84 Abs. 1 S. 2 BetrVG.....	302
	c. Ergebnis	302
	2. Hinzuziehung eines Rechtsanwaltes	303
	a. Anspruch auf Hinzuziehung.....	303
	b. Kein Anspruch auf Hinzuziehung	304
	c. Vermittelnde Ansicht.....	304
	d. Stellungnahme	305
	3. Einsichtnahmerecht in das Protokoll.....	306
	a. Einsichtnahmerecht	307
	b. Kein Einsichtnahmerecht.....	308
	c. Vermittelnde Ansicht.....	309
	d. Stellungnahme	310
	4. Zusammenfassung.....	310
XI.	Aussagepflicht gegenüber externen Ermittlern	310
XII.	Belehrungspflicht?.....	312
XIII.	Strafbarkeitsrisiken.....	314
	1. § 240 StGB – Nötigung.....	314
	a. Nötigungshandlung.....	314
	b. Nötigungserfolg.....	315
	c. Vorsatz	315
	d. Rechtswidrigkeit – § 240 Abs. 2 StGB	315
	e. Ergebnis	316
	2. § 239 StGB – Freiheitsberaubung.....	316
	3. § 132 StGB – Amtsanmaßung	317
	4. § 201 StGB – Verletzung der Vertraulichkeit des Wortes	317
	5. § 185 StGB – Beleidigung.....	318
	6. §§ 43, 44 BDSG – Bußgeld- und Strafvorschriften	318
XIV.	Zusammenfassung.....	318

D.	Kontrolle des Postverkehrs.....	321
I.	Einleitung	321
II.	Strafbarkeitsrisiken.....	321
1.	§ 206 StGB – Verletzung des Post- oder Fernmeldegeheimnisses.....	322
2.	§ 202 StGB – Verletzung des Briefgeheimnisses	322
a.	Objektiver Tatbestand.....	322
aa.	Tatobjekt	322
(I)	Verschlossener Brief – § 202 Abs. 1 Nr. 1, 2 StGB.....	322
(II)	Verschlossenes Behältnis – § 202 Abs. 2 StGB	322
bb.	Nicht zu seiner Kenntnis bestimmt	323
(I)	Dienstpost	323
(II)	Privatpost	324
cc.	Tathandlungen	324
b.	Subjektiver Tatbestand.....	325
c.	Rechtswidrigkeit	325
d.	Ergebnis	325
3.	§§ 43, 44 BDSG – Bußgeld- und Strafvorschriften	325
III.	Zusammenfassung.....	326
E.	Kontrolle und Auswertung von Telefonaten und Verbindungsdaten – Telefonüberwachung	326
I.	Verbindungsdaten	327
1.	Dienstgespräche oder dienstlich veranlasste Gespräche.....	327
2.	Privatgespräche.....	328
a.	Zulässigkeit nach BDSG	328
b.	Zulässigkeit nach TKG.....	329
II.	Inhaltskontrolle.....	329
1.	Dienstgespräche.....	330
2.	Privatgespräche.....	331
a.	Zulässigkeit nach BDSG	331
b.	Zulässigkeit nach TKG.....	332
III.	Ausnahme: Besondere Berufsgruppen	332
IV.	Strafbarkeitsrisiken.....	333
1.	§ 201 StGB – Verletzung der Vertraulichkeit des Wortes	333
a.	Objektiver Tatbestand.....	333
aa.	Nichtöffentlich gesprochenes Wort.....	333
bb.	Tathandlung	334
(I)	Aufnahme auf einen Tonträger – § 201 Abs. 1 Nr. 1 StGB	334

(II) Gebrauchen oder Zugänglichmachen einer Aufnahme – § 201 Abs. 1 Nr. 2 StGB	335
(III) Abhören mit einem Abhörgerät – § 201 Abs. 2 S. 1 Nr. 1 StGB	335
(IV) Öffentliches Mitteilen – § 201 Abs. 2 S. 1 Nr. 2 StGB	336
(V) Unbefugt.....	337
b. Subjektiver Tatbestand.....	337
c. Rechtswidrigkeit.....	337
aa. Spezielle Befugnisnormen.....	337
(I) BDSG	337
(II) TKG.....	338
bb. Allgemeine Rechtfertigungsgründe.....	338
(I) Notwehr.....	338
(II) Rechtfertigender Notstand.....	339
d. Ergebnis	339
2. § 202b StGB – Abfangen von Daten	339
3. § 206 StGB – Verletzung des Post- oder Fernmeldegeheimnisses.....	340
4. §§ 43, 44 BDSG – Bußgeld- und Strafvorschriften	340
5. Strafbarkeitsrisiken nach dem TKG.....	340
V. Zusammenfassung.....	341
F. Inaugenscheinnahme des Arbeitsplatzes	342
G. Elektronischer Datenabgleich.....	343
I. Begriff.....	343
II. Datenschutzrechtliche Zulässigkeit.....	344
1. Voraussetzungen des § 32 Abs. 1 S. 2 BDSG.....	344
2. Verhältnismäßigkeit.....	345
a. Geeignetheit	345
b. Erforderlichkeit.....	345
aa. Pseudonymisierung.....	346
bb. Vorherige Unterrichtung.....	346
c. Angemessenheit.....	347
3. Ergebnis	348
III. Strafbarkeitsrisiken.....	348
IV. Zusammenfassung.....	349
H. Sonstige Strafbarkeitsrisiken.....	349
I. § 17 UWG – Verrat von Geschäfts- und Betriebsgeheimnissen	349
II. § 203 StGB – Verletzung von Privatgeheimnissen.....	350

III.	§§ 119 ff. BetrVG – Straf- und Bußgeldvorschriften	350
1.	§ 119 BetrVG.....	350
2.	§§ 120 f. BetrVG	351
I.	Zusammenfassung.....	351
I.	E-Mail-Screening.....	352
II.	Verwertung von Dokumenten, Dateien und Personalakten	354
III.	Interviews	354
IV.	Kontrolle des Postverkehrs.....	355
V.	Telefonüberwachung.....	355
VI.	Inaugenscheinnahme.....	356
VII.	Datenabgleich	356
VIII.	Sonstiges	356

Kapitel 4 – Prozessuale Folgeprobleme: Verwertbarkeit

	privater Beweismittel	359
A.	Einleitung	359
B.	Beweisverwertungsverbot	359
I.	Strafprozess	360
1.	Zwei extreme Ansichten	360
2.	Vermittelnde Ansicht	360
3.	Abwägungslehre	362
4.	Zusammenfassung.....	363
II.	Zivilprozess	364
1.	Grundsätze der Verwertbarkeit	364
a.	Annahme eines Beweisverwertungsverbotes	365
b.	Ablehnung eines Beweisverwertungsverbotes.....	366
c.	Vermittelnde Ansicht – Abwägung im Einzelfall.....	366
d.	Stellungnahme	368
2.	Verwertungsverbot des Sachvortrags.....	369
III.	Arbeitsgerichtsverfahren	371
1.	Rechtswidrige Beweisgewinnung.....	371
a.	Zwei extreme Ansichten	372
b.	Vermittelnde Ansicht	372
c.	Stellungnahme	373
2.	Nichteinbeziehung des Betriebsrates.....	374
a.	Annahme eines Beweisverwertungsverbotes	374
b.	Grundsätzliche Ablehnung	375

C. Fernwirkung.....	376
I. Strafprozess	376
II. Zivilprozess und Arbeitsgerichtsverfahren	377
D. Zusammenfassung.....	378
Kapitel 5 – Zusammenfassung.....	379
A. Kapitel 1 – Einführung	379
B. Kapitel 2 – Beschäftigtendatenschutz	380
C. Kapitel 3 – Strafbarkeitsrisiken einzelner Ermittlungsmaßnahmen	382
I. E-Mail-Screening.....	382
II. Kontrolle und Auswertung von Dokumenten, Dateien und Personalakten	383
III. Interviews	384
IV. Kontrolle des Postverkehrs.....	384
V. Kontrolle und Auswertung von Telefonaten und Verbindungsdaten – Telefonüberwachung	385
VI. Inaugenscheinnahme des Arbeitsplatzes	385
VII. Elektronischer Datenabgleich.....	385
D. Kapitel 4 – Prozessuale Folgeprobleme: Verwertbarkeit privater Beweismittel	386
Literaturverzeichnis	387