

Abhandlungen zum deutschen und
internationalen Arbeits- und Sozialrecht

Band 41

Die Kontrolle der Computernutzung von Arbeitnehmern

Von

Hendrik Jacob Wolters



Duncker & Humblot · Berlin

HENDRIK JACOB WOLTERS

Die Kontrolle der Computernutzung von Arbeitnehmern

Abhandlungen zum deutschen und
internationalen Arbeits- und Sozialrecht

Band 41

Die Kontrolle der Computernutzung von Arbeitnehmern

Von

Hendrik Jacob Wolters



Duncker & Humblot · Berlin

Die vorliegende Arbeit wurde im Sommersemester 2025
vom Fachbereich Rechtswissenschaft der Universität Trier
als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten

© 2026 Duncker & Humblot GmbH, Berlin

Satz: Typodienst – Büro für typographische Dienstleistungen, Altenberge

Druck: Prime Rate Zrt., Budapest, Ungarn

ISSN 2747-9021

ISBN 978-3-428-19815-3 (Print)

ISBN 978-3-428-59815-1 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Verlagsanschrift: Duncker & Humblot GmbH, Carl-Heinrich-Becker-Weg 9,
12165 Berlin, Germany | E-Mail: info@duncker-humblot.de
Internet: <https://www.duncker-humblot.de>

Inhaltsverzeichnis

Einleitung und Gang der Untersuchung	23
A. Einleitung	23
B. Gang der Untersuchung	26

1. Kapitel

Grundbegriffe und Interesse des Arbeitgebers an der Kontrolle der Computernutzung

A. Keylogger und Screenshot-Programme	28
B. Abgrenzung von privater und dienstlicher Nutzung	29
I. Dienstliche Nutzung	30
II. Private Nutzung	31
C. Erlaubnis der privaten Nutzung von Dienstrechnern	31
I. Grundsätzlich Entscheidungsrecht des Arbeitgebers	32
II. Zulässigkeit der privaten Nutzung bei fehlender Regelung?	32
1. Arbeitsgerichtliche und landesarbeitsgerichtliche Rechtsprechung	32
2. BAG	33
3. Literatur	34
4. Stellungnahme	35
III. Zulässigkeit aufgrund gesetzlicher Pflichten des Arbeitgebers	36
IV. Arbeitsvertragliche Regelung	37
V. Ausdrückliche Erlaubnis aufgrund des Direktionsrechts	37
1. Weisungsrecht	37
2. Gesamtusage	38
VI. Konkludente Erlaubnis	38
1. Vergabe von zwei E-Mail-Adressen	38
2. Zulassung der Privatnutzung von Telefoneinrichtungen	39
3. Voreinstellungen bei Webbrowsern	39
4. Zusammenfassung konkludenter Erlaubnisgründe	40

VII. Betriebsvereinbarung	40
1. Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 1?	40
a) Gegenstand der Mitbestimmungsrechte von § 87 Abs. 1 Nr. 1 BetrVG	40
b) Rechtsprechung und Literatur	41
c) Stellungnahme	42
d) Zwischenergebnis	42
2. Freiwillige Betriebsvereinbarung	43
3. Zusammenfassung	43
VIII. Betriebliche Übung	43
1. Dogmatische Herleitung	43
2. Betriebliche Übung bezüglich der privaten Internet- und Computernutzung?	44
a) Leistung des Arbeitgebers	45
aa) Vorliegen einer Leistung?	45
bb) Ausreichender Erklärungstatbestand	47
cc) Umfang der Nutzung	47
b) freiwillig	48
c) vorbehaltlos	48
d) gleichförmig	49
e) allgemein	49
f) wiederkehrend	49
3. Ergebnis	50
IX. Zusammenfassung	50
D. Interessen des Arbeitgebers an einer Kontrolle der Computernutzung	50
I. Kontrolle der Leistung des Arbeitnehmers	51
II. Pflichtverletzungen des Arbeitnehmers	51
1. Private Nutzung des Dienstrechners ohne Erlaubnis	51
2. Verletzung der Arbeitspflicht	51
3. Schutz von Geschäftsgeheimnissen	52
4. Verhinderung und Aufdeckung von Straftaten	52
5. Schutz der betrieblichen IT-Infrastruktur	53
III. Funktionsfähigkeit des Betriebes	53
IV. Zusammenfassung	53
E. Zusammenfassung	54

*2. Kapitel***Rechtsquellen**

55

A. Einfaches Recht	55
I. § 26 Abs. 1 BDSG	56
1. Entwicklung des BDSG	56
2. § 26 Abs. 1 BDSG als Rechtsgrundlage für die Arbeitnehmerüberwachung	57
3. Tatbestandsvoraussetzungen des § 26 Abs. 1 S. 1 BDSG	58
a) Personenbezogene Daten von Beschäftigten	58
b) Verarbeiten	59
c) Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses	59
d) Erforderlichkeit	60
4. Tatbestandsvoraussetzungen von § 26 Abs. 1 S. 2 BDSG	60
a) Auf tatsächlichen Anhaltspunkten begründeter Verdacht	61
b) Im Beschäftigungsverhältnis begangene Straftat	61
c) Dokumentation der Verdachtsgründe	61
d) Interessenabwägung	62
5. Keine Sperrwirkung des § 26 Abs. 1 S. 2 BDSG	62
II. Einwilligung des Arbeitnehmers in die Überwachung	63
1. Voraussetzungen für eine wirksame Einwilligung im Beschäftigungsverhältnis	63
2. Einwilligung in die Überwachung der Computernutzung?	64
a) Repressive Maßnahmen	65
b) Präventive Maßnahmen	65
c) Wirksamkeit der Einwilligung	65
aa) Rechtsprechung	65
bb) Literatur	66
cc) Stellungnahme	66
3. Ergebnis	69
III. § 3 TDDDG	69
1. Persönlicher Anwendungsbereich	70
a) Meinungsstand zu § 88 TKG a.F.	71
b) Übertragbarkeit auf die neue Rechtslage	72
aa) Arbeitgeber als Anbieter von Telekommunikationsdiensten	72
bb) Mitwirkung im Sinne von § 3 Abs. 2 Nr. 1 und 2 TDDDG	73
cc) Vorrang der DSGVO	73

c) Zwischenergebnis	75
2. Ergebnis	75
IV. Zusammenfassung	75
B. Verfassungsrecht	75
I. Grundrechtswirkung im Arbeitsverhältnis	76
1. Schutzpflichtenlehre	77
2. Ausstrahlungswirkung der Grundrechte	78
3. Einbruchstellen der Grundrechte bei der Kontrolle der Computernutzung ..	79
II. Recht auf informationelle Selbstbestimmung	79
1. Entwicklung des Grundrechts	79
2. Schutzbereich	81
3. Eingriff	82
4. Rechtfertigung von Datenverarbeitungen	82
5. Eröffnung des Schutzbereichs bei der Überwachung der Computernutzung	83
III. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	84
1. Schutzbereich	85
a) Sachlicher Schutzbereich	85
b) Persönlicher Schutzbereich	87
2. Eingriff	87
3. Rechtfertigung	88
a) Gewichtigkeit der geschützten Rechtsgüter	88
b) Gefahrengrad	88
c) Richtervorbehalt	89
d) Kernbereichsschutz	89
e) Zusammenfassung	90
4. Eröffnung des Schutzbereichs bei einer Überwachung der Computernutzung von Arbeitnehmern	91
a) Nutzung des informationstechnischen Systems „als eigenes“?	92
aa) Arbeitsgerichtliche Rechtsprechung	92
bb) Sachenrechtliche Auslegung	93
cc) Kriterium der berechtigten Nutzung	94
dd) Zwischenergebnis	95
b) Eröffnung des sachlichen Schutzbereichs bei Einsatz eines Keyloggers	95
aa) Informationstechnisches System	95
bb) Vertraulichkeit	96

cc) Integrität	96
dd) Zwischenergebnis	97
c) Ergebnis	97
5. Zwischenergebnis	97
IV. Fernmeldegeheimnis	97
1. Schutzbereich	98
2. Eröffnung des Schutzbereichs bei der Überwachung mittels Keyloggern ..	98
a) Gegen die Eröffnung des Schutzbereichs sprechende Argumente	99
b) Für eine Eröffnung des Schutzbereichs sprechende Argumente	99
c) Ergebnis	101
V. Konkurrenzen	101
1. Verhältnis Fernmeldegeheimnis und allgemeines Persönlichkeitsrecht	101
2. Verhältnis des Rechts auf informationelle Selbstbestimmung und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	102
a) Subsidiarität des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	103
b) Vorrang des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme bei Datenverarbeitung aus informationstechnischen Systemen	103
c) Zwischenergebnis	105
3. Ergebnis	105
VI. Zusammenfassung	106
C. Unionsrecht	106
I. Primärrecht	107
1. Art. 16 AEUV	107
2. Europäische Grundrechtecharta	108
a) Entwicklung	108
b) Anwendungsbereich der Unionsgrundrechte	108
c) Art. 7 GRC	109
d) Art. 8 GRC	110
3. Zwischenergebnis	111
II. Sekundärrecht	111
1. Kompetenzen und Wirkung	111
a) Kompetenz zum Erlass von Sekundärrechtsakten	112
b) Wirkung des sekundären Unionsrechts	112
2. DSRL	112

3. DSGVO	113
a) Geschichte	113
b) Anwendungsbereich	114
c) Regelungsgrundsätze der DSGVO	115
aa) Rechtmäßigkeit der Verarbeitung	115
bb) Verarbeitung nach Treu und Glauben	115
cc) Grundsatz der Transparenz	116
dd) Zweckbindungsgrundsatz	117
ee) Grundsatz der Datenminimierung	117
ff) Grundsatz der Richtigkeit	117
gg) Grundsatz der Speicherbegrenzung	117
hh) Integrität und Vertraulichkeit	118
ii) Rechenschaftspflicht	118
d) Art. 88 DSGVO	119
e) Zwischenergebnis	119
III. Anwendbare Grundrechte bei der Überwachung der Computernutzung	119
1. Verhältnis von Unionsrecht und nationalem Recht	120
a) Entwicklung der Rechtsprechung des EuGH zum Verhältnis von nationalem Recht und europäischem Recht	120
b) Rechtsprechung des EuGH zum Grundrechtsschutz bei mitgliedstaatlichen Handlungsspielräumen	121
c) Rechtsprechung des Bundesverfassungsgerichts zum Anwendungsvorrang	122
aa) Solange-Rechtsprechung des BVerfG	123
bb) Ausnahme: Überprüfung am Maßstab nationaler Grundrechte bei Umsetzungsspielraum	123
cc) Recht auf Vergessen I: Nebeneinander von Unionsgrundrechten und Grundrechten des GG	124
dd) Recht auf Vergessen II: Überprüfung am Maßstab der Unionsgrundrechte	125
d) Zwischenergebnis	126
2. Anwendbarkeit der Grundrechte des GG bei der Überwachung der Computernutzung von Arbeitnehmern	127
a) Gestaltungsspielraum bei der Umsetzung von Art. 88 DSGVO	127
aa) Kriterien des BVerfG	128
bb) Art. 88 DSGVO	128
(1) 1. Ansicht: Keine Abweichungen vom Harmonisierungsniveau der DSGVO möglich	129

(2) 2. Ansicht: Abweichungen nach oben vom Schutzniveau der DSGVO möglich	130
(3) 3. Ansicht: Abweichungen nach oben und nach unten vom Schutzniveau der DSGVO	131
(4) EuGH v. 30.03.2023, C-34/21 – Hauptpersonalrat der Lehrerinnen und Lehrer	132
(5) Stellungnahme	132
cc) Zwischenergebnis	134
b) Ausnahmsweise Prüfung am Maßstab der GRC wegen mangelnder Mitgewährleistung der Schutzstandards der GRC	135
3. Ergebnis	136
D. Völkerrecht	136
I. Vereinte Nationen	137
1. Allgemeine Erklärung der Menschenrechte	137
2. Art. 17 des internationalen Pakts über bürgerliche und politische Rechte	138
a) Der Menschenrechtsausschuss	139
aa) Zusammensetzung und Aufgaben	139
bb) Rechtsnatur der Berichte und general comments des Menschenrechtsausschusses	140
cc) Zusammenfassung	141
b) Art. 17 IPBPR	142
aa) Anwendbarkeit von Art. 17 IPBPR im Arbeitsverhältnis	142
bb) Materielle Gewährleistungen von Art. 17 IPBPR	143
cc) Zusammenfassung	144
c) Ergebnis	144
3. Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte	144
a) Der Ausschuss für wirtschaftliche, soziale und kulturelle Rechte	145
b) Art. 7 lit. b IPWSKR	145
c) Zusammenfassung	146
4. Zwischenergebnis	146
II. Internationale Arbeitsorganisation	146
1. Handlungsformen der ILO	147
2. Die Leitlinien zum Schutz von personenbezogenen Daten von Beschäftigten	148
3. Rezeption des Leitfadens	150
4. Zusammenfassung	150
III. Europarat	151
1. Allgemeines zum Europarat, der EMRK und der ESC	152

a) Der Europarat	152
b) Die EMRK	153
c) Der EGMR	153
d) Die ESC	154
e) Rechtsstellung der EMRK und der ESC in der deutschen Rechtsordnung	155
2. Art. 8 EMRK	156
a) Schutzbereich	156
b) Eingriff und positive Schutzpflichten des Staates	158
c) Rechtfertigung	159
3. EGMR v. 05.09.2017, 61496/08 (Bărbulescu/Rumänien)	160
a) Sachverhalt	160
b) Entscheidung des Gerichtshofs	161
aa) Anwendbarkeit von Art. 8 EMRK	161
bb) Einhaltung von Art. 8 EMRK	162
c) Analyse	165
aa) Eröffnung des Schutzbereichs von Art. 8 EMRK	166
bb) Information des Arbeitnehmers über Überwachung der elektronischen Kommunikation	167
cc) Ausmaß der Überwachung	168
dd) Legitimer Grund und Anlass für die Überwachungsmaßnahme	169
ee) Kein milderes Mittel	170
ff) Konsequenzen der Überwachung	170
gg) Verfahrensgarantien	171
d) Übertragbarkeit der Kriterien auf die Überwachung mittels Keylogger und andere Maßnahmen zur Kontrolle der Computernutzung	171
4. EGMR v. 22.02.2018, 588/13 (Libert/Frankreich)	171
a) Sachverhalt	172
b) Entscheidung des Gerichtshofs	173
aa) Eingriff in Art. 8 EMRK	173
bb) Rechtfertigung	173
c) Analyse	175
aa) Eröffnung des Schutzbereichs von Art. 8 EMRK	175
bb) Berechtigtes Ziel der Überwachung	175
cc) Angemessene und ausreichende Absicherungen gegen Missbrauch	175
5. Schutz vor Überwachung in der Europäischen Sozialcharta	176
6. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	177

7. Empfehlung des Ministerkomitees des Europarats vom 01.04.2015 – CM/Rec [2015]5 über die Verarbeitung von personenbezogenen Daten in Arbeitsverhältnissen	178
a) Rechtsnatur und Verbindlichkeit der Empfehlung	178
b) Regelung bezüglich der Arbeitnehmerüberwachung	178
c) Folgen der Regelungen in Ziff. 14 und 15 der Empfehlung für die Kontrolle der Computernutzung	179
aa) Verbot der Überwachung privater Kommunikation	180
bb) Vorrang milderer Mittel	180
cc) Ausschluss der Leistungs- und Verhaltenskontrolle	180
dd) Verbot heimlicher Überwachung	180
d) Zwischenergebnis	181
8. Zusammenfassung	181
IV. Zusammenfassung	182

3. Kapitel

Die Zulässigkeit der Überwachung der Computernutzung nach der arbeitsgerichtlichen Rechtsprechung 183

A. Rechtsprechung des BAG	184
I. BAG v. 27.07.2017, 2 AZR 621/16	184
1. Sachverhalt	184
2. Entscheidung des Gerichts	185
3. Analyse	187
a) Keine Einwilligung durch Schweigen	188
b) Auf tatsächliche Anhaltspunkte gestützter Verdacht	188
aa) Verdacht nur bei eingriffsintensiven Maßnahmen notwendig	189
bb) Verdacht einer schwerwiegenden Pflichtverletzung	189
cc) Notwendiger Verdachtsgrad	189
dd) Zusammenfassung	190
c) Keine Prüfung am Maßstab des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	190
d) Zusammenfassung	191
II. BAG v. 31.01.2019, 2 AZR 426/18	191
1. Sachverhalt	191
2. Entscheidung des Gerichts	192
3. Analyse	194
a) Nicht willkürlicher Anlass	194

b)	Hinweis des Arbeitgebers im Vorfeld der Maßnahme	195
c)	Keine Berücksichtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	196
aa)	Urteil zur Online-Durchsuchung	196
bb)	E-Mail Beschluss des BVerfG	197
cc)	Urteil des BVerfG zum BKA-Gesetz	198
dd)	Rechtsprechung des BVerfG zur Durchsicht elektronischer Speichermedien gemäß § 110 Abs. 3 StPO	199
ee)	Verwaltungsgerichtliche Rechtsprechung	202
ff)	Stellungnahme	203
gg)	Ergebnis	206
d)	Zusammenfassung	206
B.	Rechtsprechung der Landesarbeitsgerichte und Arbeitsgerichte	207
I.	ArbG Augsburg v. 04. 10. 2012, 1 BV 36/12	207
1.	Sachverhalt	207
2.	Entscheidung des Gerichts	208
3.	Analyse	209
a)	Einsatz des Screenshot-Programms nicht verhältnismäßig	209
b)	Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	210
II.	ArbG Cottbus v. 25. 11. 2014, 3 Ca 359/14	210
1.	Sachverhalt	210
2.	Entscheidung des Gerichts	211
3.	Analyse	211
a)	Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	212
b)	Kein konkreter Verdacht	212
III.	LAG Berlin-Brandenburg vom 14.01.2016, 5 Sa 657/15	212
1.	Sachverhalt	212
2.	Entscheidung des Gerichts	213
3.	Analyse	215
a)	Keine Erwähnung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	215
b)	Auswertung des Verlaufs in Abwesenheit des Arbeitnehmers	216
c)	Keine Ausführungen zu einem Anfangsverdacht	217
4.	Zusammenfassung	217

IV. LAG Hessen v. 21.09.2018, 10 Sa 601/18	218
1. Sachverhalt	218
2. Entscheidung des Gerichts	219
3. Analyse	221
a) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	221
b) Mangelnde Transparenz der Regelungen in der IT-Richtlinie	222
c) Zusammenfassung	223
C. Systematisierung der Rechtsprechung	223
I. Keine Prüfung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	223
II. Systematisierung der Rechtsprechung hinsichtlich der notwendigen Verdachtsgrade für Überwachungsmaßnahmen	224
1. Erste Stufe: Eingriffsintensive Maßnahmen	224
2. Zweite Stufe: Weniger eingriffsintensive Maßnahmen	225
a) Repressive wenig eingriffsintensive Maßnahme	225
b) Präventive wenig eingriffsintensive Maßnahmen	226
aa) Kein Verdacht notwendig	226
bb) Stichprobenhafte Kontrollen	227
D. Zusammenfassung	227

4. Kapitel

Das Urteil des EuGH vom 30.03.2023, C-34/21 – Hauptpersonalrat der Lehrerinnen und Lehrer und dessen Folgen für § 26 BDSG	229
A. Urteil des EuGH v. 30.03.2023, C-34/21 – Hauptpersonalrat der Lehrerinnen und Lehrer	229
I. Sachverhalt	229
II. Entscheidung des Gerichtshofs	230
1. Eröffnung des sachlichen und persönlichen Anwendungsbereichs der DSGVO	230
2. Erste Vorlagefrage	231
3. Zweite Vorlagefrage	233
B. Folgen für § 26 BDSG	234
I. Anforderungen des EuGH an spezifischere Vorschriften im Sinne des Art. 88 Abs. 1 DSGVO	234
1. Unterscheidung des Regelungsgehalts der nationalen Vorschriften von der DSGVO	235
2. Besondere Schutzmaßnahmen	236

II.	Bisheriger Standpunkt des BAG	236
III.	Konsequenzen des EuGH Urteils vom 30.03.2023 für § 26 BDSG	237
	1. § 26 Abs. 1 S. 1 BDSG	237
	2. § 26 Abs. 1 S. 2 BDSG	238
	3. § 26 Abs. 2 BDSG	240
	4. Zwischenergebnis	241
IV.	Folgen der Unanwendbarkeit von § 26 Abs. 1 S. 1 BDSG	241
	1. Anwendbarkeit von Art. 6 Abs. 1 DSGVO	241
	2. Zuständigkeit des EuGH	242
	3. Anzuwendende Grundrechte	242
	4. Konsequenzen für die Zulässigkeit der Kontrolle der Computernutzung	243
	a) Art. 6 Abs. 1 lit. b und f als Rechtsgrundlage für Überwachungsmaßnahmen	243
	b) Orientierung des EuGH an der Rechtsprechung des EGMR zu Art. 8 EMRK	243
	c) Verhältnis zu den Kriterien des BAG	244
	5. Zwischenergebnis	245
V.	Zusammenfassung	245

5. Kapitel

Anforderungen an eine neue gesetzliche Regelung zur Kontrolle der Computernutzung von Beschäftigten 247

A.	Einbeziehung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	248
I.	Schutzpflicht und Gestaltungsspielraum des Gesetzgebers	248
	1. Anerkennung einer Schutzpflicht hinsichtlich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch das BVerfG	248
	2. Gestaltungsspielraum des Gesetzgebers	250
II.	Anforderungen an das geschützte Rechtsgut	251
	1. Ausgangslage	251
	2. „Einfache“ Pflichtverletzungen nicht ausreichend	252
	3. § 626 Abs. 1 BGB: Außerordentliche Kündigung als Maßstab	253
	4. Schwerwiegendste Pflichtverletzungen als Maßstab	254
	5. Zwischenergebnis	255
III.	Verdachtsgrad	255
	1. Bedeutung und Begriff des Verdachts	255

2. Rechtsprechung des BAG	257
3. Verfassungsrechtliche Anforderungen an den Verdachtsgrad	258
a) Rechtsprechung des BVerfG zu präventiver Online-Durchsuchung	258
b) Rechtsprechung des BVerfG zu repressiver Online-Durchsuchung	259
c) Zwischenergebnis	260
4. Konsequenz der Rechtsprechung	260
5. Qualifizierter Tatverdacht in einer gesetzlichen Regelung zum Beschäftigtendatenschutz	262
6. Zwischenergebnis	262
IV. Vorherige Prüfung durch eine unabhängige Stelle	263
1. Rechtsprechung des BVerfG	263
2. Bisher keine Genehmigung vor einer Überwachungsmaßnahme vorgesehen	264
3. Denkbare Konstellationen für eine vorbeugende Kontrolle bei der Überwachung durch den Arbeitgeber	264
a) Richtervorbehalt	264
b) Prüfung durch Landesdatenschutzbeauftragte	265
c) Bewertung der Regelungsmöglichkeiten	265
aa) Richtervorbehalt	265
bb) Prüfung durch Landesdatenschutzbeauftragte	267
d) Zwischenergebnis	268
V. Kernbereichsschutz	268
1. Kernbereichsschutz bei staatlichen Eingriffen	268
2. Gefährdungslage bei der Überwachung der Computernutzung von Arbeitnehmern	269
3. Schutz des Kernbereichs privater Lebensgestaltung bei der Überwachung mittels Keylogger	270
a) Verhältnismäßigkeitsgrundsatz als ausreichender Schutz des Kernbereichs	270
b) Orientierung am Schutzkonzept des BVerfG	271
c) Kein besonderer Kernbereichsschutz bei verbotener Privatnutzung	271
d) Zwischenergebnis	271
4. Ergebnis	271
VI. Verhältnismäßigkeitsprüfung	272
VII. Abweichende Maßstäbe bei weniger intensiven Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	272
1. Offene Durchsicht des Dienstrechners	273
a) Rechtsprechung des BVerfG	273

b) Rechtsprechung des BAG	273
c) EGMR in der Rechtssache Libert	274
d) Anforderungen an eine gesetzliche Regelung	274
aa) Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	274
bb) Berechtigte Interessen des AG	275
cc) Kriterien	275
(1) Anlass der offenen Durchsuchung	275
(2) Vorherige Information	277
(3) Kennzeichnungsmöglichkeit privater Dateien	277
e) Zwischenergebnis	278
2. Kontrolle des Browserverlaufs	278
a) Rechtsprechung	278
b) Anforderungen an eine gesetzliche Regelung	279
aa) Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	279
bb) Berechtigte Interessen des Arbeitgebers	279
cc) Kriterien	280
(1) Anlass für die Kontrolle des Browserverlaufs	280
(2) Vorherige Information des Arbeitnehmers	280
(3) Begrenzte Speicherdauer	281
c) Ergebnis	281
VIII. Der Referentenentwurf eines Beschäftigtendatengesetzes	281
1. Aufbau des Beschäftigtendatengesetzes	282
2. Keine eigene Regelung zur Kontrolle der Computernutzung im BeschDG	282
3. Ergebnis	283
IX. Ergebnis	283
B. Spezifischere Vorschriften im Sinne von Art. 88 DSGVO	284
I. Unterscheidung des Regelungsgehalts von den Vorschriften der DSGVO	284
II. Besondere Schutzmaßnahmen	285
III. Zwischenergebnis	286
C. Zusammenfassung	286

6. Kapitel

Rechtsfolgen einer unrechtmäßigen Kontrolle	287
A. Geldbußen	287
B. Schadensersatz	288
C. Verwertungsverbot	288
I. Das prozessuale Problem	289
II. Keine einfachrechtliche Grundlage für Sachvortrags- und Beweisverwertungsverbote	289
III. Verfassungsrechtliche Herleitung von Sachvortrags- und Beweisverwertungsverbotten	290
IV. Einbeziehung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	291
V. Regelung im Referentenentwurf eines Beschäftigtendatengesetzes	291
D. Zusammenfassung	292
Fazit	293
Literaturverzeichnis	298
Sachwortverzeichnis	312

Einleitung und Gang der Untersuchung

A. Einleitung

Die Überwachung von Arbeitnehmern ist gängige Praxis. Arbeitgeber haben ein Interesse daran, ihre Arbeitnehmer zu überwachen und zu kontrollieren, um hierdurch etwa deren Leistungsfähigkeit und Arbeitseinsatz zu überprüfen, Arbeitsabläufe zu optimieren oder Schäden durch Diebstahl, Arbeitszeit- und Entgeltfortzahlungsbetrug oder den Verrat von Geschäftsgeheimnissen zu verhindern oder aufzuklären. Im Zuge der Corona-Pandemie dürfte sich das Interesse der Arbeitgeber, die Arbeitsleistung ihrer Arbeitnehmer zu kontrollieren noch weiter gesteigert haben. Denn viele Arbeitnehmer arbeiteten im Homeoffice, womit die Möglichkeit des „Blickes über die Schulter“ durch Arbeitgeber und Vorgesetzte wegfiel. Damit einher ging die Befürchtung der Arbeitgeber, die Arbeitnehmer könnten sich während ihrer Arbeitszeit im Homeoffice anderen Dingen als dem Erbringen ihrer Arbeitsleistung widmen.¹ Auch nach dem Ende der Corona-Pandemie bleibt der Anteil der Beschäftigten, die zumindest einen Teil ihrer Arbeitszeit im Homeoffice verbringen, deutlich über dem Niveau vor der Pandemie.²

Arbeitgeber überwachen ihre Arbeitnehmer mit unterschiedlichen Mitteln. Hierzu gehören etwa der Einsatz von Privatdetektiven, die Arbeitnehmer innerhalb, aber auch außerhalb der Arbeitszeit beobachten³, Schrankkontrollen⁴ oder die Torkontrolle zur Diebstahlsprävention⁵. Eine neue Dimension erlangen die oben genannten durchaus legitimen Arbeitgeberanliegen durch den technologischen Fortschritt. Neue Techniken lassen es zu, mit geringem finanziellem und personellem Aufwand eine lückenlose Überwachung der Beschäftigten zu installieren. Technologisch sind hier keine Grenzen mehr gesetzt. Zu erwähnen sind etwa die Videoüberwachung, die Ortung des mobilen Arbeitnehmers mittels GPS oder die Möglichkeit, die Nutzung des PC durch den Arbeitnehmer zu überwachen.

Letzterem kommt eine wachsende Bedeutung zu. Denn 55 % aller Beschäftigten in Deutschland nutzen nach einer Untersuchung des Statistischen Bundesamtes einen Computer mit Internetanschluss für geschäftliche Zwecke, wobei sich diese Nutzung keines-

¹ Aus den USA gibt es Berichte, dass Arbeitnehmer das Homeoffice nutzten, um eine zweite Vollzeittätigkeit aufzunehmen, wobei keiner der beiden Tätigkeiten die volle geschuldete Arbeitszeit gewidmet wird, vgl. <https://www.wsj.com/articles/these-people-who-work-from-home-have-a-secret-they-have-two-jobs-11628866529>, zuletzt abgerufen am 12.01.2026.

² <https://www.destatis.de/DE/Themen/Arbeit/Arbeitsmarkt/Qualitaet-Arbeit/Dimension-3/home-office.html> (zuletzt abgerufen am 12.01.2026).

³ BAG v. 29.07.2017, 2 AZR 597/16, NZA 2017, 1179; v. 19.02.2015, 8 AZR 1007/13, NZA 2015, 994; LAG Hamm v. 08.03.2007, 17 Sa 1604/06, BeckRS 2007, 44885; LAG Nürnberg v. 28.03.2003, 4 Sa 136/02, BeckRS 2003, 160990.

⁴ BAG v. 20.06.2013, 2 AZR 546/12, NZA 2014, 143.

⁵ BAG v. 09.07.2013, 1 ABR 2/13, NZA 2013, 1433.

wegs auf die klassischen Bürotätigkeiten beschränkt. Denn auch in produzierenden Wirtschaftszweigen, wie etwa der Automobilindustrie und dem Maschinen- und Anlagebau, arbeiten nur geringfügig weniger Beschäftigte, nämlich durchschnittlich 53 %, mit einem Rechner.⁶ Laut einer repräsentativen Befragung von Beschäftigten durch den DGB-Index Gute Arbeit aus dem Jahr 2022 nutzen 83 % der Arbeitnehmer in Deutschland digitale Anwendungen bei der Arbeit.⁷ Mit diesem hohen Anteil an Computerarbeitsplätzen korrespondiert die Möglichkeit des Arbeitgebers, seine Beschäftigten bei der Arbeit minutiös zu kontrollieren.

Die Frage, ob eine Überwachung zulässig ist, ist für beide Arbeitsvertragsparteien von erheblichem Interesse. Denn Arbeitgeber setzen die Überwachungsmaßnahmen nicht zum Selbstzweck ein. Sie möchten die gewonnenen Erkenntnisse als Grundlage für das Arbeitsverhältnis betreffende Entscheidungen, wie etwa Kündigungen oder Abmahnungen, zur Leistungskontrolle oder zum Schutz der betrieblichen IT-Infrastruktur verwenden.

Die Kontrolle der Computernutzung durch den Arbeitgeber kann auf verschiedenen Wegen erfolgen. So kann der Arbeitgeber die Festplatte durchsuchen⁸, kontrollieren welche Webseiten von dem Arbeitnehmer aufgerufen wurden⁹ oder spezielle Überwachungsprogramme¹⁰ einsetzen. Über den Einsatz eines solchen Überwachungsprogramms in Form eines Keylogger- und Screenshot-Programms hatte das BAG im Jahr 2017 zu entscheiden.¹¹ In dem der Entscheidung zugrundeliegenden Sachverhalt installierte ein Arbeitgeber auf dem Dienstrechner eines Arbeitnehmers ein Keylogger- und Screenshotprogramm. Hierdurch fand er heraus, dass der Arbeitnehmer den Computer – teilweise während der Arbeitszeit – für private Angelegenheiten nutzte. Daraufhin kündigte der Arbeitgeber das Arbeitsverhältnis. Das BAG entschied, dass diese Kündigung unwirksam sei, da der Einsatz des Programms unzulässig gewesen sei und deshalb die dadurch erlangten Informationen in dem Verfahren nicht verwertet werden dürften.

Da die Technologie dem Willen von Arbeitgebern, ihre Beschäftigten zu überwachen keine Grenzen mehr setzt, ist dies Aufgabe des Rechts. Es sind zwar durchaus berechtigte Gründe denkbar, die es rechtfertigen können, dass ein Arbeitgeber seine Beschäftigten überwacht. Den Interessen des Arbeitgebers stehen allerdings die Rechte und Interessen der Arbeitnehmer, insbesondere deren Persönlichkeitsrechte in ihrer Ausformung als Recht auf informationelle Selbstbestimmung und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (im Folgenden: IT-System-Grundrecht), entgegen. Die Schutzwürdigkeit des Rechts auf informationelle Selbstbestimmung, wonach jeder grundsätzlich selbst über die Verarbeitung seiner perso-

⁶ Statistisches Bundesamt, Unternehmen und Arbeitsstätten, Nutzung von Informations- und Kommunikationstechnologien in Unternehmen, 2017, S. 39, abrufbar unter: https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/IKT-in-Unternehmen-IKT-Branche/_inhalt.html#_x5j641si2 (zuletzt abgerufen am 02. 11. 2023).

⁷ DGB-Index Gute Arbeit, Report 2022: Digitale Transformation der Arbeitswelt, S. 4.

⁸ BAG v. 31.01.2019, 2 AZR 426/18, NZA 2019, 893.

⁹ LAG Berlin Brandenburg v. 14.01.2016, 5 Sa 657/15, BeckRS 2016, 67048.

¹⁰ ArbG Augsburg v. 04. 10. 2012, 1 BV 36/12, BeckRS 2013, 65588.

¹¹ BAG v. 27.07.2017, 2 AZR 681/16, NZA 2017, 1327; auch das Schweizerische Bundesgericht hatte einen ähnlichen Fall zu entscheiden, vgl. Schweizerisches Bundesgericht v. 17.01.2013, Leitentscheide des Schweizerischen Bundesgerichts (BGE) 139 II 7.

nenbezogenen Daten entscheiden darf, begründet das BVerfG nicht bloß mit seiner Bedeutung für die individuelle Freiheitsentfaltung, sondern vor allem auch mit der Bedeutung der informationellen Selbstbestimmung für ein freiheitlich demokratisches Gemeinwesen.¹² Das IT-System-Grundrecht hat das BVerfG 2008 angesichts des rasanten technologischen Fortschritts und der Tatsache, dass Computer in allen Lebensbereichen eine immer bedeutendere Rolle spielen entwickelt. Informationstechnische Systeme wie Computer und Smartphones erfüllen mehr und mehr die Funktion eines „ausgelagerten Gehirns“¹³, so dass Zugriffe auf diese oftmals ein umfassendes Persönlichkeitsbild ergeben. Dementsprechend stellt das BVerfG strenge Anforderungen an Eingriffe in dieses Grundrecht. Weder in der arbeitsrechtlichen Literatur noch in der arbeitsgerichtlichen Rechtsprechung hat das Grundrecht allerdings große Resonanz gefunden. Aufgrund der, insbesondere im Verhältnis zum Recht auf informationelle Selbstbestimmung, geringen Rezeption des neuen Grundrechts ist teilweise die Rede von dem „vergessenen Grundrecht“.¹⁴ Hinsichtlich der Arbeitnehmerüberwachung stellt sich die Frage, ob der Schutzbereich des IT-System-Grundrechts eröffnet ist. Ist dies der Fall, ist zu untersuchen, welche Anforderungen sich aus dem Grundrecht für eine zulässige Kontrolle der Computernutzung ergeben. Denn die hohen Hürden des BVerfG für einen gerechtfertigten Eingriff in dieses Grundrecht müssten dann auch berücksichtigt werden, wenn Arbeitnehmer durch ihren Arbeitgeber überwacht werden.

Im deutschen Recht regelt seit 2009 § 26 BDSG (§ 32 BDSG a. F.), ob Arbeitnehmerdaten verarbeitet werden dürfen und damit auch inwieweit Überwachungsmaßnahmen zulässig sind. Der Gesetzgeber orientierte sich bei der Norm inhaltlich an der zu dieser Thematik ergangenen Rechtsprechung des BAG. Dieses hatte schon, bevor es in Form des § 26 BDSG eine gesetzliche Grundlage für die Überwachung von Arbeitnehmern gab, eine Vielzahl von Fällen hierzu entschieden und eine Kasuistik entwickelt.

Die Frage, ob und auf welche Weise Arbeitgeber ihre Arbeitnehmer bei der Arbeit überwachen dürfen, ist nicht nur eine Frage des nationalen Rechts. Das liegt daran, dass das Datenschutzrecht unionsrechtlich überformt ist. Unionsrechtlich ist hier insbesondere die am 25. Mai 2018 in Kraft getretene Datenschutzgrundverordnung (DSGVO) zu beachten, die in Art. 88 eine eigene Norm zum Beschäftigtendatenschutz enthält, welche es den Mitgliedstaaten erlaubt, spezifischere Regelungen zum Schutz von Beschäftigtendaten zu erlassen. Auf diese Öffnungsklausel stützte der Gesetzgeber auch den bereits genannten § 26 BDSG.

Im Jahr 2023 entschied allerdings der EuGH, dass die im Wortlaut mit § 26 Abs. 1 S. 1 BDSG fast identische Regelung in § 23 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG) nicht mit Art. 88 DSGVO vereinbar ist.¹⁵ Dies wirft die Fragen auf, ob die Bestimmungen des § 26 BDSG nunmehr unanwendbar sind und arbeitgeberseitige Kontrollmaßnahmen nicht mehr auf diese Norm gestützt werden können. Weiterhin stellt

¹² BVerfG v. 15. 12. 1983, 1 BvR 209/83, BVerfGE 65, 1, Rn. 43.

¹³ Hoffmann-Riem, JZ 2008, 1009, 1112.

¹⁴ FAZ v. 26. 02. 2013, „Das vergessene Grundrecht“, online abrufbar unter: https://www.faz.net/aktuell/feuilleton/debatten/datenschutz-das-vergessene-grundrecht-12095331.html#pageIndex_2, zuletzt abgerufen am 12. 01. 2026.

¹⁵ EuGH v. 30. 03. 2023, C-34/21, ECLI:EU:C:2023:270 – Hauptpersonalrat der Lehrerinnen und Lehrer.

sich nunmehr die Frage, auf welche Rechtsgrundlage Arbeitgeber eine Kontrollmaßnahme stützen können, wenn § 26 BDSG nicht mehr angewendet werden kann.

Im Hinblick auf die Europäische Menschenrechtskonvention ist vor allem der von Art. 8 EMRK gewährleistete Schutz des Privatlebens zu berücksichtigen. Hierzu hat der EGMR jüngst in der gegen Rumänien ergangenen Entscheidung in der Rechtssache *Bărbulescu*¹⁶ Kriterien für die Zulässigkeit von Überwachungsmaßnahmen gegenüber Arbeitnehmern aufgestellt.

Neben dem Europarecht im weiteren Sinne ist für die Untersuchung des Themas auch ein Blick auf die Vorgaben von ILO und UNO zu werfen. Dementsprechend kann vor dem Hintergrund dieser europa- und völkerrechtlichen Regelungen die Frage, ob Überwachungsmaßnahmen zulässig sind, nicht mehr ohne eine internationale Perspektive beantwortet werden. Hier stellt sich die Frage, welche völkerrechtlichen Regelungen zum Arbeitnehmerdatenschutz existieren und welche Wirkungen sie auf das deutsche Recht haben.

B. Gang der Untersuchung

Die Arbeit hat zum Ziel aufzuzeigen, unter welchen Voraussetzungen die Kontrolle der Computernutzung von Arbeitnehmern zulässig ist und welche Anforderungen eine etwaige Neuregelung der Materie erfüllen muss, um mit den verfassungsrechtlichen sowie europa- und völkerrechtlichen Vorgaben vereinbar zu sein. Da die Überwachungsmethoden, wie oben angedeutet, sehr vielseitig sind, konzentriert sich die Untersuchung auf die Überwachung mittels sogenannter Keylogger- und Screenshot-Programme. Diese Programme sind interessant, da es sich dabei um relativ neue Methoden handelt, die in den letzten Jahren die Rechtsprechung beschäftigt haben.¹⁷ Obschon das Hauptaugenmerk der Arbeit auf dem Einsatz von Keylogger- und Screenshot-Programmen liegt, werden auch weitere Methoden zur Überwachung der Computernutzung, soweit sie die Rechtsprechung beschäftigt haben, untersucht. Dabei handelt es sich insbesondere um die Durchsicht des Dienstrechners und die Kontrolle von Browserverläufen. Diese Arbeit erhebt damit nicht den Anspruch, alle Überwachungsmethoden zur Kontrolle des Dienstrechners vollständig abzudecken. Insbesondere die Frage, ob eine Überwachung der E-Mail-Nutzung von Arbeitnehmern zulässig sein kann, ist nicht Thema der Arbeit. Dieser Problemkreis wurde in der Arbeitsrechtswissenschaft schon umfänglich diskutiert.¹⁸

Im ersten Kapitel werden zunächst einige Grundbegriffe, auf denen die Arbeit aufbaut, geklärt. Es wird beschrieben, was unter einem Keylogger- und Screenshot-Programm zu

¹⁶ EGMR v. 05.09.2017, 61496/08 (*Bărbulescu/Rumänien*), ECLI:CE:ECHR:2017:0905JUD006149608.

¹⁷ BAG v. 27.07.2017, 2 AZR 621/16, NZA 2017, 1327; ArbG Augsburg v. 04.10.2012, 1 BV 36/12, BeckRS 2013, 65588.

¹⁸ *Meyer-Michaelis*, Die Überwachung der Internet- und E-Mail-Nutzung am Arbeitsplatz; Koepen, Rechtliche Grenzen der Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz; *Mattl*, Die Kontrolle der Internet- und E-Mail-Nutzung am Arbeitsplatz; *Hoppe*, Private Nutzung betrieblicher Informations- und Kommunikationsmittel am Arbeitsplatz.

verstehen ist und wie diese funktionieren (A.). Zudem ist im Verlauf der Arbeit immer wieder der Unterschied, ob ein Arbeitnehmer den dienstlichen Rechner und Internetanschluss privat nutzt oder dienstlich nutzt, relevant. Denn die Rechtsprechung betont, dass die Überwachung privater Inhalte besonders schwerwiegend ist.¹⁹ Arbeitnehmer verletzen ihre arbeitsvertraglichen Pflichten, wenn sie den dienstlichen Rechner privat nutzen. Dies kann Anlass für den Arbeitgeber sein, Kontrollmaßnahmen zu ergreifen, um die Pflichtverletzung aufzudecken oder zu verhindern. Aus diesem Grund ist es notwendig, vorab zu klären, wann von einer privaten und wann von einer dienstlichen Nutzung von Rechner und Internetanschluss auszugehen ist (B.). Im Anschluss an diese Abgrenzung stellt sich die Folgefrage, wann es dem Arbeitnehmer erlaubt ist, den Dienstrechner für private Zwecke zu verwenden (C.). Denn bei dem Computer handelt es sich um Betriebsmittel, über deren Verwendung der Arbeitgeber als Eigentümer entscheiden kann. Darüber hinaus wird aufgezeigt, welche Interessen Arbeitgeber daran haben können, die Computernutzung ihrer Beschäftigten zu kontrollieren (D.).

Im zweiten Kapitel werden sodann die für die Kontrolle der Computernutzung von Arbeitnehmern relevanten Normen des nationalen einfachen Rechts (A.) sowie des Verfassungsrechts (B.), des Unionsrechts (C.) und des Völkerrechts (D.) dargestellt. Im Rahmen des nationalen Verfassungsrechts wird insbesondere geprüft, ob der Schutzbereich des IT-System-Grundrechts eröffnet ist, wenn ein Arbeitgeber die Computernutzung seiner Arbeitnehmer kontrolliert. Des Weiteren ist zu untersuchen, ob im Zusammenhang mit der Kontrolle der Computernutzung von Arbeitnehmern die Grundrechte des Grundgesetzes überhaupt anzuwenden sind. Da das Datenschutzrecht mit der DSGVO unionsrechtlich überformt ist, ist grundsätzlich auch der Anwendungsbereich der Unionsgrundrechte eröffnet.

Ausgehend von diesem rechtlichen Rahmen werden im dritten Kapitel die im Zusammenhang mit der Kontrolle der Computernutzung ergangene arbeitsgerichtliche Rechtsprechung analysiert und die dort entwickelten Kriterien dargestellt.

Sodann ist im vierten Kapitel das Urteil des EuGH vom 30.03.2024 und dessen Auswirkung auf die Regelung zum Beschäftigtendatenschutz in § 26 BDSG zu untersuchen. Denn der Gerichtshof führt in diesem Urteil aus, wann eine nationale Regelung zum Beschäftigtendatenschutz mit Art. 88 DSGVO vereinbar ist. Damit gibt er dem Gesetzgeber Anlass, den Beschäftigtendatenschutz neu zu regeln.

Dies führt zu der im fünften Kapitel untersuchten Frage, welche verfassungsrechtlichen, unionsrechtlichen und völkerrechtlichen Vorgaben bei einer solchen Neuregelung zu beachten sind.

Im sechsten Kapitel werden abschließend noch die möglichen Rechtsfolgen einer unrechtmäßigen Überwachung in Form von Geldbußen, Schadensersatz und Verwertungsverboten untersucht.

¹⁹ Vgl. LAG Hessen v. 21.09.2018, 10 Sa 601/18, NZA-RR 2019, 130, 134, Rn. 73.