Rechtsanwalt Dr. Klaus Herrmann und Dr. Michael Soiné*

Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz

Der Beitrag befasst sich mit Fragen des Grundrechtsschutzes bei Durchsuchungen und sonstigen Zugriffen auf persönliche Datenspeicher. Anhand der Zulässigkeitsvoraussetzungen und Anordnungskompetenzen werden zugleich deren Grenzen im Straf-, Disziplinar- und Arbeitsrecht aufgezeigt.

I. Einleitung

Durchsuchung ist die planmäßige Suche nach verborgenen Personen oder Sachen, deren genaue räumliche Lage den Durchsuchungsorganen nicht bekannt ist[1]. Zu den Durchsuchungsobjekten zählen auch persönliche Datenspeicher wie Personal-Computer (PC), lokale Datenspeicher auf nicht vernetzten DV-Geräten, mobile Speichermedien und Speicherlaufwerke in Netzwerken.

Im Unterschied dazu dienen allgemeine und ungezielte Kontrollen von Speichermedien durch Behörden und Unternehmen ausschließlich dem Schutz der eigenen IT-Infrastruktur. Sie betreffen die bestimmungsgemäße Behandlung von Daten sowie die Ausübung von Befugnissen durch die Nutzer (IT-Aufsicht). Schon diese systembezogenen Beschränkungen und Schutzmaßnahmen werfen grundrechtliche und datenschutzrechtliche Fragen auf, da die Nutzer dieser IT-Systeme in der Praxis z. B. über Umfang und Dauer der Speicherung täglicher Sicherheitskopien nicht unterrichtet werden.

II. Grundrechtsrelevanz von Durchsuchungen

Die Grundrechtsrelevanz von Durchsuchungen im IT-Bereich zeigt sich daran, dass gerade hier die Grenzen zwischen Sozial-, Privat- und Intimsphäre fließend sind[2]. Dabei geben weder die technische noch die eigentumsrechtliche Zuordnung der Speichermedien befriedigende Antworten hinsichtlich des grundrechtlichen Schutzbereichs. Während bei mobilen Speichermedien (USB-Sticks, Speicher von Fotokameras oder Mobiltelefonen) und lokalen Datenspeichern auf nicht vernetzten Datenverarbeitungsgeräten (Festplatten) die grundrechtsbezogene Berechtigung an den gespeicherten Inhalten mit der technischen Zugriffsbefugnis und regelmäßig auch

* Der Autor *Herrmann*, Fachanwalt für Verwaltungsrecht, ist Partner bei *Dombert* Rechtsanwälte, Potsdam; der Autor *Soiné* ist Bundesbeamter und Lehrbeauftragter an der Ludwig-Maximilians-Universität München.

1 Für Durchsuchungen nach der StPO vgl. *BVerfGE* 75, 318 (327) = NJW 1987, 2500; *BVerfG*, NJW 2000, 944; *BGH*, StV 2007, 60, und im Disziplinarrecht s. *BVerwGE* 120, 193 (203) = BeckRS 2009, 36932; *OVG Bremen*, ZBR 2007, 394. Für verwaltungsrechtliche Ermittlungen vgl. *BVerwGE* 121, 345 (349) = NJW 2005, 454. – Auf Durchsuchungen von Personen und Sachen nach dem Polizeirecht des Bundes und der Länder wird hier nicht eingegangen; s. dazu etwa die Aufstellung bei *Soiné*, in: *Wirth* (Hrsg.), Kriminalistik-Lexikon, 4. Aufl. (2011), S. 148.

2 Vgl. *Park*, Durchsuchung und Beschlagnahme, 2. Aufl. (2009), Rdnr. 763.

mit der Eigentümerstellung übereinstimmt, stellt sich vor allem bei der Nutzung von Netzwerkspeichern die Frage, ob es neben der technischen Zugriffsbefugnis und der privatrechtlichen Eigentümerstellung auch eine andere Berechtigung an den gespeicherten Daten gibt, die durch die Rechtsordnung und womöglich schon durch die Grundrechte geschützt ist. Dabei geht es in der Praxis nicht nur um die mehr oder weniger abgeschlossenen, jedenfalls örtlich fixierten Behörden- und Firmennetzwerke. Zunehmend stellen sich die Berechtigungsfragen für entfernte, zum Teil von nur vertraglich gebundenen Dienstleistern zur Verfügung gestellte Speicherressourcen, bei denen die einzelnen Nutzer nicht oder nur schwer lokalisieren können, auf welchem körperlichen Speichermedium ihre Daten abgelegt sind („Cloud Computing")[3].

Grundrechtliche Gefährdungen entstehen nicht nur durch Zugriffe auf die in Netzwerken gespeicherten Daten von außen, auch die fehlerhafte Handhabung ordnungsgemäß eingeräumter Befugnisse kann Grundrechtsverletzungen zur Folge haben: So obliegt die Wartung und Pflege der Server und Datenspeicher einem Systemadministrator, dem auch der Zugriff auf die von einzelnen Nutzern gespeicherten Daten, wie etwa die abgelegte ein- und ausgehende elektronische Post (E-Mails), technisch möglich ist. Dieser nimmt nach den technischen Erfordernissen alle Konfigurationen an der Hard- und Software vor. Er kann Daten selbst löschen und gelöschte Daten wiederherstellen. Durch das Beschäftigungs- bzw. Dienstverhältnis ist er verpflichtet, die Zugriffsmöglichkeiten ausschließlich im Rahmen konkret definierter Aufgaben auszuüben, die nur der Funktion des Netzwerks dienen. Er ist zwar technisch in der Lage, aber rechtlich nicht befugt, Inhalte fremder Datenbestände einzusehen oder zu nutzen[4].

Angesichts dieser kaum geregelten Ausübungsbereiche grundrechtlicher Freiheit wird deutlich, dass der individuelle Schutzanspruch für die Nutzung von IT-Systemen an die Zweckbestimmung der verarbeiteten Daten geknüpft ist. Vor diesem Hintergrund bedarf es einer Klärung der einschlägigen Grundrechtsfragen.

III. Recht auf informationelle Selbstbestimmung und Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Nach der Rechtsprechung des *BVerfG* gewährleistet das allgemeine Persönlichkeitsrecht (Art. 2 I i.V. mit Art. 1 I GG) dem Einzelnen einen räumlich und thematisch bestimmten Bereich, der grundsätzlich frei von unerwünschter staatlicher Einsichtnahme bleiben soll[5]. Das hieraus abgeleitete Recht auf informationelle Selbstbestimmung gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen[6]. Der Schutzumfang dieses Grundrechts beschränkt sich nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. Auch der Umgang mit personenbezogenen Daten, die für sich genommen nur geringen Informationsgehalt haben, kann – je nach Ziel des Zugriffs und der bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten – Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben[7]. Das allgemeine Persönlichkeitsrecht umfasst auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[8].

Das Speichern von Daten auf einem Speichermedium stellt als Nutzung informationstechnischer Systeme eine Grundrechtsausübung dar, wobei die erhobenen, verarbeiteten und genutzten Daten durch das Recht auf informationelle Selbstbestimmung geschützt sind (vgl. § 3 III, IV, V BDSG), auch wenn der speichernde Nutzer nicht das ausschließliche Zugriffsrecht hat (zumindest auch der Systemadministrator) und ihm die zum Netzwerk verbundenen technischen Geräte auch nicht als Eigentümer gehören.

Dem Recht auf informationelle Selbstbestimmung sind ebenso wie dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme Schranken gesetzt. Nach Ansicht des *BVerfG* muss der Einzelne solche Beschränkungen seiner Rechte hinnehmen, die auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen, welche wiederum dem Gebot der Normenklarheit und -bestimmtheit entspricht[9]. Der Gesetzgeber hat Anlass, Zweck und Grenzen eines Eingriffs hinreichend bereichsspezifisch und präzise festzulegen[10]. Klarheit und Bestimmtheit der Vorschrift sollen sicherstellen, dass der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen kann[11]. Diesem Postulat folgend haben der Bundes- und die Landesgesetzgeber Schrankenregelungen in unterschiedlichen Parlamentsgesetzen getroffen.

Parlamentsgesetze können demnach als Ermächtigungsgrundlage für Durchsuchungen und andere Zugriffe auf Speichermedien nur dienen, wenn sie ausdrücklich Eingriffe in das Recht auf informationelle Selbstbestimmung oder das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme regeln. Im Gegensatz dazu können Bundes- oder Landesgesetze, die diese Grundrechtseingriffe nicht explizit gestatten, ebenso wenig zu ihrer Rechtfertigung herangezogen werden wie die in der Normenhierarchie unterhalb von Parlamentsgesetzen stehenden Verwaltungsvorschriften sowie Dienst- und Betriebsvereinbarungen[12] (z. B. Verschlusssachenanweisungen, IT-Sicherheitskonzepte oder IT-Richtlinien), die dem Vorbehalt des Gesetzes nicht genügen[13].

Allein die auf Freiwilligkeit basierende Einwilligung schließt einen Grundrechtseingriff bei Durchsuchungen und anderen Zugriffen auf Speichermedien aus. Die ausdrücklich erteilte Einwilligung, die frei von Zwang zu Stande gekommen sein muss[14], bezieht sich nur auf den Einzelfall und setzt die eindeutige Kenntnis der Verweigerungsmöglichkeit voraus; eine stillschweigende Duldung genügt nicht[15]. Eine Einwilligung kann jederzeit vom Betroffenen widerrufen werden.

IV. Durchsuchungen nach dem Strafprozessrecht

§§ 102 ff. StPO gestatten als offene Ermittlungsmaßnahmen[16] Einschränkungen von Art. 2 I i. V. mit Art. 1 I und Art. 13 I GG. Das Verbot der Heimlichkeit bei Durchsuchungen ergibt sich aus §§ 105 II, 106 und 107 StPO[17]. Allgemein sind bei der Durchsuchung nach bzw. von Datenspeichern die Beschränkungen des § 104 StPO zu beachten.

Keiner Anordnung bedarf es bei ausdrücklicher Einwilligung des Betroffenen in die Durchsuchung. Liegen die Voraussetzungen der §§ 102 ff.

3 S. bereits *Obenhaus*, NJW 2010, 651.
4 *LAG Köln*, NZA-RR 2010, 579 (581).
5 *BVerfGE* 27, 344 (350 ff.) = NJW 1970, 555; *BVerfGE* 44, 353 (372 f.) = NJW 1977, 1489; *BVerfGE* 90, 255 (260) = NJW 1995, 1015; *BVerfGE* 101, 361 (382 f.) = NJW 2000, 1021.
6 *BVerfGE* 65, 1 (43) = NJW 1984, 419; *BVerfGE* 84, 192 (194) = NJW 1991, 2411.
7 *BVerfGE* 118, 168 (184 f.) = NJW 2007, 2464; *BVerfGE* 120, 274 (312) = NJW 2008, 822; *BVerwG*, NVwZ-RR 2011, 698.
8 *BVerfG*, NJW 2008, 822.
9 *BVerfGE* 120, 378 (407 f.) = NJW 2008, 1505.
10 *BVerfGE* 100, 313 (359 f., 372) = NJW 2000, 55; *BVerfGE* 110, 33 (53) = NJW 2004, 2213; *BVerfGE* 113, 348 (375) = NJW 2005, 2603; *BVerfG*, NJW 2007, 2464 (2467).
11 *BVerfGE* 110, 33 (52 ff.) = NJW 2004, 2213; *BVerfGE* 113, 348 (375 ff.) = NJW 2005, 2603.
12 *BVerwG*, NVwZ-RR 2011, 698.
13 Für Beihilfevorschriften des Bundes vgl. *BVerwGE* 121, 103 = NVwZ 2005, 713.
14 In Bezug auf die strafprozessuale Durchsuchung, s. *Hartmann*, in: HK Gesamtes StrafR, 2. Aufl. (2011), § 105 Rdnr. 1.
15 Hinsichtlich einer repressiven Durchsuchung, vgl. *Schmitt*, in: *Meyer-Goßner*, 54. Aufl. (2011), § 105 Rdnr. 1; *Gercke*, in: HK-StPO, 4. Aufl. (2009), § 105 Rdnr. 4.
16 *BVerfG*, NJW 2006, 976; NJW 2008, 822; *BGH*, NJW 2007, 930.
17 *BGH*, NJW 1997, 1934; *Zöller*, GA 2000, 573.

StPO nicht vor, ist er über die Freiwilligkeit zu belehren[18]. Der Betroffene kann seine Einwilligung formlos oder durch konkludentes Verhalten erklären[19]. Der Widerruf einer Einwilligung ist als Antrag entsprechend § 98 II 2 StPO zu verstehen[20]. Erfolgt der Widerruf während der Durchsuchung, so bedarf es zu deren Fortsetzung einer Anordnung nach § 105 I StPO; von den Ermittlungsbeamten kann in diesem Fall gegebenenfalls Gefahr im Verzug angenommen und die Maßnahme ohne richterlichen Beschluss fortgesetzt werden[21].

1. Durchsuchung beim Verdächtigen

§ 102 StPO ermächtigt zur Ermittlungsdurchsuchung bei einem Verdächtigen zum Auffinden von beschlagnahmefähigen Beweismitteln[22]. Computer, andere EDV-Anlagen sowie Datenträger unterliegen als Sachen[23] der Durchsuchung, wobei die vorherige Inbetriebnahme des Arbeitsplatzrechners zulässig ist[24]. Bei der Suche nach beweiserheblichen Daten auf internen oder externen Speichermedien handelt es sich um das ziel- und zweckgerichtete Gewinnen von Informationen, dem gegebenenfalls räumliche Einschränkungen bei vernetzten EDV-Systemen gesetzt sind. Werden Beweismittel auf den durchsuchten Speichermedien gefunden, ist der Durchsuchungszweck erreicht und die Durchsuchung muss beendet werden[25].

Der Grundsatz der Verhältnismäßigkeit ist bei der Anordnung und Durchführung von Durchsuchungen besonders zu beachten, das heißt die Maßnahme muss ebenso zur Aufklärung des Tatverdachts erfolgversprechend und erforderlich sein als auch angemessen im Hinblick auf die Schwere der Tat und die Stärke des Tatverdachts[26].

Soweit vorhanden und erfolgversprechend, sind weniger eingriffsintensive Ermittlungsmaßnahmen vorzuziehen[27]. Ein Verstoß gegen den Grundsatz der Verhältnismäßigkeit kann etwa vorliegen, wenn durch eine Anfrage beim Internet-Provider über die hinter einer E-Mail-Adresse stehende Person oder die Zurückverfolgung einer Zahlung qua (digitaler) Bankunterlagen eine Durchsuchung im EDV-Bereich beim Betroffenen vermieden oder deren Eingriffsintensität gemindert werden kann[28].

Beweismittel, die im Zuge einer ohne berechtigten Anfangsverdacht durchgeführten strafrechtlichen Durchsuchung und ohne wirksame Einwilligung des Betroffenen sichergestellt werden, unterliegen einem Verwertungsverbot[29].

2. Durchsuchung bei anderen Personen

§ 103 StPO ermächtigt zur Durchsuchung der Wohnung und anderer Räume, der Person und der Sachen von Personen, die nicht Verdächtige (§ 102 StPO) sind, z. B. Banken[30], Presseredaktionen oder Rechtsanwälte[31]. In Verfahren gegen Unbekannt ist eine Durchsuchung nach § 103 StPO zulässig[32], wenn gegen die noch nicht namentlich bekannte Person ein Tatverdacht gem. § 152 II StPO besteht[33]. Der Verhältnismäßigkeitsgrundsatz gebietet, den Betroffenen zunächst aufzufordern, den konkret gesuchten Beweisgegenstand freiwillig herauszugeben[34].

§ 103 StPO regelt die Suche nach bestimmten Gegenständen, so dass eine allgemeine Suche nach Beweismitteln unzulässig wäre[35]. Nach § 103 II StPO gelten die Beschränkungen des § 103 I 1 StPO nicht für Räume, in denen der Beschuldigte von Strafverfolgungsorganen oder Privatpersonen gem. § 127 I StPO ergriffen worden ist oder in denen er sich während der Verfolgung – auch nur kurzzeitig – aufhielt[36]. Da ein Verfolgter in den von ihm betretenen Räumen regelmäßig Spuren hinterlässt oder sich der Beute oder sonstiger Beweisstücke entledigt[37], kann z. B. auch die Durchsuchung des E-Mail-Postfachs eines Verdächtigen bei einem Provider oder des bei einer Bank eingeräumten Online-Kundenbereichs zur Sicherung entsprechender Spuren und tatrelevanter schriftlicher Äußerungen eines Verdächtigen führen.

§ 103 StPO gestattet auch die Durchsuchung von Dienstgebäuden und -räumen deutscher Behörden mit dem Ziel der Beschlagnahme elektronischer Behördenpost oder -akten. Datenspeicher in einem Dienstgebäude oder einer nicht allgemein zugänglichen Einrichtung oder Anlage der Bundeswehr werden nach § 105 III StPO durch die vorgesetzte Dienststelle der Bundeswehr durchsucht, wobei die ersuchende nichtmilitärische Stelle zur Mitwirkung, nicht nur zur bloßen Anwesenheit berechtigt ist. Über § 103 StPO darf aber nicht die Herausgabe von Akten und Unterlagen – auch Daten und Speichermedien – durchgesetzt werden, wenn eine Sperrerklärung der obersten Dienstbehörde nach § 96 StPO vorliegt[38]. Voraussetzung ist allerdings, dass die Inanspruchnahme von Amtshilfe zwischen den betroffenen Verwaltungsbehörden den Zwecken einer wirkungsvollen Strafverfolgung nicht genügt hat[39].

3. Vollzugskompetenzen

Nach § 105 I 1 StPO sind Durchsuchungen grundsätzlich vom Richter anzuordnen. Dies gilt auch für eine ohne Einverständnis des Betroffenen vorgenommene Durchsuchung des persönlichen Laufwerks eines Dienst-PC zur Konkretisierung eines Anfangsverdachts, unabhängig davon, ob der PC nach Dienstanweisungen oder -vereinbarungen auch privat genutzt werden darf[40]. Der Richtervorbehalt zielt auf eine vorbeugende Kontrolle der Durchsuchungsanordnung durch eine unabhängige neutrale Instanz ab[41]. Der Richter prüft eigenverantwortlich, ob die Voraussetzungen für den Erlass eines Durchsuchungsbeschlusses vorliegen, insbesondere, ob die Maßnahme verhältnismäßig ist[42].

Die Vollstreckung der richterlichen Durchsuchungsanordnung obliegt gem. § 36 II 1 StPO im Ermittlungsverfahren der Staatsanwaltschaft, die die Polizei oder andere Behörden

---

18 *OLG Hamburg*, StV 2008, 12; *Schmitt*, in: *Meyer-Goßner* (o. Fußn. 15), § 105 Rdnr. 1 m. w. Nachw.
19 S. *Hartmann*, in: HK Gesamtes StrafR (o. Fußn. 14), § 105 Rdnr. 1 m. w. Nachw.
20 *OLG Düsseldorf*, wistra 1997, 77; *LG Arnsberg*, wistra 1993, 199.
21 *BGH*, NStZ 1986, 85.
22 Eine auf Gewinnung von Tatsachen zur Begründung des Verdachts gerichtete *Ausforschungs*durchsuchung ist unzulässig, vgl. *BVerfGE* 20, 162 (192) = NJW 1966, 1603; *BVerfGE* 117, 244 = NJW 2007, 1117; *BVerfG*, NJW 2006, 2974; *LG Offenburg*, StV 1997, 626; *Schmitt*, in: *Meyer-Goßner* (o. Fußn. 15), § 102 Rdnr. 2; *Gercke*, in: HK-StPO (o. Fußn. 15), § 102 Rdnr. 2; *Beulke*, StrafprozessR, 11. Aufl. (2010), Rdnr. 256.
23 Vgl. *Graf/Hegmann*, StPO, 2010, § 102 Rdnr. 12.
24 *LG Bremen*, StV 2006, 571 (572); *Bär*, Hdb. zur EDV-Beweissicherung im Strafverfahren, 2007, Rdnrn. 361, 363, 364; *Eisenberg*, BeweisR der StPO, 7. Aufl. (2011), Rdnr. 2410.
25 S. *Bär* (o. Fußn. 24), Rdnr. 364.
26 *BVerfG*, NJW 2011, 2275.
27 *BVerfG*, NStZ-RR 2006, 110.
28 *BVerfG*, NStZ-RR 2006, 111; *Gercke*, in: HK-StPO (o. Fußn. 15), § 102 Rdnr. 32 m. w. Nachw.
29 *LG Bremen*, StV 2006, 571 mit Anm. *Stege*; *LG Freiburg*, StraFo 2006, 168 = BeckRS 2011, 10497.
30 Vgl. *Nack*, in: KK-StPO, 6. Aufl. (2008), § 103 Rdnr. 1 m. w. Nachw.
31 *LG Saarbrücken*, NStZ-RR 2002, 267.
32 *LG Trier*, StraFo 2007, 371 = BeckRS 2007, 11717.
33 S. *Nack*, in: KK-StPO (o. Fußn. 30), § 103 Rdnr. 2.
34 *LG Kaiserslautern*, NStZ 1981, 438; *LG Köln*, StV 2005, 260; *LG Mühlhausen*, wistra 2007, 195 = BeckRS 2007, 09062.
35 *BGH*, NStZ 2000, 155; NStZ 2002, 216; *LG Frankfurt a. M.*, MMR 2004, 339.
36 S. *Schmitt*, in: *Meyer-Goßner* (o. Fußn. 15), § 103 Rdnr. 15.
37 So *Pfeiffer*, StPO, 5. Aufl. (2005), § 103 Rdnr. 4; *Joecks*, StPO, 3. Aufl. (2011), § 103 Rdnr. 8.
38 Vgl. *Joecks* (o. Fußn. 37), § 103 Rdnr. 3.
39 *LG Wuppertal*, NJW 1992, 770.
40 *LG Bremen*, StV 2006, 571 (572).
41 Grundlegend *BVerfGE* 57, 346 (355) = NJW 1981, 2111; vgl. auch *BVerfGE* 76, 83 (91) = NJW 1987, 2499; *BVerfGE* 103, 142 (151) = NJW 2001, 1121.
42 *BVerfGE* 57, 346 (356) = NJW 1981, 2111; *BVerfGE* 103, 142 (151) = NJW 2001, 1121; *BVerfG*, NJW 2004, 3171; *LG Bielefeld*, wistra 2008, 117 (118) = BeckRS 2008, 12757.

mit ihrem Vollzug beauftragen kann[43]. Bei Gefahr im Verzug, das heißt, wenn die vorherige Einholung der richterlichen Anordnung den Erfolg der Maßnahme gefährden würde[44], sind die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 GVG) gem. § 105 I 1StPO auch zur Anordnung der Durchsuchung befugt. Nicht nur wegen des Ausnahmecharakters der nichtrichterlichen Anordnung, sondern vor allem wegen der grundrechtssichernden Schutzfunktion des Richtervorbehalts sind die Eilvoraussetzungen eng auszulegen und die tatsächlichen Anknüpfungspunkte besonders zu dokumentieren[45].

Die Eilbedürftigkeit darf z. B. nicht allein deshalb unterstellt werden, weil Dateien grundsätzlich von einem Berechtigten gelöscht werden können[46]. Hier muss dargelegt werden, dass eine kurzfristige Löschung unmittelbar bevorsteht. Gerade in Behörden- und Firmennetzwerken muss zudem von regelmäßig angefertigten Sicherungskopien und davon ausgegangen werden, dass trotz Löschung einzelner Daten oder ganzer Verzeichnisse verwertbare Daten noch in den Sicherungskopien gefunden werden können, sofern der Betroffene auf die Sicherungsdaten keinen Zugriff hat.

4. Durchsicht von Speichermedien

Nach § 110 III StPO sind die Ermittlungsorgane zur Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen befugt. Hierbei handelt es sich um eine inhaltliche Überprüfung der aufgefundenen Dateien daraufhin, ob die richterliche Beschlagnahme zu beantragen oder die Frei- bzw. Rückgabe notwendig ist[47]. Die Durchsicht gilt als Teil der Durchsuchung[48]. Sie stellt einen eigenständigen, gesondert anzuordnenden Eingriff dar, soweit sie über die (räumliche und gegenständliche) Eingrenzung des Durchsuchungszwecks im richterlichen Anordnungsbeschluss hinausgeht[49]. Liegen die Durchsuchungsvoraussetzungen zum Zeitpunkt der Durchsicht nicht mehr vor, ist auch die Durchsicht unzulässig[50].

§ 110 III StPO erfasst nicht nur die lokalen Speichermedien, etwa den Arbeitsplatzrechner, sondern ausdrücklich auch „räumlich getrennte Speichermedien", die von diesem Arbeitsplatzrechner aus erreichbar sind. Um die räumliche und gegenständliche Beschränkung des Durchsuchungszwecks in der richterlichen Anordnung mit ihrer grundrechtsschonenden Funktion praktisch nicht leerlaufen zu lassen, müssen die räumlich getrennten Speichermedien, auf die sich die Durchsicht beziehen kann (z. B. Nutzerkonten bei E-Mail-Providern), im Durchsuchungsbeschluss wenigstens gegenständlich beschrieben werden[51]. Die Zugriffe auf zugangsgeschützte Datenbestände sind stets offen durchzuführen, eine heimliche Durchsuchung oder Durchsicht ist von vornherein unzulässig[52].

Die damit eröffnete „Online-Durchsuchung" und die Durchsicht der aufgefundenen Dateien unterliegen wiederum dem Gebot der Verhältnismäßigkeit. Die Ermittlung muss in einem angemessenen Verhältnis zu der Schwere der Straftat und der Stärke des Tatverdachts stehen. Dabei sind auch die Bedeutung des potenziellen Beweismittels für das Strafverfahren sowie der Grad des auf verfahrenserhebliche Daten bezogenen Auffindeverdachts zu bewerten. Im Einzelfall können die Geringfügigkeit der zu ermittelnden Straftat, eine geringe Beweisbedeutung der auf dem Datenträger vermuteten Informationen sowie die Vagheit des Auffindeverdachts einer Sicherstellung des Datenbestands entgegenstehen[53]. Die Durchsicht „räumlich getrennter Speichermedien" per Online-Zugriff hat jedenfalls – so weltfremd dies in einer durch den globalen Austausch von Daten geprägten Informationsgesellschaft klingt – an der Staatsgrenze halt zu machen[54].

Nur die Staatsanwaltschaft und auf deren Anordnung ihre Ermittlungspersonen sind zur Durchsicht von Speichermedien befugt (§ 110 I StPO). Polizeibeamte, sonstige Beamte und Ermittler, die nicht zu dem in § 152 GVG bezeichneten Personenkreis gehören, können Dateien nicht ohne Einverständnis des Betroffenen durchsehen (§ 110 II 1 StPO), schon eine inhaltliche „Grobsichtung" wäre unzulässig[55]. Bei Arbeitsplatzrechnern und Servern kann für Zwecke der Durchsicht eine Kopie der Speichermedien erstellt werden[56]. Im Falle einer Mitnahme der betroffenen Hardware[57] sind geeignete Schutzvorkehrungen zu treffen, um einen unberechtigten Zugriff, einen Verlust oder eine Beschädigung auszuschließen[58].

Bei der Durchsicht eines externen Speichermediums gefundene potenziell beweiserhebliche Daten dürfen gem. § 110 III 2 Halbs. 1 StPO gesichert, das heißt gespeichert werden[59]. Ist ein Dritter Inhaber des nach § 110 III 1 StPO durchgesehenen externen Speichermediums und sind darauf gespeicherte Daten gem. § 110 III 2 Halbs. 1 StPO gesichert worden, ordnet § 110 III 2 Halbs. 2 StPO zur Wahrung der Rechte des Dritten die entsprechende Anwendung des § 98 II StPO an. Danach soll der zuständige Beamte unter den Voraussetzungen des § 98 II 1 StPO binnen drei Tagen die gerichtliche Bestätigung der Sicherung der aufgefundenen Daten beantragen. Wird die Sicherstellung von dem nach § 98 II 3–5 StPO zuständigen Gericht nicht bestätigt, sind die erhobenen Daten zu löschen, notfalls ist der Datenträger zu vernichten, um den zuvor bestandenen Zustand wiederherzustellen[60].

V. Strafandrohung des § 202 a StGB

Die strafprozessualen Beschränkungen des staatlichen Zugriffs auf persönliche Daten werden ergänzt durch den in § 202 a StGB zum Ausdruck gebrachten strafrechtlichen Schutz der Vertraulichkeit von Computernetzwerken. Die Vorschrift schützt auch solche Daten, die der Berechtigte in einem nicht von ihm betriebenen Netzwerk speichert, soweit durch die geschaffenen Beschränkungen der Zugriff unberechtigter Personen wesentlich erschwert wird[61]. § 202 a StGB soll dem Schutz des Verfügungsrechts über eine „formale Geheimsphäre" dienen. Diese ist deshalb formal, weil es nicht darauf ankommt, ob die Daten tatsächlich geheim sind. Maßgeblich ist, dass sie von Dritten ferngehalten werden sollen[62]. Dies gilt für die auf einem vom Arbeitgeber bzw.

43 S. *Nack*, in: KK-StPO (o. Fußn. 30), § 105 Rdnr. 7; ähnlich *Gercke*, in: HK-StPO (o. Fußn. 15), § 105 Rdnr. 63.
44 *BVerfGE* 51, 97 (111) = NJW 1979, 1539; *BVerfGE* 103, 142 (154) = NJW 2001, 1121; *BVerfG*, NJW 1979, 1540; *BGH*, NStZ 2006, 115; NJW 2007, 2269 = StV 2007, 337.
45 So ausdrücklich *BVerfGE* 103, 142 (153) = NJW 2001, 1121; *BVerfG*, NJW 2003, 2303; *OLG Hamm*, NStZ 2007, 356; *OLG Koblenz*, NStZ 2002, 660 = StV 2002, 533 (534).
46 Vgl. aber z. B. *Eisenberg* (o. Fußn. 24), Rdnr. 2410.
47 *OLG Frankfurt a. M.*, NStZ-RR 1997, 74; *OLG Jena*, NJW 2001, 1290, mit abl. Anm. *Hohmann*, wistra 2001, 196.
48 *BGHSt* 44, 265 (273) = NJW 1999, 730.
49 *BVerfG*, NJW 2003, 2669 (2670 f.).
50 *BVerfG*, NJW 2009, 2518 (insoweit nicht abgedr.) = BeckRS 2009, 32749.
51 Vgl. *Knierim*, StV 2009, 211; *Ladiges*, in: *Radtke/Hohmann*, StPO, 2011, § 110 Rdnr. 16.
52 *BGHSt* 51, 211 = NJW 2007, 930; zum Ganzen s. nur *Schmitt*, in: *Meyer-Goßner* (o. Fußn. 15), § 110 Rdnr. 6 m. w. Nachw.
53 *BVerfG*, Beschl. v. 19. 6. 2008 – 2 BvR 1111/08, BeckRS 2008, 37758.
54 So schon *Bär* (o. Fußn. 24), Rdnr. 374; weiterführend *ders.*, Zeitschrift für internationale Strafrechtsdogmatik (ZIS) 2011, 53; *Schmitt*, in: *Meyer-Goßner* (o. Fußn. 15), § 110 Rdnr. 7 a: Durchsicht bei offen zugänglichen Daten im Ausland zulässig.
55 *Schmitt*, in: *Meyer-Goßner* (o. Fußn. 15), § 110 Rdnr. 4 m. w. Nachw.; a. A. *Nack*, in: KK-StPO (o. Fußn. 30), § 110 Rdnr. 7.
56 Vgl. *Bäcker/Freiling/Schmitt*, DuD 2010, 80; *Ladiges*, in: *Radtke/Hohmann* (o. Fußn. 51), § 110 Rdnr. 12 m. w. Nachw.
57 *BVerfG*, NJW 2002, 1410.
58 So *Nack*, in: KK-StPO (o. Fußn. 30), § 110 Rdnr. 5; *Ladiges*, in: *Radtke/Hohmann* (o. Fußn. 51), § 110 Rdnr. 13.
59 *Schmitt*, in: *Meyer-Goßner* (o. Fußn. 15), § 110 Rdnr. 7 m. w. Nachw.
60 So *Schmitt*, in: *Meyer-Goßner* (o. Fußn. 15), § 110 Rdnr. 8.
61 Vgl. *Schmitz*, JA 1995, 478 (482) mit Beispielen.
62 S. *Hilgendorf/Frank/Valerius*, Computer- und InternetstrafR, 2005, Rdnr. 654; *Dietrich*, NStZ 2011, 249: Bezeichnung im Dateinamen z. B. als „geheim" oder „privat".

Dienstvorgesetzten zur Verfügung gestellten Speicherlaufwerk abgelegten persönlichen Daten, sofern dieser Datenspeicher auch zur persönlichen Nutzung überlassen wird[63]. Mit der Bereithaltung eines individuellen kennwortgeschützten Laufwerks wird eine „geschützte Persönlichkeitsenklave" geschaffen[64].

Die „besondere Sicherung" i. S. von § 202 a StGB verlangt keinen umfassenden Schutz der gespeicherten Daten[65]. Generell genügen Passwortsysteme[66] oder Zugangssicherungen[67], solange die grundsätzliche Zugriffssteuerung im Datenverarbeitungszentrum – so genannter „closed shop"[68] – gewährleistet wird[69]. Die Vorkehrung muss objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sein, den Zugriff auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren[70].

Deshalb liegt eine Überwindung „besonderer Sicherungen gegen unberechtigten Zugriff" auch vor, wenn sich andere Mitarbeiter des Arbeitgebers, sogar der Systemadministrator, faktische Zugriffsmöglichkeiten auf die gespeicherten Daten verschaffen. Allein das Wissen um ein Passwort begründet noch keine Berechtigung[71]. § 202 a StGB verlangt nach seinem Wortlaut gerade nicht, dass die gespeicherten Daten vor dem Zugriff des Täters gesichert sind, weil dann die korrekte Gesetzesfassung hätte lauten müssen: „... und *ihm gegenüber* gegen Zugang besonders gesichert sind"[72]. Hierbei muss zwischen der faktischen Zugriffsmöglichkeit und der Verwendungsbestimmung der gespeicherten Daten unterschieden werden[73]. Täter i. S. von § 202 a StGB kann nur jemand sein, für den die Daten nach dem insoweit maßgeblichen Willen des Verfügungsberechtigten, der die persönlichen Daten auf dem Speichermedium abgelegt hat, nicht bestimmt sind[74].

VI. § 27 BDG und beamtenrechtliche Befugnisse während und außerhalb des Disziplinarverfahrens

Gefahren für die vom Schutz des Rechts auf informationelle Selbstbestimmung umfassten personenbezogenen Daten bestehen auch bei hoheitlichen Ermittlungen in den Sonderstatusverhältnissen der Beamten, Richter und Soldaten.

1. Durchsuchung als Ermittlungsmaßnahme im Disziplinarverfahren

§ 27 I BDG regelt die Durchsuchungsbefugnisse zur Aufdeckung und Ahndung von Dienstvergehen abschließend und setzt eine förmliche Einleitung des Disziplinarverfahrens nach § 17 BDG voraus, in dem rechtsstaatliche Sicherungen zu Gunsten des betroffenen Beamten greifen[75]. Diese Vorschrift rechtfertigt aber keinen Zugriff des Dienst- oder Disziplinarvorgesetzten auf persönliche Datenspeicher eines Beamten. Gemäß § 27 I 1 BDG bedarf im Disziplinarverfahren jede Durchsuchung (und Beschlagnahme) – grundsätzlich auch bei Gefahr im Verzug – einer richterlichen Anordnung des zuständigen Verwaltungsgerichts[76]. Dies gilt nach der Rechtsprechung auch für die Durchsuchung (und Beschlagnahme) von Dateien auf einem dienstlichen Computer[77]. Durchsuchungsfähig sind nicht nur die im Eigentum, Besitz oder Gewahrsam des betreffenden Beamten befindlichen privaten Gegenstände, sondern auch die sich im Besitz oder Gewahrsam befindlichen dienstlichen Gegenstände. Es genügt faktischer Mitbesitz oder Mitgewahrsam an der Sache. Dieser liegt vor, wenn der Beamte über ein Passwort – abgesehen von den Systemadministratoren – andere Personen vom Zugriff auf den ihm dienstlich zur Verfügung gestellten Datenspeicher ausschließen kann[78].

Die Durchsuchung setzt stets einen Ermittlungsantrag gegenüber dem Verwaltungsgericht durch einen bestellten oder beauftragten Beschäftigten des Dienstherrn voraus, der die Befähigung zum Richteramt hat (§ 27 I 1 i. V. mit § 25 III BDG). Da § 27 II BDG auch den Vollzug der richterlichen Durchsuchungsanordnung den „nach der Strafprozessordnung dazu berufenen Behörden" vorbehält, kommt eine Durchsuchung durch Bedienstete des Dienstherrn auch bei Vorliegen einer richterlichen Anordnung grundsätzlich nicht in Betracht[79]. Unter Verstoß gegen die Anordnungsvoraussetzungen gewonnene Beweismittel unterliegen einem Verwertungsverbot[80].

Erforderlich ist der dringende Verdacht eines schwerwiegenden Dienstvergehens, das eine Entfernung aus dem Dienst, die Aberkennung des Ruhegehalts oder wenigstens eine Zurückstufung rechtfertigt; der Anfangsverdacht – wie bei der Einleitung des Disziplinarverfahrens (§ 17 BDG) – genügt nicht[81]. Zieht das mutmaßliche Dienstvergehen nur einen Verweis oder eine Geldbuße nach sich (wie es z. B. für eine Veröffentlichung von Kritik an innerdienstlichen Entscheidungen von Dienstvorgesetzten angenommen wurde[82]), sind diese Maßnahmen unverhältnismäßig[83]. Hingegen ist eine Durchsuchung des Heim-PCs verhältnismäßig, wenn die dort aufgefundenen Daten zum Nachweis eines im erheblichen Umfang geführten Internet-Versandhandels führen, den der Beamte vor allem in zahlreichen seiner krankheitsbedingten Fehlzeiten betrieben hat, weil insofern wenigstens eines Zurückstufung in Betracht käme[84].

Die bei einer Durchsuchung nach § 27 BDG aufgefundenen Daten können erst nach einer – gesondert zu beantragenden und zu begründenden – Beschlagnahme für das Disziplinarverfahren verwertet werden. Dies ist aber nur zulässig, wenn sie schon nach der äußeren Beschaffenheit (Datei-Informationen, Fundort) zum Nachweis eines erheblichen Dienstvergehens dienen und der Beamte in die Sicherstellung und Verwertung nicht einwilligt. Das Öffnen der Dateien und die Überprüfung ihres Inhalts ohne Einverständnis des Beamten bedarf als Durchsicht entsprechend § 110 III StPO einer ei-

63 *LG Bremen*, StV 2006, 571 (572).
64 *BVerwG*, NVwZ-RR 2011, 698; vgl. bereits *Weißgerber*, NZA 2003, 1005 (1006).
65 So *Schmachtenberg*, DuD 1998, 401 (402).
66 Vgl. *Fischer*, StGB, 58. Aufl. (2011), § 202 a Rdnr. 9 a; *Kindhäuser*, LPK-StGB, 4. Aufl. (2010), § 202 a Rdnr. 4.
67 S. *Lackner/Kühl*, StGB, 27. Aufl. (2010), § 202 a Rdnr. 4; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, 28. Aufl. (2010), § 202 a Rdnr. 8.
68 Zum Begriff vgl. *Marberth-Kubicki*, Computer- und InternetstrafR, 2005, Rdnr. 69.
69 S. *Hilgendorf/Frank/Valerius* (o. Fußn. 62), Rdnr. 669.
70 So *Marberth-Kubicki* (o. Fußn. 68), Rdnr. 69.
71 So jetzt ausdrücklich *Marberth-Kubicki*, Computer- und InternetstrafR, 2. Aufl. (2010), Rdnr. 92.
72 Vgl. *Lenckner/Eisele*, in: *Schönke/Schröder* (o. Fußn. 67), § 202 a Rdnr. 9.
73 S. *Hilgendorf/Frank/Valerius* (o. Fußn. 62), Rdnr. 669 m. w. Nachw.
74 So *Schmitz*, JA 1995, 478 (481 f.).
75 *BVerwG*, NVwZ-RR 2011, 698.
76 S. *Weiß*, in: GKÖD Bd II, Losebl. (Stand: 2/2011), § 27 BDG Rdnr. 16; *Gansen*, DisziplinarR in Bund und Ländern, Losebl. (Stand: Mai 2009), § 27 BDG Rdnr. 4. – Ausnahmen finden sich z. B. bei § 17 II 2 BadWürttDG und § 20 II 1 WDO.
77 *LG Bremen*, StV 2006, 571; *OVG Bremen*, NordÖR 2006, 414 = ZBR 2007, 394; *VGH München*, Beschl. v. 8. 8. 2005 – 16 a CD 05.1692, BeckRS 2005, 30107.
78 *BVerwG*, NZWehrr 2008, 71 (72 f.) = BeckRS 2011, 53972; NVwZ-RR 2011, 698; *OVG Bremen*, NordÖR 2006, 414 = ZBR 2007, 394; *OVG Bautzen*, Urt. v. 7. 6. 2010 – D 6 A 32/09, BeckRS 2010, 54103.
79 *BVerwG*, NVwZ-RR 2011, 698; *Gansen* (o. Fußn. 76), § 27 Rdnr. 40; Ausnahme: § 17 II 3 BadWürttDG – Ausführung durch Disziplinarbehörde.
80 Vgl. *Hummel*, in: *Hummel/Köhler/Mayer*, BDG, 4. Aufl. (2009), § 27 Rdnr. 10; *Gansen* (o. Fußn. 76), § 27 Rdnrn. 38 f. – Daneben kommt eine Strafbarkeit des unzuständigen Beamten gem. § 132 StGB in Betracht.
81 S. *Hummel*, in: *Hummel/Köhler/Mayer* (o. Fußn. 80), § 27 Rdnr. 5; *Gansen* (o. Fußn. 76), § 27 Rdnr. 22; *Claussen/Benneke/Schwandt*, Das Disziplinarverfahren, 6. Aufl. (2010) Rdnrn. 77, 607.
82 *BVerfG*, NVwZ 2006, 1282 (1283).
83 Vgl. *Gansen* (o. Fußn. 76), § 27 Rdnr. 25.
84 *OVG Koblenz*, NVwZ-RR 2007, 318 (320 f.).

genständigen Ermächtigungsgrundlage[85]. Da eine vergleichbare Eingriffsbefugnis im Disziplinarrecht fehlt und § 27 BDG auf diese Vorschrift nicht verweist[86], sind der Disziplinarvorgesetzte und seine Bediensteten (Ermittlungsführer, Systemadministrator) zur inhaltlichen Prüfung von Daten, die auf persönlichen Laufwerken des Beamten abgelegt sind, ohne Zustimmung des Betroffenen nicht berechtigt.

2. Keine Durchsuchung im Rahmen von „Verwaltungsermittlungen" oder „Vorermittlungen"

Außerhalb des Disziplinarverfahrens, d. h. vor oder ohne dessen Einleitung (§ 17 BDG), besteht keine Befugnis des Dienstvorgesetzten, ohne Einwilligung des Betroffenen gezielt Verzeichnisse auf Arbeitsplatzrechnern und Servern zu durchsuchen, die dem Beamten zur personenbezogenen Datenablage zugewiesen sind[87]. Darüber hinaus ist der Dienstvorgesetzte weder im Disziplinarverfahren noch bei „dienstlichen" Ermittlungen zu einer heimlichen Durchsuchung befugt. § 27 I 3 BDG setzt ebenso wie § 102 StPO voraus, dass die Ermittlungen dem Betroffenen gegenüber offengelegt werden[88].

Heimliche Überwachungsmaßnahmen sind mit einem Anpassungsdruck auf das Verhalten und Einschüchterungseffekten verbunden[89] und kollidieren regelmäßig mit den Grundrechten[90]. Selbst Sicherheitsbehörden wie Polizei und Nachrichtendienste werden durch die ihre Aufgaben und Befugnisse regelnden und für die Eigensicherung geltenden Gesetze (BKAG, BPolG, Polizeigesetze der Länder, BVerfSchG, BNDG, MADG, SÜG, Verfassungsschutzgesetze der Länder)[91] nicht zu derartigen Eingriffen ermächtigt; Gleiches gilt für private Unternehmen mit besonderen Sicherheitsaufgaben.

3. IT-Routinemaßnahmen

Die Beamtengesetze[92] gestatten das Erheben, Verarbeiten und Nutzen personenbezogener Daten von Beschäftigten durch öffentliche Stellen, soweit dies unter anderem zur Durchführung des Dienst- und Arbeitsverhältnisses bzw. personeller Maßnahmen erforderlich ist. Die in Verwaltungsvorschriften geregelte dienstliche Nutzung von IT-Systemen betrifft z. B. die Erhebung und Speicherung von betriebsinternen Datenverlaufsprotokollen (Log-Files), dienstinternem Mailverkehr sowie Internetverlaufsprotokollen. Die Maßnahmen dienen nicht nur zur Datenschutzkontrolle, Datensicherung oder Gewährleistung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage, sondern können auch zum Zwecke der Dienstaufsicht erstellt werden. So dürfen etwa Internetverlaufsprotokolle in einem Disziplinarverfahren zum Nachweis der umfangreichen nichtdienstlichen PC-Nutzung herangezogen werden[93].

Aus der Organisationshoheit des Dienstherrn fließende allgemeine Maßnahmen, z. B. das Speichern und Veröffentlichen von personenbezogenen Daten für Zwecke des Publikumsverkehrs (Behördenwegweiser, Übersichtstafeln, Namensschilder, Geschäftsverteilungspläne auf Internetseiten)[94], sind aber von ziel- und zweckgerichteten Zugriffen abzugrenzen. Das *BVerwG* hat Maßnahmen der präventiven Dienstaufsicht – gegenüber der gezielten Durchsuchung – auch für den IT-Bereich danach charakterisiert, ob dienstliche Ressourcen und Gegenstände lediglich auf Vollzähligkeit, pflegliche Behandlung, Einsatzbereitschaft, Sauberkeit, Sicherheit und Ordnung überprüft werden[95].

Hinsichtlich weitergehender Datenerhebungen muss der Dienstvorgesetzte das Einverständnis des Beamten für jede Identifikation von Dateien und deren Einsichtnahme einholen, die durch ein persönliches Kennwort oder die Ablage in einem nur ihm zugänglichen Ordner in einem Speichermedium gegen unberechtigten Zugriff gesichert sind.

Auf Grund des auch im Disziplinarrecht geltenden Grundsatzes der Selbstbelastungsfreiheit ist ein Beamter nicht verpflichtet, Ermittlungsmaßnahmen zum Nachweis von Dienstpflichtverletzungen durch Erklärung seines Einverständnisses zu unterstützen[96]. Jedenfalls setzt eine Einwilligung des Beamten sowohl Freiwilligkeit als auch Kenntnis vom Durchsuchungszweck voraus, so dass eine nachträglich eingeholte „Genehmigung" einer bereits erfolgten Durchsuchung dann unwirksam und unbeachtlich ist, wenn der Betroffene nicht über die bereits stattgefundene Maßnahme informiert wird.

VII. Ermittlungen zur Durchsetzung zivilrechtlicher Ansprüche im Arbeitsrecht

Auch im Bereich der arbeitsrechtlichen Beschäftigungsverhältnisse (einschließlich des öffentlichen Dienstes) ist eine Durchsuchung bzw. Durchsicht von persönlichen Datenspeichern ohne Einwilligung des Betroffenen grundsätzlich unzulässig; ein unbefugtes Eindringen in diese Speichermedien kann unter Bezugnahme auf das Recht auf informationelle Selbstbestimmung abgewehrt werden[97].

Der Arbeitgeber kann eine Befugnis zur Auswertung von passwortgeschützten Dateien eines Arbeitnehmers (z. B. persönlich empfangene E-Mails) auch nicht aus § 88 III TKG ableiten, wonach ein Anbieter von Telekommunikationsdienstleistungen zum Schutz seiner technischen Systeme bestimmte Inhalte und nähere Umstände der Telekommunikation aufzeichnen darf. Zum einen betrifft § 88 TKG nur die Übermittlung von Informationen an individuelle Empfänger und umfasst deshalb nicht die Auswertung von übermittelten und gespeicherten Daten. Zum anderen wird ein Arbeitgeber, der seinen Arbeitnehmern die private Nutzung des dienstlichen E-Mail-Accounts gestattet, noch nicht zum Diensteanbieter i. S. des TKG[98].

Die Drittwirkung der Grundrechte im Arbeitsverhältnis haben die Fach- und Verfassungsgerichte etwa bei den unbefugt abgehörten oder mitgeschnittenen Telefonaten gestärkt, indem bei nicht gerechtfertigten Grundrechtseingriffen ein Beweisverwertungsverbot aus dem betroffenen Grundrecht abgeleitet wird[99]. Ähnliche Verwertungsverbote gelten bei geheimen Videoaufnahmen[100] und der Überwachung durch andere Personen[101]. Der Arbeitnehmer willigt mit dem Arbeitsvertrag nicht automatisch in eine ganzheitliche Überwachung seines Arbeitsplatzes und seiner Arbeit ein[102].

§ 32 I 2 BDSG gestattet aber die Erhebung personenbezogener Daten des Arbeitnehmers bezüglich einer zu vermutenden Straftat. Notwendig

85 So *LG Bremen*, StV 2006, 571. A. A. *Gansen* (o. Fußn. 76), § 27 BDG Rdnrn. 16, 44.
86 Vgl. *Weiß*, in: GKÖD Bd. II (o. Fußn. 76), § 27 BDG Rdnrn. 32 ff., zur Reichweite des Verweises in § 27 I 3 BDG.
87 *BVerwG*, NVwZ-RR 2011, 698; *OVG Bremen*, NordÖR 2006, 414 = ZBR 2007, 394 – in Bezug auf einen Polizeibeamten; *Gansen* (o. Fußn. 76), § 27 BDG Rdnr. 13. – Unzulässig wäre aber das Verschleiern einer Durchsuchung mit vorgeblichen „IT-Routinekontrollen", um an geschützte Daten zu gelangen.
88 *BVerwG*, NVwZ-RR 2011, 698.
89 *BAGE* 111, 173 = NJW 2005, 313.
90 *BVerfG*, NJW 2008, 1505.
91 Für Maßnahmen der Eigensicherung des BND vgl. *Soiné*, DÖV 2006, 205.
92 Vgl. z. B. § 106 IV BBG, § 117 IV SächsBG.
93 *OVG Bautzen*, Urt. v. 7. 6. 2010 – D 6 A 32/09, BeckRS 2010, 54103.
94 *BVerwG*, ZTR 2008, 406 = BeckRS 2008, 33735, verneinte insoweit schon einen Grundrechtseingriff.
95 *BVerwGE* 120, 193 (203) = BeckRS 2009, 36932; *BVerwG*, NZWehrr 2008, 71 = BeckRS 2011, 53972.
96 *BVerwGE* 73, 118 = BeckRS 2010, 55415 (Verweigerung der Mitwirkung an Atemalkoholmessung).
97 *BAGE* 20, 96 (102) = NJW 1968, 72; *BAGE* 41, 37 = NJW 1983, 1691 (1692); *Wiese*, ZfA 1977, 273 (277) m. w. Nachw. – Dies setzt aber die Kenntnis des Betroffenen vor Durchführung der Maßnahme voraus.
98 *LAG Berlin-Brandenburg*, NZA-RR 2011, 342; *LAG Hannover*, NZA-RR 2010, 406.
99 *BVerfG*, AP BGB § 611 Persönlichkeitsrecht Nr. 32 = BeckRS 2001, 30197086; *BGH*, NJW 2003, 1727 = AP BGB § 611 Persönlichkeitsrecht Nr. 38; *BAGE* 41, 37 = NJW 1983, 1691; *BAG*, NZA 1988, 92.
100 *BAG*, NJW 2003, 3436 = NZA 2003, 1193; NJW 2005, 313 = NZA 2004, 1278; NZA 2008, 1187 = AP BetrVG 1972 § 75 Nr. 54.
101 So *Röckl/Fahl*, NZA 1998, 1035.
102 S. *BAG*, NJOZ 2005, 2708 = NZA 2005, 839 Os. (für Videoüberwachung des Arbeitsplatzes).

sind tatsächliche Anhaltspunkte und eine Dokumentation, die den Verdacht und die Datenerhebung rechtfertigen[103]. Erforderlich ist ferner eine Interessenabwägung zwischen den jeweiligen Individualinteressen des Arbeitnehmers und Arbeitgebers[104], die den betroffenen Grundrechten Rechnung trägt[105].

VIII. Fazit

Das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme setzen der Durchsuchung persönlicher Datenspeicher verfassungsrechtliche Grenzen. Einfachgesetzlich schränken der Vorbehalt richterlicher Anordnungen, ausgewählte Vollzugskompetenzen und die Pflicht zur Beachtung des Grundsatzes der Verhältnismäßigkeit den erlaubten Zugriff von Strafverfolgungsbehörden, Disziplinarvorgesetzten und Arbeitgebern drastisch ein. Willigt der Betroffene zuvor in die Einsichtnahme der Speichermedien ein, bedürfen Durchsuchungen keiner gesetzlichen Ermächtigungsgrundlage, denn in diesen Fällen scheidet ein Grundrechtseingriff aus. Zu berücksichtigen ist jedoch, dass eine frei von Zwang zu Stande gekommene und ausdrücklich erteilte Einwilligung sich nur auf den Einzelfall bezieht und die eindeutige Kenntnis der Verweigerungsmöglichkeit voraussetzt. Auch kann eine Einwilligung jederzeit vom Betroffenen widerrufen werden. ■

---

103 Vgl. etwa *ArbG Berlin*, BB 2010, 2309 = BeckRS 2010, 68681 Rdnr. 23.

104 *BGH*, NJW 1984, 1889; *Hoppe*, Private Nutzung betrieblicher Informations- und Kommunikationsmittel am Arbeitsplatz, 2010, S. 534 ff.

105 *BAG*, NJW 2003, 3436 (3437 m. w. Nachw.); *Wybita*, BB 2010, 1086.