

CB-BEITRAG

Univ.-Prof. Dr. Christian Koenig, LL. M. (LSE), und Dr. Anton Veidt, Wiss. Mit.*

E-Mail- und Internetnutzung von Beschäftigten auf dem Prüfstand des Fernmeldegeheimnisses – Teil 2

In Teil 1 dieses Beitrags (erschienen in CB 2024, 194) wurden die unionsrechtliche Abgrenzungsproblematik des Fernmeldegeheimnisses nach § 3 TDDDG zur DSGVO und die Adressatenstellung des Arbeitgebers nach § 3 Abs. 2 S. 1 TDDDG behandelt. Teil 2 widmet sich nun dem Schutzbereich des Fernmeldegeheimnisses und den Verhaltenspflichten nach § 3 Abs. 3 TDDDG für Arbeitgeber bei der Einsichtnahme in E-Mails und Internet-Surf-Verläufe von Beschäftigten. Zudem werden konkrete Handlungs- und Gestaltungsempfehlungen für Arbeitgeber formuliert.

I. Schutzbereich des Fernmeldegeheimnisses und Verhaltenspflichten nach § 3 Abs. 3 TDDDG

1. Grundlagen

Der sachliche Schutzbereich des Fernmeldegeheimnisses erstreckt sich auf den Inhalt und die näheren Umstände der Telekommunikation (§ 3 Abs. 1 TDDDG).¹ Die zeitliche Reichweite des Schutzes durch das Fernmeldegeheimnis wurde im Wesentlichen durch die Rechtsprechung des BVerfG zu Art. 10 Abs. 1 GG konturiert, die maßgebende Auslegungsdirektiven für den Schutzbereich des einfachgesetzlichen Fernmeldegeheimnisses nach § 3 TDDDG beinhaltet.² Danach endet der Schutz des Fernmeldegeheimnisses erst nach Abschluss des Kommunikationsvorgangs (1.) im ausschließlichen Herrschaftsbereich des Kommunikationsteilnehmers in einer Weise, die ihm das Löschen der Kommunikationsinhalte und -verkehrsdaten ermöglicht (2.).³ Der Schutz des Fernmeldegeheimnisses ist damit nicht auf den eigentlichen Übertragungsakt im Sinne eines dynamischen Vorgangs beschränkt, sondern besteht auch nach Beendigung des Übertragungsvorgangs fort, solange ein Zugriff auf den Inhalt und die näheren Umstände durch einen Telekommunikationsdienstleister erfolgt (bzw. erfolgen kann).

Sofern der Schutzbereich des Fernmeldegeheimnisses eröffnet ist, ist es den Normadressaten nach § 3 Abs. 3 S. 1 TDDDG untersagt, sich Kenntnis von geschützten Kommunikationsinhalten und -umständen zu verschaffen, sofern dies nicht zur Erbringung eines Telekommunikationsdienstes oder zum Schutz eines technischen Systems erforderlich ist. Als grundsätzlich erforderlich wird insbesondere die – bis zu einem gewissen Grad mit der Kenntnisnahme von Kommunikationsinhalten und -umständen einhergehende – Viren- und Spam-Filterung angesehen.⁴ Die zulässige Informationsbeschaffung ist in den Datenschutzvorschriften der §§ 9 ff. TDDDG geregelt. Soweit besondere Regelungen für Eingriffe mit gehobener Intensität bestehen, wie etwa zur Verarbeitung von Verkehrsdaten (§ 9 TDDDG) sowie zur Störungsbeseitigung (§ 12 TDDDG), sind

diese abschließend. Eine weitergehende Überwachung wird durch § 3 Abs. 3 S. 1 TDDDG gesperrt.⁵ Nach § 3 Abs. 3 S. 2 TDDDG dürfen die adressierten Anbieter und Betreiber Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in § 3 Abs. 3 S. 1 TDDDG genannten Zweck verwenden, d.h. zur Erbringung ihrer Dienste und für den Betrieb ihrer Netze und Anlagen einschließlich des Schutzes ihrer technischen Systeme (sog. Zweckbindungsgrundsatz).

2. Zulässigkeit der Kontrolle von E-Mails und der Internetnutzung von Beschäftigten durch den Arbeitgeber nach § 3 TDDDG

Die Kommunikation via E-Mail fällt in den Schutzbereich des § 3 TDDDG.⁶ Auch bereits versendete bzw. empfangene E-Mails von Beschäftigten sind im Lichte der Rechtsprechung des BVerfG Schutzgegenstand nach § 3 TDDDG und damit vom Kenntnisnahmeverbot umfasst, solange sie auf dem arbeitgeberseitigen E-Mail-Server gespeichert sind und eine Zugriffsmöglichkeit des Arbeitgebers besteht.⁷ Die gegenläufige Literatur- und Rechtsprechungsansicht, wonach E-Mails mit dem Zugang im Postfach des Beschäftigten in seinen Herrschaftsbereich gelangt seien und daher nicht mehr dem Fern-

* Der Beitrag beruht auf einem Rechtsgutachten.

1 Siehe hierzu weitergehend *Eckhardt*, in: Schwartmann/Jaspers/Eckhardt (Hrsg.), TTDSG, 1. Aufl. 2022, § 3 Rn. 13 ff. sowie *Nolte*, in: Säcker/Körber (Hrsg.), Kommentar TKG – TTDSG, 4. Aufl. 2023, § 3 TTDSG Rn. 11 ff.

2 *Eckhardt*, in: Schwartmann/Jaspers/Eckhardt (Fn. 1), § 3 Rn. 18.

3 BVerfG, 2.3.2006 – 2 BvR 2099/04, MMR 2006, 220; 16.6.2009 – 2 BvR 902/06, MMR 2009, 674.

4 *Hadidi*, in: Geppert/Schütz (Hrsg.), Beck'scher TKG-Kommentar, 5. Aufl. 2023, § 3 TTDSG Rn. 24.

5 *Nolte*, in: Säcker/Körber (Fn. 1), § 3 TTDSG Rn. 35.

6 *Munz*, in: Taeger/Gabel (Hrsg.), DSGVO – BDSG – TTDSG, 4. Aufl. 2022, § 3 TTDSG Rn. 9.

7 *Nolte*, in: Säcker/Körber (Fn. 1), § 3 TTDSG Rn. 15.

meldegeheimnis unterliegen würden,⁸ verkennt hingegen, dass auf den IT-Systemen des Arbeitgebers gespeicherte E-Mails sich *nicht ausschließlich* im Herrschaftsbereich des Beschäftigten befinden, da stets eine Zugriffsmöglichkeit des Arbeitgebers besteht.⁹ Nur wenn E-Mails nach Abschluss des Übertragungsvorgangs im alleinigen Herrschaftsbereich des Beschäftigten – etwa lokal und passwortgeschützt auf einem dienstlichen Endgerät oder auf einem eigenen Endgerät des Beschäftigten ohne Zugriffsmöglichkeit des Arbeitgebers – gespeichert werden und damit auch die Möglichkeit zur vollständigen Löschung durch den Beschäftigten besteht, endet der Schutz des Fernmeldegeheimnisses mit der Beendigung des Übertragungsvorgangs.¹⁰

Auch nach der Auffassung, wonach der Arbeitgeber bei erlaubter Privatnutzung Normadressat nach § 3 Abs. 2 S. 1 TDDDG sei,¹¹ gilt das Fernmeldegeheimnis nur, soweit der Arbeitgeber geschäftsmäßig Telekommunikationsdienste anbietet (Nr. 2) bzw. erbringt (Nr. 4), also nur soweit es um die Privatnutzung geht. Befinden sich in einem Postfach sowohl dienstliche als auch private E-Mails, schlägt das Kontrollverbot für die privaten E-Mails allerdings auf die im Übrigen (nach § 3 TDDDG) zulässige Kontrolle der dienstlichen E-Mails durch, da bei der Einsichtnahme in das Postfach stets auch eine Kenntnisnahme privater E-Mails – sei es nur deren Betreffzeile – erfolgen könnte.¹²

Im Ergebnis wäre eine Einsichtnahme in das E-Mail-Postfach von Beschäftigten grundsätzlich nach § 3 Abs. 3 S. 1 TDDDG unzulässig, sofern man annimmt, dass der Arbeitgeber Normadressat gem. § 3 Abs. 2 S. 1 TDDDG sei. Auch § 3 Abs. 3 S. 4 TDDDG, wonach die Anzeigepflicht nach § 138 StGB Vorrang gegenüber der Pflicht zur Wahrung des Fernmeldegeheimnisses genießt, vermittelt keine Befugnis zu einer systematischen Überwachung der Telekommunikation nach derartigen Katalogstraftaten für das verpflichtete Unternehmen.¹³ Etwas anderes könnte sich lediglich im jeweiligen Einzelfall aus einer behördlichen Anordnung, etwa auf Grundlage von § 2 Abs. 1a G 10, § 100a StPO oder 100g StPO, ergeben.¹⁴ Eine Einsichtnahme in das E-Mail-Postfach von Beschäftigten kann auch nicht auf §§ 9 oder 12 TDDDG gestützt werden. Insbesondere gilt § 12 Abs. 4 TDDDG (Missbrauch von Telekommunikationsdiensten) nicht analog für andere, nicht aufgeführte Straftaten, die nicht auf die rechtswidrige Inanspruchnahme des Telekommunikationsdienstes gerichtet sind und dadurch den Entgeltanspruch des Diensteanbieters gefährden.¹⁵ In der Literatur wird zwar mitunter vertreten, dass eine Inhaltskontrolle der E-Mails von Beschäftigten in besonderen Ausnahmefällen zulässig sei, etwa bei einem hinreichend konkreten Verdacht auf die Begehung einer Straftat oder den Verrat von Geschäftsgeheimnissen.¹⁶ Diese – nicht näher begründete – Ansicht findet im Wortlaut des § 3 Abs. 3 TDDDG jedoch keine Stütze und bildet jedenfalls keine rechtssichere Grundlage für die Kontrolle der E-Mails von Beschäftigten zur Aufklärung von Straftaten oder (schweren) Vertragspflichtverletzungen.

Auch ein empfängergesteuerter Abruf von Informationen aus dem Internet erfüllt die Kriterien der körperlosen Übermittlung von Signalen mittels Telekommunikationsanlagen, also der Telekommunikation.¹⁷ Das „Surfen“ im Internet ist daher ebenfalls durch § 3 TDDDG geschützt. Sofern eine Kontrolle der Internetnutzung durch sog. Webtracking-Tools erfolgt, welche die besuchten URLs sowie die verwendeten dynamischen IP-Adressen speichern und verarbeiten, gelten damit die Verhaltenspflichten des § 3 Abs. 3 TDDDG,¹⁸ sodass eine Kontrolle der Internetnutzung grundsätzlich unzulässig wäre. Ist hingegen lediglich die Einsichtnahme in Browserchroniken von Be-

schäftigten beabsichtigt, stellt sich wiederum die Frage nach der Eröffnung des zeitlichen Anwendungsbereichs des § 3 TDDDG. Das LAG Berlin-Brandenburg hat in seinem Urteil vom 14.1.2016 die Auffassung vertreten, dass die in der Browserchronik auf einem dienstlichen Endgerät eines Beschäftigten gespeicherten Verbindungsdaten nicht durch § 88 TKG a.F. (§ 3 TDDDG) geschützt würden, da der Übertragungsvorgang bereits abgeschlossen war und die Verbindungsdaten im Herrschaftsbereich des Kommunikationsteilnehmers gespeichert seien.¹⁹ Sofern (und solange) hingegen eine (gleichzeitige) Zugriffsmöglichkeit des Arbeitgebers – etwa aufgrund einer Speicherung der Verbindungsdaten (auch) auf dem Internet-Server des Arbeitgebers – besteht, sind die in der Browserchronik gespeicherten Verbindungsdaten hingegen nicht dem ausschließlichen Herrschaftsbereich des Kommunikationsteilnehmers zuzurechnen und unterliegen daher dem Fernmeldegeheimnis.²⁰

II. Handlungs- und Gestaltungsempfehlungen für Arbeitgeber

Sofern man annimmt, dass Arbeitgeber, welche die Privatnutzung betrieblicher E-Mail- und Internetzugangsdienste erlauben, Normadressaten des Fernmeldegeheimnisses seien, ist die Einsichtnahme in E-Mails und Internet-Surf-Verläufe von Beschäftigten nach § 3 Abs. 3 TDDDG somit grundsätzlich verboten. Fraglich ist daher, welche Maßnahmen Arbeitgeber ergreifen könnten bzw. sollten, um ihre Kontrollmöglichkeiten gegenüber den Beschäftigten in gewissem Umfang zu wahren und zugleich einen Verstoß gegen § 3 TDDDG zu vermeiden.

1. Einholung der Einwilligung des Beschäftigten

Eine Kenntnisnahme lässt sich im Rahmen des § 3 Abs. 3 TDDDG grundsätzlich durch eine Einwilligung rechtfertigen. Die Einwilligung wird als Rechtfertigungstatbestand in § 3 TDDDG zwar nicht aufgeführt, muss aber im Wege einer unionsrechtskonformen Auslegung im Lichte des Art. 5 Abs. 1 S. 2 der Richtlinie 2002/58/EG²¹ (E-Privacy-RL), der eine Einwilligung ausdrücklich als Ausnahme zur grundsätz-

8 LAG Berlin-Brandenburg, Urt. v. 16.2.2011 – 4 Sa 2132/10, NZA-RR 2011, 342, 343 f.; aus der Literatur etwa *Fischer*, ZD 2012, 265, 269.

9 *Jenny*, in: Plath (Hrsg.), DSGVO/BDSG/TTDSG, 4. Auflage 2023, § 3 TTDSG Rn. 29.

10 *Nolte*, in: Säcker/Körper (Fn. 1), § 3 TTDSG Rn. 15.

11 Siehe hierzu Teil 1 dieses Beitrags (CB 2024, 194).

12 *Brink/Joos*, in: Boecken/Düwell/Diller/Hanau (Hrsg.), Gesamtes Arbeitsrecht, 2. Aufl. 2022, § 26 BDSG Rn. 125; *Riesenhuber*, in: BeckOK Datenschutzrecht, 46. Edition, § 26 BDSG Rn. 171.

13 *Hadidi*, in: Geppert/Schütz (Fn. 4), § 3 TTDSG Rn. 45.

14 *Nolte*, in: Säcker/Körper (Fn. 1), § 3 TTDSG Rn. 38.

15 *Nolte*, in: Säcker/Körper (Fn. 1), § 3 TTDSG Rn. 29.

16 *Vietmeyer/Byers*, MMR 2010, 807 (809); *Wolf/Mulert*, BB 2008, 446.

17 Vgl. BVerfG, 6.7.2016 – 2 BvR 1454/13, NJW 2016, 3508, Rn. 38.

18 *Greening/Weigl*, CR 2012, 787, 788 f.

19 LAG Berlin-Brandenburg, 14.1.2016 – 5 Sa 657/15, BB 2016, 819, Rn. 144.

20 So wohl LAG Hessen, 21.9.2018 – 10 Sa 601/18, NZA-RR 2019, 130, Rn. 66 unter Verweis auf BVerfG, 6.7.2016 – 2 BvR 1454/13, NJW 2016, 3508, Rn. 38.

21 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 v. 31.7.2002, S. 37–47.

lichen Vertraulichkeit der Kommunikation vorsieht, in § 3 Abs. 3 TDDDG hineingelesen werden.²²

Gem. Art. 5 Abs. 1 S. 2 E-Privacy-RL müssen allerdings „*alle betroffenen Nutzer*“ einwilligen. Im Hinblick auf die Einsichtnahme in das E-Mail-Postfach wäre eine Einwilligung durch die Beschäftigten daher nicht ausreichend, da der Schutz des § 3 Abs. 3 TDDDG gegenüber den Kommunikationspartnern der Beschäftigten fortbestehen würde.²³ Die – nicht näher begründete – Gegenansicht, wonach eine Einwilligung der Beschäftigten in die Einsichtnahme des E-Mail-Verkehrs im Rahmen des § 3 Abs. 3 TDDDG rechtfertigend wirken könne,²⁴ ist hingegen nicht mit den unionsrechtlichen Anforderungen an eine rechtfertigende Einwilligung gem. Art. 5 Abs. 1 S. 2 E-Privacy-RL vereinbar.

In der Literatur wird zwar mitunter vertreten, dass der Beschäftigte und seine Kommunikationspartner eine konkludente Einwilligung in die Kenntnisnahme durch den Arbeitgeber erteilen würden, sofern der Beschäftigte über eine offensichtlich dienstliche E-Mail-Adresse kommuniziert.²⁵ Gerade im Hinblick auf den privaten E-Mail-Verkehr dürfte es jedoch an einem entsprechenden (mutmaßlichen) Kenntnisnahmewillen beider Kommunikationspartner fehlen. Jedenfalls hat sich diese Auffassung weder in der Literatur durchgesetzt²⁶ noch wurde sie bisher durch die Rechtsprechung aufgegriffen. Es ist daher davon auszugehen, dass Behörden und Gerichte auch zukünftig keine mutmaßliche Einwilligung des Kommunikationspartners beim Nachrichtenaustausch mit einer offensichtlich dienstlichen E-Mail-Adresse annehmen werden.

Die Kontrolle der Internetnutzung von Beschäftigten könnte hingegen grundsätzlich durch eine Einwilligung der Beschäftigten gerechtfertigt werden. Ausweislich von Art. 2 lit. f) E-Privacy-RL, dessen Verweis auf die mittlerweile aufgehobene Richtlinie 95/46/EG²⁷ nach Art. 94 Abs. 2 S. 1 DSGVO als Verweis auf die DSGVO gilt, unterliegt die Wirksamkeit der Einwilligung denselben Anforderungen wie nach der DSGVO. Nach Art. 4 Nr. 11 DSGVO ist eine wirksame Einwilligung „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“. Weitere Anforderungen an eine wirksame Einwilligung regeln Art. 6 Abs. 1 lit. a), Art. 7 und 8 DSGVO. Soweit sich daraus spezifischere Regelungen ergeben, sind die Vorgaben zur Einwilligung gem. § 26 Abs. 2 BDSG zudem vorrangig gegenüber der DSGVO anwendbar.

Aufgrund der Abhängigkeit des Beschäftigten gegenüber seinem Arbeitgeber ist im Beschäftigungsverhältnis insbesondere die „Freiwilligkeit“ einer Einwilligung problematisch. Nach Erwägungsgrund Nr. 43 zur DSGVO sollte eine Einwilligung nicht rechtfertigend wirken, „wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht [...] und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde“ (vgl. auch § 26 Abs. 2 S. 1 BDSG). Trotz ungleicher Machtverteilung zwischen Arbeitgeber und Beschäftigten ist daher stets im Einzelfall zu prüfen, ob sich die ungleiche Machtverteilung auf die Einwilligung auswirkt. Nach § 26 Abs. 2 S. 2 BDSG kann Freiwilligkeit trotz Machtdisparität im Beschäftigungsverhältnis insbesondere dann vorliegen, „wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.“

Eine Einwilligung ist vor diesem Hintergrund als freiwillig und damit – bei Einhaltung der weiteren Vorgaben des BDSG und der DSGVO – als wirksam anzusehen, wenn die Einwilligung in die Kontrolle der Internetnutzung lediglich eine Bedingung für die Erlaubnis der privaten Nutzung des Internetzugangs bildet²⁸ und der Arbeitgeber zudem gewährleistet, dass den Beschäftigten bei Ablehnung der Einwilligung keine Nachteile drohen.²⁹ Im Lichte der – noch aufgrund der alten Rechtslage veröffentlichten – Orientierungshilfe der Datenschutzkonferenz („DSK“) sollte zudem „auf erster Stufe“ eine Betriebsvereinbarung (vgl. Art. 88 Abs. 2 DSGVO, § 26 Abs. 4 BDSG) geschlossen werden, in welcher der Gegenstand der individuellen Einwilligungen umrissen wird.³⁰ Erst nachgelagert sollten auf dieser Grundlage die individuellen Einwilligungen der einzelnen Beschäftigten eingeholt werden, denen zuvor Gelegenheit zu geben ist, die Betriebsvereinbarung zur Kenntnis zu nehmen. Eine Betriebsvereinbarung selbst vermag eine Kenntnisnahme i. S. d. § 3 Abs. 3 TDDDG allerdings nicht zu rechtfertigen.³¹ Sie dient daher nur als Instrument der Ausübung von Mitbestimmungsrechten, kann die jeweils individuelle Einwilligung der Beschäftigten jedoch nicht ersetzen.³² Zusätzlich zu einer Betriebsvereinbarung müsste also stets eine (wirksame) individuelle Einwilligung des Beschäftigten eingeholt werden.

2. Verbot der privaten Nutzung

Sofern die private Nutzung betrieblicher E-Mail-Dienste verboten wird, ist der Arbeitgeber nach einhelliger Literatur- und Rechtsprechungsansicht insoweit nicht Normadressat nach § 3 Abs. 2 S. 1 TDDDG.³³ Im Falle einer verbotenen Privatnutzung wird der Arbeitgeber nicht zum „Anbieter“ von Telekommunikationsdiensten i. S. d. § 3 Nr. 1 TKG, sodass eine Adressatenstellung nach § 3 Abs. 2 S. 1 Nr. 2 TDDDG ausscheiden würde. Der E-Mail-Dienst wird nämlich nicht aufgrund eines Angebots des Arbeitgebers bereitgestellt, welches der

22 Dieckhoff/Assion, ZD 2023, 371, 376.

23 Assion, in: Assion (Hrsg.), TTDSG, 1. Aufl. 2022, § 3 TTDSG, Rn. 139 m. w. N.; Brink/Joos, in: Boecken/Düwell/Diller/Hanau (Fn. 12), § 26 BDSG Rn. 126; Klachin/Rauer, BB 2022, 1588, 1590; Nolte, in: Säcker/Körber (Fn. 1), § 3 TTDSG Rn. 43.

24 Dieckhoff/Assion, ZD 2023, 371, 376.

25 Härting, CR 2009, 581, 583.

26 Ausdrücklich ablehnend: Klachin/Rauer, BB 2022, 1588, 1590.

27 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 v. 23.11.1995 S. 31–50.

28 Brink/Joos, in: Boecken/Düwell/Diller/Hanau (Fn. 12), § 26 BDSG Rn. 126; Riesenhuber, in: BeckOK Datenschutzrecht, (Fn. 12), § 26 BDSG Rn. 171.

29 Dieckhoff/Assion, ZD 2023, 371, 376.

30 DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, Stand Januar 2016 („Orientierungshilfe“), S. 7, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf (zuletzt abgerufen am 15.3.2024).

31 Dieckhoff/Assion, ZD 2023, 371, 376; Hoppe/Braun, MMR 2010, 80, 84; Mengel, NZA 2017, 1494, 1496; a. A. Riesenhuber, in: BeckOK Datenschutzrecht, (Fn. 12), § 26 BDSG Rn. 171; Thüsing/Granetzny, in: Thüsing, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 4 Rn. 8 ff.

32 Maschmann, NZA-Beil. 2018, 115, 123.

33 DSK, Orientierungshilfe, S. 4; Byers, Mitarbeiterkontrollen, 2. Aufl. 2022, Rn. 66; Eckhardt, in: Schwartmann/Jaspers/Eckhardt (Fn. 1), § 3 Rn. 78, 106; Klachin/Rauer, BB 2022, 1588, 1590; Maschmann, in: Kühling/Buchner (Hrsg.), DS-GVO BDSG, 4. Aufl. 2024, § 26 BDSG Rn. 48a; Munz, in: Taeger/Gabel (Fn. 6), § 3 TTDSG Rn. 24; Riesenhuber, in: BeckOK Datenschutzrecht, (Fn. 12), § 26 BDSG Rn. 175; Thüsing, in: Thüsing (Fn. 31), § 3 Rn. 63 m. w. N.

Beschäftigte annehmen oder ablehnen kann. Vielmehr gründet die Dienstebereitstellung im Rahmen der Erfüllung von Arbeitsaufträgen letztlich auf dem arbeitgeberseitigen Weisungsrecht (§ 106 GewO), wonach der Beschäftigte zur (dienstlichen) Nutzung verpflichtet wird. Mithin gibt es gar kein Angebot, schon gar nicht bei einem expliziten Privatnutzungsverbot, welches aufgrund einer privatautonomen Willensbildung angenommen bzw. abgelehnt werden könnte. Jedenfalls werden E-Mail-Dienste bei verbotener Privatnutzung nicht „geschäftsmäßig“, insbesondere nicht gegenüber Dritten, angeboten (§ 3 Abs. 2 S. 1 Nr. 2 TDDDG) bzw. erbracht (§ 3 Abs. 2 S. 1 Nr. 4 TDDDG), da Beschäftigte bei verbotener Privatnutzung unstreitig – auch nach der Rechtsprechung – der Sphäre des Arbeitgebers zuzurechnen sind.³⁴ Eine Anwendbarkeit des § 3 TDDDG folgt auch nicht daraus, dass die private Nutzung des Internetzugangs, der eine Funktionsbedingung für die Verwendung der dienstlichen E-Mail darstellt, weiterhin erlaubt bleibt. E-Mail-Dienste sind nämlich selbst (interpersonelle) Telekommunikationsdienste i. S. d. § 3 Nr. 61 lit. b) TKG, für welche die Adressatenstellung nach § 3 TDDDG gesondert zu bestimmen ist.

Nach der vorzugswürdigen Literaturansicht steht eine Duldung der Privatnutzung auch nicht der Erlaubnis zur Privatnutzung gleich.³⁵ Eine Duldung hätte nämlich nur dann rechtliche Relevanz, wenn dies zu einer Änderung des Arbeitsvertrags hin zu einer Gestattung führen würde.³⁶ Eine dementsprechende Änderung des Arbeitsvertrags durch Duldung könnte nur über das Instrument der betrieblichen Übung erfolgen. Nach der ständigen Rechtsprechung des BAG bildet eine betriebliche Übung die regelmäßige Wiederholung bestimmter Verhaltensweisen des Arbeitgebers, aus denen der Arbeitnehmer schließen kann, ihm solle eine Leistung auf Dauer gewährt werden, weshalb er diesen Anspruch auch erhält.³⁷ Bei bloßen Annehmlichkeiten wird eine Rechtsbindung durch betriebliche Übung jedoch verneint.³⁸ Die private Nutzung betrieblicher E-Mail-Dienste dürfte als bloße Annehmlichkeit i. S. d. Rechtsprechung des BAG einzustufen sein, deren Duldung durch den Arbeitgeber nicht auf einen Rechtsbindungswillen für die Zukunft schließen lässt.³⁹

Dafür spricht auch die Rechtsprechung des LAG Nürnberg, wonach ein Anspruch auf bezahlte Raucherpausen aus betrieblicher Übung abzulehnen sei.⁴⁰ Aus der arbeitgeberseitigen Duldung entstehe nämlich noch kein Vertragsangebot, aus dem der Beschäftigte einen Anspruch aus betrieblicher Übung herleiten kann. Insbesondere fehlte es an der regelmäßigen Wiederholung bestimmter Verhaltensweisen, da die Beschäftigten Raucherpausen mit unterschiedlicher Häufigkeit in Anspruch genommen haben. Diese Fallkonstellation hat das LAG Nürnberg ausdrücklich mit der Duldung der privaten E-Mail- und Internetnutzung verglichen, wobei das Entstehen einer betrieblichen Übung ebenfalls abzulehnen sei.⁴¹

Zudem kann eine betriebliche Übung im Falle einer ausdrücklich entgegenstehenden Anweisung des Arbeitgebers nicht entstehen, da das Verhalten des Arbeitgebers dann weder aus der Sicht eines objektiven Empfängers (Vertragstheorie) als Angebot zur Vertragsänderung aufgefasst werden kann noch in diesem Fall ein schutzwürdiges Vertrauen des Arbeitnehmers besteht (Vertrauenstheorie).⁴² Das Entstehen einer betrieblichen Übung kann daher auch ausgeschlossen werden, indem der Arbeitgeber einen Vorbehalt äußert, wodurch zum Ausdruck kommt, dass der Arbeitgeber sich durch eine etwaige Duldung nicht binden will.⁴³

In der Literatur wird zwar auch die Ansicht vertreten, dass eine Duldung der Privatnutzung der Erlaubnis zur Privatnutzung gleichstehe, sodass der Anwendungsbereich des Fernmeldegeheimnisses trotz ausschließlicher Nutzungsbefugnis nur für dienstliche Zwecke

eröffnet wäre.⁴⁴ Diese Ansicht wird zumeist nicht näher begründet und hat in der arbeitsgerichtlichen Rechtsprechung bisher keine Berücksichtigung gefunden. In Ermangelung einer BAG-Grundsatzentscheidung besteht zwar das Risiko, dass ein Arbeitsgericht das Vorliegen einer betrieblichen Übung bei geduldeter Privatnutzung bejaht und der Arbeitgeber daher in den Anwendungsbereich des § 3 TDDDG fällt. Im Lichte der Rechtsprechung des BAG zur betrieblichen Übung sprechen allerdings sehr überzeugende Argumente gegen das Entstehen einer solchen betrieblichen Übung, sodass mit der wohl herrschenden Auffassung davon auszugehen ist, dass eine Duldung der Privatnutzung nicht einer Erlaubnis zur Privatnutzung gleichkommt. Jedenfalls ließe sich das Entstehen einer betrieblichen Übung verhindern, indem der Arbeitgeber die private Nutzung betrieblicher E-Mail-Dienste ausdrücklich verbietet und sich hinsichtlich einer etwaigen Duldung der privaten Nutzung betrieblicher E-Mail-Dienste unmissverständlich vorbehält, sich dadurch nicht binden zu wollen.

3. Organisatorische Trennung zwischen dienstlicher und privater E-Mail-Nutzung

In der Literatur wird zur Vermeidung eines Verstoßes gegen § 3 TDDDG mitunter vorgeschlagen, dass der Arbeitgeber die Beschäftigten anweisen solle, private E-Mails gesondert – also in einem dafür vorgesehenen Ordner im E-Mail-Account – zu speichern oder private E-Mails zu löschen.⁴⁵ Dann unterliege die Einsichtnahme in den Ordner mit dienstlichen E-Mails nicht dem Fernmeldegeheimnis, sondern lediglich den datenschutzrechtlichen Vorgaben nach der DSGVO und § 26 BDSG. Zur Begründung wird insbesondere auf die Rechtsprechung des EGMR⁴⁶ verwiesen, wonach eine Einsichtnahme in private Dateien auf einem dienstlichen Rechner durch den Arbeitgeber keine Verletzung des Art. 8 EMRK (Recht auf Achtung des Privat- und Familienlebens) darstelle, wenn der Beschäftigte eine zur dienstlichen Verwendung bestimmte Festplatte nicht eindeutig als „privat“ kennzeichnet. Auch in der arbeitsgerichtlichen Rechtsprechung ist anerkannt, dass der Arbeitgeber die Beschäftigten grundsätzlich anhalten kann, private E-Mails in einem separaten Ordner abzuspeichern oder nach Kenntnisnahme zu löschen.⁴⁷ Allerdings müssen diese Vorgaben selbst dem aus Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG abzuleitenden Verhältnismäßigkeitsgrundsatz entsprechen,

34 Aus der Rechtsprechung etwa: VG Karlsruhe, 27.5.2013 – 2 K 3249/12, NVwZ-RR 2013, 797, Rn. 60 ff.

35 *Beckschulze*, BB 2009, 2097; *Riesenhuber*, in: BeckOK Datenschutzrecht (Fn. 12), § 26 BDSG Rn. 170; *Schmidt*, BB 2009, 1297; *Thüsing*, in: Thüsing (Fn. 31), § 3 Rn. 65 ff.

36 *Thüsing*, in: Thüsing (Fn. 31), § 3 Rn. 65.

37 BAG, 26.3.1997 – 10 AZR 612/96, NZA 1997, 1007; 13.6.2007 – 5 AZR 849/06, NJOZ 2007, 3931.

38 BAG, 17.9.1970 – 5 AZR 539/69, NJW 1971, 163; 12.1.1994 – 5 AZR 41/93, NZA 1994, 694.

39 *Beckschulze*, DB 2007, 1526; *Thüsing*, in: Thüsing (Fn. 31), § 3 Rn. 70; *Waltermann*, NZA 2007, 529.

40 LAG Nürnberg, 5.11.2015 – 5 Sa 58/15, DB 2016, 600.

41 LAG Nürnberg, 5.11.2015 – 5 Sa 58/15, DB 2016, 600, Rn. 58.

42 *Thüsing*, in: Thüsing (Fn. 31), § 3 Rn. 68.

43 *Thüsing*, in: Thüsing (Fn. 31), § 3 Rn. 68.

44 *Mengel*, NZA 2017, 1494, 1496; vgl. *Barton*, NZA 2006, 460.

45 *Brink/Joos*, in: Boecken/Düwell/Diller/Hanau (Fn. 12), § 26 BDSG Rn. 126; *Maschmann*, in: Kühling/Buchner (Fn. 33), § 26 BDSG Rn. 51; *Riesenhuber*, in: BeckOK Datenschutzrecht (Fn. 12), § 26 BDSG Rn. 176.

46 EGMR (V. Sektion), 22.2.2018 – 588/13 – Libert/Frankreich.

47 LAG Hessen, 21.9.2018 – 10 Sa 601/18, NZA-RR 2019, 130, 4. Leitsatz.

also transparent und erforderlich sein, um die vom Arbeitgeber verfolgten Zwecke zu wahren.⁴⁸

Die (rechtmäßige) Anweisung, dienstliche und private E-Mails getrennt zu speichern oder private E-Mails zu löschen, würde indes nicht dazu führen, dass die Adressatenstellung des Arbeitgebers nach § 3 Abs. 3 S. 1 TDDDG wegfällt. Vielmehr ist der Arbeitgeber auf das pflichtgemäße Verhalten der Beschäftigten angewiesen, um im Rahmen der Kontrolle des Ordners mit dienstlichen E-Mails nicht auch private E-Mails zur Kenntnis zu nehmen und damit dem Fernmeldegeheimnis zu unterliegen.⁴⁹ Das LAG Hessen hat betont, dass bei arbeitnehmerseitigen Einschätzungen im Hinblick auf den privaten (bzw. nicht privaten) Charakter von E-Mails ein „erhebliches Fehlerrisiko“ bestehe,⁵⁰ sodass Arbeitgeber bei der Kontrolle der dienstlichen Korrespondenz weiterhin das Risiko eingehen würden, dem Fernmeldegeheimnis zu unterliegen.

Gleichwohl könnte eine solche Vorgehensweise als Alternative zu einem vollständigen Verbot der privaten Nutzung betrieblicher E-Mail-Dienste zumindest das Risiko mindern, bei der Einsicht in die dienstlichen E-Mails von Beschäftigten dem Fernmeldegeheimnis zu unterliegen. Zur Reduktion der Fehleranfälligkeit und zur Gewährleistung der Verhältnismäßigkeit der anschließenden Kontrolle sollte der Arbeitgeber stets möglichst konkret definieren, unter welchen Voraussetzungen E-Mails als „privat“ zu qualifizieren und daher gesondert zu speichern bzw. zu löschen sind. Zudem sollte der Arbeitgeber gegenüber den Beschäftigten ex ante transparent machen, in welchen Situationen eine Einsichtnahme beabsichtigt ist.⁵¹ Sicherheitshalber sollte die Anweisung zur Trennung von privaten und dienstlichen E-Mails bzw. zur Löschung privater E-Mails vor jeder beabsichtigten Kontrolle wiederholt werden, um zu vermeiden, dass der Arbeitnehmer nicht in wenigen Einzelfällen private E-Mails falsch speichert bzw. nicht löscht und damit die Kontrolle der dienstlichen E-Mails nach § 3 Abs. 3 S. 1 TDDDG mit der Unzulässigkeit infiziert. Zu empfehlen wäre zudem, dass der Arbeitgeber anschließend die Bestätigung des Beschäftigten einholt, dass sich keine privaten E-Mails in dem für dienstliche E-Mails vorgesehenen Ordner befinden.

III. Fazit

Angesichts der in Teil 1 dieses Beitrags dargelegten Rechtsunsicherheit hinsichtlich der Adressatenstellung des Arbeitgebers nach § 3 Abs. 2 S. 1 TDDDG ist Arbeitgebern zu empfehlen, die private Nutzung betrieblicher E-Mail-Dienste zu verbieten. Alternativ könnten Arbeitgeber ihre Beschäftigten anweisen, private E-Mails gesondert zu speichern oder private E-Mails zu löschen. Aufgrund der Fehleranfälligkeit arbeitnehmerseitiger Einschätzungen im Hinblick auf den privaten (bzw. nicht privaten) Charakter von E-Mails besteht hierbei indes weiterhin das Risiko, dass der Arbeitgeber bei der Einsichtnah-

me in die E-Mails von Beschäftigten dem Fernmeldegeheimnis unterliegt. Im Hinblick auf die Nutzung des Internetzugangs ist zu empfehlen, auf Grundlage einer Betriebsvereinbarung individuelle Einwilligungen der Beschäftigten einzuholen, die eine private Nutzung des Internetzugangs an die Bedingung knüpfen, dass der Arbeitgeber die Internetnutzung unter bestimmten, gegenüber dem Beschäftigten transparent zu machenden Voraussetzungen kontrollieren darf.

AUTOREN



Prof. Dr. Christian Koenig, LL.M., ist Direktor am Zentrum für Europäische Integrationsforschung und Mitglied der Rechts- und Staatswissenschaftlichen Fakultät der Universität Bonn. Seine Lehrtätigkeiten, Veröffentlichungen, Forschungsprojekte sowie rechtswissenschaftlichen Gutachtertätigkeiten konzentrieren sich schwerpunktmäßig auf das Recht des Europäischen Binnenmarktes, insbesondere das EU-Wettbewerbsrecht und das Regulierungsrecht (Telekommunikations-, Post- und Energierecht, EU-Beihilferecht, Glücksspielrecht, Gesundheits- und Arzneimittelrecht u. a.). In diesen Rechtsgebieten tritt Prof. Koenig auch vor dem Europäischen Gerichtshof und deutschen Verwaltungsgerichten als Prozessbevollmächtigter auf. Im Rahmen seiner Expertisen berät er regelmäßig Bundes- und Landesministerien sowie Kommunen.



Dr. Anton Veidt ist Wissenschaftlicher Mitarbeiter am Zentrum für Europäische Integrationsforschung (ZEI) der Universität Bonn und Rechtsreferendar am Landgericht Bonn. Sein Forschungsschwerpunkt ist das Telekommunikationsrecht. Daneben beschäftigt er sich mit dem Deutschen und Europäischen Verwaltungsrecht, dem Energiewirtschaftsrecht und dem EU-Wettbewerbsrecht.

48 LAG Hessen, 21.9.2018 – 10 Sa 601/18, NZA-RR 2019, 130, 4. Leitsatz.

49 *Vietmeyer/Byers*, MMR 2010, 807, 809.

50 LAG Hessen, 21.9.2018 – 10 Sa 601/18, NZA-RR 2019, 130, Rn. 91.

51 Vgl. LAG Hessen, 21.9.2018 – 10 Sa 601/18, NZA-RR 2019, 130, Rn. 87 ff.