IT-Arbeitsrecht

Kramer

4. Auflage 2026
ISBN 978-3-406-83314-4
C.H.BECK

Pflichtverletzung bereits bei einer abstrakten Möglichkeit der Rückverfolgung zu dem Internetanschluss des Arbeitgebers. Versendet ein Arbeitnehmer E-Mails mit der Signatur des Arbeitgebers über das geschäftliche E-Mail-Postfach, kann unmittelbar der Eindruck entstehen, der Arbeitgeber befasse sich mit Pornografie. Einer tatsächlichen Rückverfolgung bedarf es in diesen Fällen nicht. Weniger streng sah dies allerdings das LAG Rheinland-Pfalz. So verneinte das LAG Rheinland-Pfalz eine besonders schwere Pflichtverletzung bei der Verbreitung pornografischer **Inhalte an mehrere Arbeitskollegen** über das geschäftliche E-Mail-Postfach. Das LAG Rheinland-Pfalz begründete seine Entscheidung damit, dass der betroffene Arbeitnehmer durch sein Verhalten keine anderen Personen belästigt habe, da die betroffenen Kollegen diese E-Mails nicht als Belästigung werteten. Zudem verneinte das Gericht eine Rufschädigung des Arbeitgebers, da der Arbeitnehmer die Mails nur unternehmensintern versandt habe. Das Gericht kam im Rahmen der Verhältnismäßigkeitsprüfung zum Ergebnis, dass hier zunächst eine Abmahnung erforderlich gewesen wäre.[503] Zum gleichen Ergebnis kam das LAG Rheinland-Pfalz in einem Parallelverfahren, in dem der Arbeitnehmer die E-Mails mit pornografischem Inhalt auch an externe Dritte versandt hat. Hier zog das Gericht zwar eine Rufschädigung des Arbeitnehmers durch das Versenden dieser E-Mails an externe Dritte über das geschäftliche E-Mail-Postfach in Erwägung. Eine Rufschädigung wurde aber letztlich durch das LAG Rheinland-Pfalz abgelehnt, da die mit dem Arbeitnehmer befreundeten Empfänger die E-Mail nicht weitergeleitet haben. Zudem sei davon auszugehen, dass die mit dem Arbeitnehmer befreundeten Empfänger wissen, dass der Inhalt der E-Mail nicht auf den Arbeitgeber zurückgeht, sondern allein vom Mitarbeiter verfasst wurde.[504] Zum gleichen Urteil kam das LAG Köln in einer Entscheidung vom 18.7.2012. Das LAG Köln sah eine Abmahnung des Arbeitgebers für ausreichend an, da es weder zu einem finanziellen Schaden noch zu einer Rufschädigung des Arbeitnehmers gekommen ist.[505] Sowohl das LAG Rheinland-Pfalz als auch das LAG Köln stellen bei der Prüfung der **Wirksamkeit der Kündigung** darauf ab, ob es zu einer tatsächlichen Rufschädigung gekommen sei. Dies ist durchaus kritisch zu sehen. Nach der vorzugswürdigen Auffassung des BAG reicht bereits die abstrakte Möglichkeit einer Rufschädigung für einen Kündigungsgrund ohne vorherige Abmahnung aus. Es kann nicht sachgerecht sein, wenn man die Wirksamkeit einer Kündigung davon abhängig machen will, ob tatsächlich eine Rufschädigung eingetreten ist. Der Ausgang des Kündigungsschutzprozesses würde letztlich von dem Zufall abhängen, ob es zu einer Rufschädigung gekommen ist oder nicht. Weiter gibt es erhebliche Abgrenzungsschwierigkeiten, unter welche Voraussetzung eine Rufschädigung vorliegen soll. Trotz aller Kritik an der Instanzrechtsprechung birgt der Ausspruch einer Kündigung ohne vorherige Abmahnung dennoch Wirksamkeitsrisiken.

Verwirklicht der Mitarbeiter mit den versandten E-Mails allerdings eine Straftat, wird der **331**
Ausspruch einer Kündigung ohne vorherige Abmahnung möglich sein. Dies kann zB bei kinderpornografischen Schriften aber auch bei gewaltverherrlichenden oder volksverhetzenden Schriften der Fall sein. Zudem kommt der **Ausspruch einer Kündigung** auch dann in Betracht, wenn die versandten E-Mails Beleidigungen des Arbeitgebers oder anderer Arbeitnehmer beinhalten. Auch in diesen Fällen kann das Vertrauensverhältnis derart nachhaltig zerstört sein, dass dem Arbeitgeber eine Fortsetzung des Arbeitsverhältnisses unzumutbar ist.

bb) Schadensersatzansprüche des Arbeitgebers. Ist dem Arbeitgeber durch die un- **332**
erlaubte Privatnutzung des Arbeitnehmers ein finanzieller Schaden entstanden, kann er Schadensersatzansprüche gegen den Arbeitnehmer geltend machen. Fraglich ist dabei, inwieweit auch hier die **Grundsätze der Arbeitnehmerhaftung** zu berücksichtigen sind. Nach den Grundsätzen der Arbeitnehmerhaftung kann der Arbeitgeber den Arbeitnehmer

[503] LAG Rheinland-Pfalz 17.12.2008 – 7 Sa 317/08, BeckRS 2009, 56437.
[504] LAG Rheinland-Pfalz 10.12.2008 – 8 Sa 318/08, BeckRS 2009, 62444.
[505] LAG Köln 18.7.2012 – 9 Sa 209/12, BeckRS 2013, 66737.

nur bei Vorsatz oder grober Fahrlässigkeit uneingeschränkt in Haftung nehmen.[506] Hat der Arbeitgeber die private Nutzung ausdrücklich verboten, kommt eine Haftungsprivilegierung nach den Grundsätzen der Arbeitnehmerhaftung grundsätzlich nicht in Betracht. Die unerlaubte Privatnutzung ist in einem solchen Fall nie dienstlich veranlasst, so dass eine Haftungsprivilegierung ausscheidet. Es fehlt in einem solchen Fall an einer Schutzwürdigkeit des Arbeitnehmers, die dem Grundsatz der eingeschränkten Arbeitnehmerhaftung zugrunde liegt. Den Arbeitnehmer trifft daher grundsätzlich die volle Haftung für eingetretene Schäden.[507] Von einer beschränkten Haftung ist allenfalls dann auszugehen, wenn der Arbeitnehmer bei der Schadensverursachung lediglich fahrlässig gehandelt hat und nicht gegen die betrieblichen Sicherheitsrichtlinien verstoßen hat.[508]

Teile der Literatur wollen die Grundsätze der Arbeitnehmerhaftung auch dann einschränken, wenn die Privatnutzung grundsätzlich erlaubt ist. Diese Auffassung lehnt auch bei einer erlaubten Privatnutzung eine dienstliche Veranlassung der privaten Nutzung ab. Der Arbeitnehmer könne auch bei einer erlaubten Privatnutzung jederzeit frei entscheiden, ob er hiervon Gebrauch macht. Daher müsse er auch ein etwaiges Risiko einer Privatnutzung grundsätzlich voll tragen.[509] Es scheint daher in jedem Fall vertretbar, eine volle Haftung des Arbeitnehmers anzunehmen, wenn dieser im Rahmen einer erlaubten Privatnutzung unkalkulierbare Sicherheitsrisiken eingeht. Dies kann beispielsweise bei einem Download von Dateien aus E-Mail-Anhängen der Fall sein. (→ Rn. 439)

333 **cc) Rücknahme der Erlaubnis zur Privatnutzung.** Bei einem Missbrauch der erlaubten Privatnutzung kann diese grundsätzlich einseitig widerrufen werden. Eine **Sperrung des dienstlichen E-Mail-Accounts** – wie dies beim Internetzugang denkbar ist – kommt nicht in Betracht. Ohne geschäftliches E-Mail-Postfach wird der Arbeitnehmer seiner arbeitsvertraglichen Tätigkeit nicht mehr nachkommen können.

8. Private Nutzung betrieblicher Hard- und Software

a) Hard- und Softwarenutzung am Arbeitsplatz zu privaten Zwecken

334 Der Umgang mit datenverarbeitenden Programmen und den dazugehörigen Systemen gehört mittlerweile häufig zum betrieblichen Alltag. Dies hat zur Folge, dass die betriebliche Hard- und Software von der Belegschaft teilweise auch zu privaten Zwecken genutzt wird. Viele Arbeitnehmer speichern private Dateien wie Bild-, Audio- und Videodateien auf der Festplatte ihres Firmencomputers. In zahlreichen Fällen werden diese privaten Daten zuvor aus dem Internet heruntergeladen, sodass auch eine Gefahr der Vireninfizierung besteht. Von noch größerer Relevanz wird die **Privatnutzung** in Fällen sein, in denen der Mitarbeiter einen Laptop vom Unternehmen erhält. Dabei wird es meist auch zur Speicherung privater Dateien auf dem Laptop kommen. Immer öfter laden die Mitarbeiter zudem EDV-Programme zur Privatnutzung auf die Festplatte des dienstlichen Rechners. Aber auch Speichermedien des Arbeitgebers wie im Büro vorhandene USB-Sticks oder Cloud-Speicher werden häufig privat durch die Mitarbeiter genutzt. Auch sind Fälle denkbar, in denen die dienstlichen IT-Ressourcen von Mitarbeitern genutzt werden, um strafrechtlich relevante Handlungen zu begehen. Einer Entscheidung des BAG aus dem Jahr 2015 lag der Sachverhalt zugrunde, nach dem mehrere Arbeitnehmer dienstliche IT-Ressourcen verwendet hatten, um private „Raubkopien" herzustellen.[510] Solche Fälle können sich in kündigungsrechtlicher Sicht – wie nachfolgend dargestellt wird – auswirken.

[506] Küttner/Griese Haftung (Arbeitnehmer) Rn. 12 ff.
[507] Arnold/Günther/Günther/Böglmüller ArbR 4.0-HdB § 4 Rn. 154; Rudkowski/Stadelmann NZA 2024, 1665; Hoppe ArbRAktuell 2010, 388.
[508] Arnold/Günther/Günther/Böglmüller ArbR 4.0-HdB § 4 Rn. 154.
[509] Arnold/Günther/Günther/Böglmüller ArbR 4.0-HdB § 4 Rn. 159; Rudkowski/Stadelmann NZA 2024, 1665; aA Hoppe ArbRAktuell 2010, 388.
[510] BAG 6.7.2015 – 2 AZR 85/15, NZA 2016, 161.

b) Verbot der Speicherung privater Dateien

Das Unternehmen kann grundsätzlich frei darüber entscheiden, ob es seiner Belegschaft die Speicherung privater Dateien auf dem Dienst-PC erlaubt. Dies gilt auch dann, wenn die **Privatnutzung des dienstlichen Computers** grundsätzlich erlaubt ist. Durch die Speicherung privater Daten auf dem Firmencomputer – insbesondere, wenn die Daten zuvor aus dem Internet heruntergeladen wurden – kann das Betriebssystem des Unternehmens erheblichen Gefahren der Vireninfizierung ausgesetzt werden. Daneben kann die Speicherung großer Datenmengen auf betriebliche Datensysteme auch zu Beeinträchtigungen des betrieblichen Systems führen. Bei einer Speicherung von Daten mit pornografischem oder strafbarem Inhalt ist zudem eine Rufschädigung des Unternehmens denkbar, wenn diese Daten zurückverfolgt werden können. 335

Ein Verbot der Privatnutzung dienstlicher Hard- und Software kann unmittelbar im Arbeitsvertrag geregelt werden. Meist wird sich dieses Verbot aber aus einer gesonderten Richtlinie zur Nutzung der betrieblichen Kommunikationssysteme ergeben. In Unternehmen mit Betriebsrat sind derartige Verbote oftmals Inhalt einer Betriebsvereinbarung zur Nutzung der dienstlichen Kommunikationseinrichtungen. 336

c) Kontrollmöglichkeiten

Arbeitgeber können die Nutzung der dienstlichen Hard- und Software grundsätzlich kontrollieren. Eine etwaige erlaubte Privatnutzung hat keine Auswirkung auf den zulässigen Kontrollumfang. Selbst bei einer erlaubten Privatnutzung finden die Vorschriften des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz **(„TDDDG")** keine Anwendung. Das TDDDG regelt Bestimmungen zum Fernmeldegeheimnis und zum Datenschutz bei Telekommunikations- und bei Telemediendiensten. Das TDDDG regelt den Begriff „Telekommunikation" nicht. Mangels spezieller Begriffsbestimmung ist gem. § 2 Abs. 1 TDDDG das TKG maßgeblich. Telekommunikation ist gem. § 3 Nr. 59 TKG der technische Vorgang des **Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen** (zB E-Mail-Korrespondenz). Bei der Nutzung der betrieblichen Hard- und Software liegt damit kein Kommunikationsvorgang im Sinne des TKG vor. Folglich gilt der Arbeitgeber auch bei einer erlaubten Privatnutzung der Hard- und Software unter keinen Umständen als Dienstanbieter iSd § 3 TDDDG. Die Zulässigkeit der Kontrollen der Nutzung der betrieblichen Hard- und Software beurteilt sich daher ausschließlich nach den Vorschriften des BDSG und der DS-GVO. Die Rechtsmäßigkeit solcher Kontrollen richtet sich dann vornehmlich nach Art. 6 Abs. 1 DS-GVO oder Art. 9 Abs. 2 DS-GVO (→ Rn. 318). Daneben sind die Informations- und Transparenzpflichten aus Art. 13 ff. DS-GVO zu beachten. Danach ist der Betroffene nach Art. 13 Abs. 1 DS-GVO unter anderem über die Datenerhebung zum Zeitpunkt der Erhebung in Kenntnis zu setzen. 337

Der Arbeitgeber kann mit Kenntnis des Arbeitnehmers grundsätzlich auf alle gespeicherten dienstlichen Daten und Programme auf dem Firmencomputer zugreifen. Es gehört zu den Rechten des Arbeitgebers, die Arbeitsabläufe und Arbeitsergebnisse seiner Mitarbeiter zu kontrollieren. Ohne Wissen des Mitarbeiters kann der Arbeitgeber jedoch nicht schrankenlos auf die dienstlichen Daten zugreifen. Nach Art. 6 Abs. 1 lit. c und f DS-GVO ist der Zugriff auf Arbeitnehmerdaten zulässig, wenn der Arbeitgeber seine im Zusammenhang mit der Durchführung des Arbeitsverhältnisses bestehenden Rechte wahrnimmt. Die bisher entwickelten Rechtsgrundsätze hinsichtlich des Umgangs mit dienstlichen Daten und Programmen auf dem Firmencomputer gelten auch nach der DS-GVO weiter. Das Unternehmen kann daher zur Ausübung seines Direktionsrechts sowie zur Durchführung einer **verdachtsunabhängigen Leistungs- und Verhaltenskontrolle** stichprobenartig auf den PC und die darauf gespeicherten Daten seiner Mitarbeiter zugreifen. Diese stichprobenartigen Kontrollen sind regelmäßig über Art. 6 Abs. 1 lit. f DS-GVO gerecht- 338

fertigt. Eine lückenlose Kontrolle der **betrieblichen Datensysteme** ohne Wissen des Arbeitnehmers greift allerdings stark in dessen **Persönlichkeitsrechte** ein und ist unverhältnismäßig, wenn sie ohne jeden konkreten Anlass erfolgt. Daher wird sich eine verdeckte lückenlose Kontrolle der auf dem dienstlichen PC gespeicherten Daten meist nicht über Art. 6 Abs. 1 lit. f DS-GVO rechtfertigen lassen.[511] Besteht allerdings der Verdacht, dass der Arbeitnehmer Straftaten mit Hilfe der dienstlichen Hard- und Software begeht, ist zur Aufklärung dieses Verdachts ausnahmsweise auch eine lückenlose Kontrolle gem. § 26 Abs. 1 S. 2 BDSG gerechtfertigt. Allerdings muss bei der Durchführung entsprechender Kontrollen stets beachtet werden, dass ein Zugriff auf erkennbar private Dateien des Mitarbeiters nicht über Art. 6 Abs. 1 DS-GVO legitimiert werden kann. Befinden sich auf dem PC das Arbeitnehmers Dateien deren Bezeichnung auf einen ausschließlich privaten Inhalt schließen lässt, dürfen diese Dateien vom Arbeitgeber regelmäßig nicht geöffnet werden (zB „Privat", „Urlaub", „Kinder" etc.). Ist anhand der Bezeichnung einer Datei aber nicht eindeutig erkennbar, ob es sich hierbei um eine private oder dienstliche Datei handelt, wird man dem Unternehmen zugestehen müssen, diese Datei zu öffnen, um dem Verdacht einer unerlaubten Privatnutzung nachzugehen. Weiter ist zu berücksichtigen, dass eine derartige lückenlose heimliche Kontrolle den Verhältnismäßigkeitsgrundsatz beachten muss. Die verdeckte Überwachung ist daher zeitlich zu begrenzen. Erweist sich die Kontrolle als erfolgreich und der Mitarbeiter wird eines schweren Pflichtverstoßes überführt, ist die Kontrolle einzustellen. Ebenfalls ist die Überwachung zu beenden, wenn sich der Verdacht nicht aufklären lässt und die Kontrolle sich als erfolglos erweist.[512] Die zulässige Dauer einer heimlichen Kontrolle ist immer anhand des konkreten Einzelfalls zu beurteilen. Im Regelfall wird eine heimliche Kontrollmaßnahme nur für den Zeitraum von 2 bis 4 Wochen rechtmäßig durchgeführt werden können.

d) Pflichtverstöße

339 Eine unbefugte und zweckwidrige Nutzung der betrieblichen IT-Ressourcen stellt eine arbeitsvertragliche Pflichtverletzung dar, die mit einer Abmahnung oder einer Kündigung sanktioniert werden kann. Insbesondere in Fällen, in denen eine vermögensschädigende oder strafbare Verhaltensweise des Mitarbeiters vorliegt, wird eine Kündigung auch ohne vorherige Abmahnung wegen der vertrauensstörenden Folgen möglich sein. Dabei wird sogar der wirksame Ausspruch einer fristlosen Kündigung in Betracht kommen. Eine Pflichtverletzung ist in diesen Fällen auch bereits dann gegeben, wenn die Nutzung nicht in einem exzessiven Umfang erfolgt.[513] Insbesondere ist in diesem Zusammenhang zu berücksichtigen, dass das BAG eine **sozialadäquate Nutzung** als Milderungsgrund ablehnt. Nach Auffassung des BAG sei bereits nicht ersichtlich, woraus sich eine solche Sozialadäquanz ergebe.[514]

340 Bei einer unerlaubten Nutzung der betrieblichen Hard- und Software ist oftmals die Verdachtskündigung von Praxisrelevanz. Gekündigte Arbeitnehmer berufen sich im Rahmen eines Kündigungsschutzprozesses häufig darauf, ein anderer Arbeitskollege hätte auf ihren dienstlichen PC zugegriffen und die streitgegenständlichen Taten begangen. Der Arbeitgeber muss in einem solchen Fall für eine wirksame Tatkündigung darlegen und beweisen, dass kein anderer Mitarbeiter für die Begehung der Pflichtverletzung in Betracht kommt. Dies wird insbesondere dann schwer werden, wenn der PC des gekündigten Mitarbeiters frei zugänglich war und daher nicht von vornherein ausgeschlossen ist, dass auch ein anderer Mitarbeiter den PC hätte nutzen können. Hat der Arbeitgeber lediglich eine Tatkündigung ausgesprochen, besteht ein erhebliches Risiko, dass sich die Kündigung

[511] Byers Mitarbeiterkontrollen Rn. 70 ff.; Wellhöner/Byers BB 2009, 2311; Heldmann DB 2010, 1238.
[512] Byers Mitarbeiterkontrollen Rn. 71.
[513] BAG 16.7.2015 – 2 AZR 85/15, NZA 2016, 161; Kramer NZA 2016, 341.
[514] BAG 7.7.2005 – 2 AZR 581/04, NZA 2006, 98; Kramer NZA 2016, 341.

mangels Tatnachweis als unwirksam erweist. Daher sollten Arbeitgeber in der Regel neben einer Tatkündigung auch eine hilfsweise **Verdachtskündigung** aussprechen.[515]

Nachfolgend werden einige Pflichtverletzungen im Zusammenhang mit der Nutzung der dienstlichen Hard- und Software und die dazu ergangene Rechtsprechung genauer dargestellt. 341

aa) „Privatarchiv" auf der Festplatte des dienstlichen PC. Speichert der Arbeitnehmer private Dateien auf dem Firmencomputer, stellt dies eine Pflichtverletzung dar, sofern diese Nutzung dem Mitarbeiter nicht ausdrücklich gestattet war.[516] Sowohl die Rechtsprechung als auch die Literatur halten eine Abmahnung des Mitarbeiters dann für ausreichend, wenn dieser die Dateien von einem eigenen Datenträger auf seinen Dienst-PC überspielt hat. Handelt es sich bei den gespeicherten Dateien nicht um strafrechtlich relevantes oder sonstiges verwerfliches Material (zB pornografische oder extremistische Inhalte) und wurde auch die **Funktionsfähigkeit des Betriebssystems** des Unternehmens nicht beeinträchtigt, wiegt das Verhalten meist nicht derart schwer, um eine Kündigung ohne vorherige Abmahnung zu begründen. Das zwischen Arbeitgeber und Arbeitnehmer bestehende Vertrauensverhältnis wird durch ein solches einmaliges Verhalten nicht unwiederbringlich zerstört.[517] Anders kann die Sachlage sein, wenn ein Mitarbeiter aus der betrieblichen IT einen solchen Pflichtverstoß begeht. Von einem IT-Mitarbeiter wird besonders erwartet, mit gutem Beispiel voranzugehen und die betriebliche IT vor Beeinträchtigungen durch private Dateien zu schützen. Hier wiegt ein Pflichtverstoß regelmäßig schwerer. 342

Speichert ein Arbeitnehmer private Bilder oder sonstige private Dateien auf seinem Firmencomputer muss der Arbeitgeber dieses Verhalten vor Ausspruch einer Kündigung regelmäßig vorher abmahnen. Eine sofortige Kündigung kann allenfalls in wenigen Ausnahmefällen in Betracht kommen, wenn der Mitarbeiter zB pornografisches oder gewaltverherrlichendes Material auf seinem Firmencomputer gespeichert hat oder es zu **erheblichen Störungen des Betriebssystems** des Unternehmens gekommen ist. Eine vorherige Abmahnung kann auch dann entbehrlich sein, wenn der Mitarbeiter die gespeicherten Daten zuvor aus dem Internet heruntergeladen hat und die Daten einen strafrechtlich relevanten oder besonders verwerflichen Inhalt aufweisen (zB pornografische oder extremistische Inhalte). In diesen Fällen kommt erschwerend hinzu, dass mit dem unerlaubten Download aus dem Internet eine erhebliche Gefahr für die betriebliche EDV hinsichtlich einer Vireninfizierung einhergeht. Zudem kann dieser Vorgang auf den dienstlichen PC zurückverfolgt werden, was zu einer Rufschädigung des Unternehmens führen kann. Folglich kann in diesen Fällen sogar ein wichtiger Grund für eine **außerordentliche Kündigung** begründet sein.[518] Allerdings sind im Rahmen einer Interessenabwägung immer die Umstände des konkreten Einzelfalls zu berücksichtigen. So hielt das BAG in einer Entscheidung aus dem Jahr 2012 eine außerordentliche Kündigung eines leitenden Angestellten, der pornografische Dateien aus dem Internet heruntergeladen hat, für unwirksam. Nach den Feststellungen des BAG sei es weder zu einer Vireninfizierung noch zu einer Rufschädigung des Arbeitgebers gekommen. Auch waren die heruntergeladenen und gespeicherten Inhalte nicht strafbar. Der Mitarbeiter hätte aufgrund seiner langen beanstandungsfreien Betriebszugehörigkeit zunächst abgemahnt werden müssen.[519] 343

bb) Private Software auf dem dienstlichen PC. Deutlich strenger handhabt die Rechtsprechung hingegen Sachverhalte, bei denen Arbeitnehmer EDV-Programme auf dem 344

[515] Kramer NZA 2016, 341; → Rn. 367.
[516] BAG 24.3.2011 – 2 AZR 282/10, NZA 2011, 1029; LAG Hamm 30.9.2011 – 10 Sa 472/11, BeckRS 2012, 65682; Däubler Digitalisierung § 12 Rn. 17.
[517] BAG 24.3.2011 – 2 AZR 282/10, NZA 2011, 1029; LAG Hamm 30.9.2011 – 10 Sa 472/11, BeckRS 2012, 65682.
[518] BAG 27.4.2006 – 2 AZR 386/05, NZA 2006, 977; BAG 7.7.2005 – 2 AZR 581/04, NZA 2006, 98; Kramer NZA 2007, 1338; Besgen/Prinz/Fausten § 1 Rn. 126.
[519] BAG 19.4.2012 – 2 AZR 186/11.

Rechner des Arbeitgebers zu privaten Zwecken installieren, wenn dadurch erhebliche Gefahren für das Unternehmen entstehen können. Die Rechtsprechung führt hierzu aus, dass jedem Arbeitnehmer klar sein muss, dass das Unternehmen nicht damit einverstanden ist, wenn EDV-Programme auf den betrieblichen PC geladen werden.[520] Installiert ein Mitarbeiter heimliche eine **Anonymisierungssoftware** auf dem betrieblichen Rechner und klärt er den Arbeitgeber hierüber auch später nicht auf, kann der Arbeitgeber das Arbeitsverhältnis wirksam fristlos kündigen. Ein solches Verhalten läuft den Interessen des Arbeitgebers eklatant zuwider.[521] Lädt ein Mitarbeiter ein Programm auf seinen dienstlichen PC, um ein Portal zum Download von Musik und Filmen zu nutzen, rechtfertigt dies ebenfalls meist eine außerordentliche Kündigung. Das LAG Schleswig-Holstein stellt in einem solchen Fall klar, dass es durch das Verhalten des Arbeitnehmers zu einer erheblichen Gefahr einer Vireninfizierung gekommen sei. Erschwerend kam im vorliegenden Fall hinzu, dass der Arbeitnehmer sog. „Share-Dateien" genutzt hatte, sodass andere Nutzer des Portals auf den betrieblichen Rechner zugreifen konnten.[522] Das LAG Rheinland-Pfalz bejahte die Wirksamkeit einer außerordentlichen Kündigung in einem Fall, in dem der Arbeitnehmer zu privaten Zwecken Software aus dem Internet heruntergeladen und auf seinem Dienst-PC installierte hatte, obwohl ihm eine solche Nutzung der dienstlichen IT-Betriebsmittel ausdrücklich verboten war. Erschwerend kam in diesem Fall hinzu, dass durch die Installation der privaten Software eine Schadsoftware auf den dienstlichen PC gelangt war, die unter anderem unautorisierte Zugriffe von außerhalb des Unternehmensnetzwerkes zuließ.[523] Deutlich strengere Anforderungen an eine wirksame Kündigung stellte hingegen das LAG Nürnberg in jüngerer Zeit auf. Hier hatte der Kläger unerlaubterweise unter anderem die Software „Google Chrome Portable" auf seinem dienstlichen Rechner installiert. Das Gericht stellte zwar klar, dass das Installieren einer nicht freigegebenen Software an sich als außerordentlicher Kündigungsgrund geeignet ist, ließ die Kündigung dann aber im Rahmen der Interessenabwägung scheitern, da allein eine abstrakte Gefährdungslage für die IT-Sicherheit des Arbeitgebers nicht ausreiche, um eine außerordentliche Kündigung zu rechtfertigen. Eine konkrete Gefährdungslage sah das Gericht nicht als gegeben. Auch die ordentliche Kündigung scheiterte am Erfordernis einer vorherigen Abmahnung.[524]

345 **cc) Privatnutzung von Speichermedien.** Nach Ansicht des BAG kann eine zweckwidrige Verwendung von Speichermedien, die auf Kosten des Unternehmens bestellt wurden, grundsätzlich einen wichtigen Grund für eine fristlose Kündigung begründen.[525] Mit dieser Auffassung bleibt das BAG seiner bisherigen Rechtsprechung zu **vermögensschädigenden Pflichtverletzungen** treu. Eigentums- oder Vermögensdelikte zum Nachteil des Arbeitgebers sind nach Ansicht das BAG grundsätzlich geeignet, eine außerordentliche Kündigung zu stützen. Solche Delikte stellen – unabhängig von der konkreten Schadenshöhe – grundsätzlich einen wichtigen Grund für eine außerordentliche Kündigung dar. Dieser Auffassung liegt die Wertung zugrunde, dass auch der Diebstahl oder die Unterschlagung von Sachen mit nur geringem Wert zu einem massiven Vertrauensverlust führen. Ein **vertrauensvolles Verhältnis** zwischen Arbeitgeber und Arbeitnehmer ist als Grundlage eines jeden Arbeitsverhältnisses unerlässlich.[526] Allerdings kommt es bei einem Diebstahl geringwertiger Gegenstände entscheidend auf die Interessenabwägung unter Berücksichtigung der Umstände des konkreten Einzelfalls an. Insbesondere in Fällen, in

[520] BAG 12.1.2006 – 2 AZR 179/05, NZA 2006, 980; LAG Rheinland-Pfalz 12.11.2015 – 5 Sa 10/15, BeckRS 2016, 66182; LAG Schleswig-Holstein 6.5.2014 – 1 Sa 421/13, NZA-RR 2014, 417; OLG Celle 27.1.2010 – 9 U 38/09, NZA-RR 2010, 299.

[521] BAG 12.1.2006 – 2 AZR 179/05, NZA 2006, 980.

[522] LAG Schleswig-Holstein 6.5.2014 – 1 Sa 421/13, NZA-RR 2014, 417.

[523] LAG Rheinland-Pfalz 12.11.2015 – 5 Sa 10/15, BeckRS 2016, 66182.

[524] LAG Nürnberg 3.11.2020 – 7 Sa 99/20; BeckRS 2020, 46004.

[525] BAG 16.7.2015 – 2 AZR 85/15, NZA 2016, 161; Kramer NZA 2016, 341.

[526] Unter anderem BAG 31.7.2014 – 2 AZR 407/13, NZA 2015, 621; BAG 21.6.2012 – 2 AZR 153/11, NZA 2012, 1025; BAG 12.8.1999 – 2 AZR 923/98, NZA 2000, 421; BAG 17.5.1984 – 2 AZR 3/83, NZA 1985, 91; Kramer NZA 2016, 341.

denen ein Mitarbeiter seine Stellung im Unternehmen gezielt ausnutzt und sein Verhalten zudem versucht zu verheimlichen, fällt die Interessenabwägung meist zum **Nachteil des Arbeitnehmers** aus. In diesen Fällen wird eine vorherige Abmahnung aufgrund des schwerwiegenden Vertrauensbruchs entbehrlich sein.[527] Nutzt ein Arbeitnehmer beispielsweise seine Verantwortung für die Bestellung von CD- und DVD-Rohlingen aus, um auf Kosten des Unternehmens CD- und DVD-Rohlinge für seine privaten Zwecke zu bestellen, kann dies eine sofortige – sogar fristlose – Kündigung rechtfertigen.

dd) Anfertigung von Raubkopien. Ein deutlich schwerwiegenderer Pflichtverstoß des Arbeitnehmers liegt vor, wenn dieser IT-Ressourcen des Unternehmens nutzt, um Raubkopien anzufertigen. Nach Auffassung des BAG stellt es einen wichtigen Grund für eine fristlose Kündigung dar, wenn der Mitarbeiter den dienstlichen Rechner nutzt, um unter **Umgehung des Kopierschutzes** privat beschaffte Musik-CDs und Film-DVDs zu vervielfältigen. Ein derartiges Verhalten des Arbeitnehmers ist grundsätzlich geeignet, eine fristlose Kündigung zu rechtfertigen. Der Mitarbeiter kann nicht davon ausgehen, der Arbeitnehmer werde ein solches Verhalten dulden. Insbesondere kann dem Arbeitgeber nicht zugemutet werden, dass er die Begehung von Straftaten mittels der betrieblichen IT-Ressourcen hinnimmt.[528] Das BAG hält weiter fest, dass dies unabhängig davon gilt, ob das dem Arbeitnehmer vorgeworfene Verhalten eine Strafbarkeit begründet. Es kann zudem nicht darauf ankommen, ob der Mitarbeiter die Vervielfältigung während seiner Arbeitszeit vorgenommen hat.[529] Allerdings kann eine Strafbarkeit der Brenn- oder Kopiervorgänge oder eine Anfertigung während der Arbeitszeit das „Gewicht des Kündigungsgrundes" noch weiter verstärken. Erfüllt die Vervielfältigung einen Straftatbestand oder hat der Arbeitnehmer durch sein Verhalten einen **„Arbeitszeitbetrug"** begangen, wird der Arbeitgeber regelmäßig auch eine Kündigung ohne vorherige Abmahnung aussprechen können. Das Beendigungsinteresse des Arbeitgebers wird im Rahmen einer Interessenabwägung dem Interesse des Mitarbeiters am Fortbestand des Arbeitsverhältnisses überwiegen. Das Unternehmen kann das Arbeitsverhältnis des Mitarbeiters wirksam kündigen.[530] **346**

9. Posting in sozialen Netzwerken

Mit der Nutzung von allgemein zugänglichen sozialen Netzwerken wie Facebook, X, Snapchat und XING sowie von unternehmensbezogenen Networks wie Yammer oder Workplace from Meta[531] geht einher, dass die bei den Kommunikationsvorgängen anfallenden personenbezogenen Daten von einer mehr oder weniger großen **Öffentlichkeit** und somit regelmäßig auch vom Arbeitgeber eingesehen und verwertet werden können. Symptomatisch weisen beispielsweise Facebook und X ihre Nutzer ausdrücklich auf die Möglichkeit einer breiten Öffentlichkeit hin, die die von Usern eingestellten Informationen zur Kenntnis nehmen könnte.[532] Postings führen zu einer **Transparenz** persönlicher Äußerungen und Vorgänge, die kündigungsrechtliche Folgen haben können.[533] **347**

[527] BAG 31.7.2014 – 2 AZR 407/13, NZA 2015, 621; BAG 21.6.2012 – 2 AZR 153/11, NZA 2012, 1025.
[528] BAG 16.7.2015 – 2 AZR 85/15, NZA 2016, 161; Kramer NZA 2016, 341.
[529] BAG 16.7.2015 – 2 AZR 85/15, NZA 2016, 161; Kramer NZA 2016, 341.
[530] BAG 16.7.2015 – 2 AZR 85/15, NZA 2016, 161; Kramer NZA 2016, 341.
[531] Seit Oktober 2016 verfügbares (mobiles Smartphone-taugliches) unternehmensinternes soziales Netzwerk (vormals Facebook at Work) mit den wesentlichen Funktionen Gruppen, News Feed, Work Chat, Veranstaltungen, Suche, Live-Video. Weitere Business-Plattform zB Slack.
[532] Vgl. Facebook-Privatsphäre-Grundlagen: https://www.facebook.com/about/basics/manage-your-privacy/posts sowie Allgemeine Geschäftsbedingungen von X: https://X.com/de/tos.
[533] Kramer NZA 2024, 965; Fuhlrott/Oltmanns NZA 2016, 785; PersLex, Kündigung, außerordentliche – Facebook-Posting; PersLex, Kündigung, verhaltensbedingte – Facebook-Posting; Burr NZA-Beil. 2015, 114; Burr NZA-Beil. 2015, 205 ff.; Thüsing/Wurth/Vossen § 10 Rn. 4 ff.; Däubler Digitalisierung § 4 Rn. 31; Kramer/Rasche FA 2013, 330; Zintl/Naumann NJW-Spezial 2013, 306; Bauer/Günther NZA 2013, 67; Pawlak/Smeyer öAT 2013, 26; Kort NZA 2012, 1321; Göpfert/Wilke ArbRAktuell 2011, 159; Edenharter NZA 2017, 1300.

a) Formen von Postings

348 Postings können in Textform (auch in Verbindung mit Emoticons/Emojis[534]) und in Gestalt von Fotos oder Videos erfolgen.[535] Sie richten sich regelmäßig an eine Vielzahl von anderen Usern. Die Reichweite und somit der Adressatenkreis können vom Nutzer im Rahmen der von ihm vorzunehmenden **Einstellungen** weit (allgemeine Veröffentlichung mit weltweitem Zugriff) oder eng („Freunde" oder „Kontakte") begrenzt werden. Eine nicht mehr vom Urheber des Posts kontrollierbare weitere Verbreitung kann durch ein Weiterleiten bzw. Teilen oder Kommentieren („Liken") erfolgen. Dabei kann es sogar zur unkontrollierten Weiterleitung in andere Netzwerke kommen, wie bei einer Verbreitung von Fotos von Instagram in Facebook oder X. Textliche Postings sind – neben den sozialen Netzwerken – Gegenstand von Gruppenchats (wie bei einer WhatsApp-Gruppe oder einem gruppenbezogenen Work Chat im Rahmen von Workplace from Meta) und Blogs auf einer **weltweit abrufbaren** Website. Auch hier entsteht – je nach dem Umfang des Adressatenkreises – eine oftmals erhebliche Öffentlichkeitswirkung.

b) Verletzung einer arbeitsvertraglichen Pflicht

349 Gegenstand des arbeitsvertraglichen Synallagmas sind Hauptpflichten in Gestalt der Arbeits- und Entgeltzahlungspflicht sowie Nebenpflichten, zu denen die Pflicht nach § 241 Abs. 2 BGB zur **Rücksichtnahme** auf den jeweils anderen Vertragspartner zählt.[536] Auf Grund letzterer ist der Arbeitnehmer insbesondere zur Verschwiegenheit und zur Unterlassung von jedwedem ruf- und geschäftsschädigenden Verhalten[537] verpflichtet. Diese Nebenpflicht zur Loyalität endet für den Arbeitnehmer nicht mit dem Ende der Arbeitszeit oder dem Verlassen des Betriebsgeländes, sondern **gilt auch** während der Freizeit[538] und damit bei **Freizeitaktivitäten** wie Postings in sozialen Netzwerken[539]. Diese Ausstrahlung von arbeitsvertraglichen Pflichten auf das private Verhalten des Arbeitnehmers führt zu unterschiedlichen Lebenssachverhalten, die sich als sanktionsrelevante Pflichtverletzung darstellen.

c) Pflichtverletzungsrelevante Schnittstellen zum Arbeitsverhältnis

350 Postings können unter dem Gesichtspunkt der vertragswidrigen IT-Nutzung als solcher und wegen ihrer konkreten Inhalte Pflichtverletzungen begründen.

351 **aa) Privates Posting am Arbeitsplatz.** Internet- und E-Mail-Zugang am Arbeitsplatz, Handy und Notebook sind gängige Betriebsmittel, über deren Einsatz und Nutzung der Arbeitgeber auf Grund seiner **Eigentümerstellung** in Ausübung seines Weisungsrechts entscheidet.[540] Ein arbeitnehmerseitiges Recht auf Inanspruchnahme der betrieblichen IT-

---

[534] Vgl. hierzu LAG Baden-Württemberg 22.6.2016 – 4 Sa 5/16, BeckRS 2016, 71236: Beleidigung von Vorgesetzten mittels Emoticons/Emojis in der Kommentarfunktion eines Arbeitskollegen.

[535] Fuhlrott/Oltmanns NZA 2016, 785; Burr S. 113.

[536] BAG 24.8.2023 – 2 AZR 17/23, NZA 2023, 1595; vgl. hierzu Kramer NZA 2024, 965; BAG 18.12.2014 – 2 AZR 265/14, NZA 2015, 797; SächsLAG 27.2.2018 – 1 Sa 515/17, NZA-RR 2018, 244.

[537] HWK/Lembke Art. 88 DS-GVO Rn. 118.

[538] BAG 24.8.2023 – 2 AZR 17/23, NZA 2023, 1595; BAG 10.9.2009 – 2 AZR 257/08, NZA 2010, 220; hierzu Gragert ArbRAktuell 2010, 93; BAG 28.10.2010 – 2 AZR 293/09, NZA 2011, 112; hierzu Schrader ArbRAktuell 2011, 44; LAG Nds 21.3.2019 – 13 Sa 371/18, ArbRAktuell 2019, 338: Kein Verstoß gegen die Loyalitäts- und Rücksichtnahmepflicht liegt vor, wenn Medien eigeninitiativ über ein außerdienstliches Fehlverhalten des Arbeitnehmers unter Nennung des Namens des Arbeitgebers berichten, diese Berichterstattung dem betroffenen Arbeitnehmer jedoch nicht vorhersehbar war.

[539] BAG 24.8.2023 – 2 AZR 17/23, NZA 2023, 1595; ArbG Mannheim 19.2.2016 – 6 Ca 190/15, NZA-RR 2016, 254; SächsLAG 27.2.2018 – 1 Sa 515/17, NZA 2018, 244.

[540] Kramer NZA 2016, 341; Kramer NZA 2013, 311; Göpfert/Wilke ArbRAktuell 2011, 159; BAG 7.7.2005 – 2 AZR 581/04, NZA 2006, 98; hierzu Kramer NZA 2006, 194.