

Bundesarbeitsgericht
Zweiter Senat

Urteil vom 27. Juli 2017
- 2 AZR 681/16 -
ECLI:DE:BAG:2017:270717.U.2AZR681.16.0

I. Arbeitsgericht Herne

Urteil vom 14. Oktober 2015
- 6 Ca 1789/15 -

II. Landesarbeitsgericht Hamm

Urteil vom 17. Juni 2016
- 16 Sa 1711/15 -

Entscheidungsstichworte:

Überwachung mittels Keylogger - Verwertungsverbot

Leitsatz:

Der Einsatz eines Software-Keyloggers ist nicht nach § 32 Abs. 1 BDSG erlaubt, wenn kein auf den Arbeitnehmer bezogener, durch konkrete Tatsachen begründeter Verdacht einer Straftat oder anderen schwerwiegenden Pflichtverletzung besteht.

BUNDESARBEITSGERICHT



2 AZR 681/16
16 Sa 1711/15
Landesarbeitsgericht
Hamm

Im Namen des Volkes!

Verkündet am
27. Juli 2017

URTEIL

Radtke, Urkundsbeamtin
der Geschäftsstelle

In Sachen

Beklagte, Berufungsklägerin und Revisionsklägerin,

pp.

Kläger, Berufungsbeklagter und Revisionsbeklagter,

hat der Zweite Senat des Bundesarbeitsgerichts aufgrund der mündlichen Verhandlung vom 27. Juli 2017 durch den Vorsitzenden Richter am Bundesarbeitsgericht Prof. Dr. Koch, die Richterin am Bundesarbeitsgericht Berger, den Richter am Bundesarbeitsgericht Dr. Niemann sowie die ehrenamtlichen Richter Löllgen und Dr. Niebler für Recht erkannt:

Die Revision der Beklagten gegen das Urteil des Landesarbeitsgerichts Hamm vom 17. Juni 2016 - 16 Sa 1711/15 - wird auf ihre Kosten zurückgewiesen.

Von Rechts wegen!

Tatbestand

Die Parteien streiten über die Wirksamkeit einer außerordentlichen, 1
hilfsweise ordentlichen Kündigung.

Der Kläger war bei der Beklagten, die in ihrem Betrieb regelmäßig mehr 2
als zehn Arbeitnehmer beschäftigt, seit Juli 2011 als Webentwickler tätig. Zu
Beginn des Arbeitsverhältnisses verpflichtete er sich schriftlich, Hard- und Soft-
ware aus Gründen der informationstechnischen Sicherheit ausschließlich zur
Erfüllung der vereinbarten Aufgaben zu nutzen.

Im Zusammenhang mit der Anbindung eines neuen Netzwerks richtete 3
die Beklagte am 19. April 2015 (Sonntag) eine E-Mail folgenden Inhalts an ihre
Mitarbeiter:

„Hallo liebes (...) Team,

es ist soweit, die Telekom hat es endlich geschafft, uns
einen schnellen Internet Anschluss bereitzustellen.

Dieses möchte ich Euch natürlich nicht vorenthalten, aus
diesem Grund erhaltet Ihr freien Zugang zum WLAN.

Da bei Missbrauch, zum Beispiel Download von illegalen
Filmen, etc. der Betreiber zur Verantwortung gezogen
wird, muss der Traffic mitgelogged werden. Da ein rechtli-
cher Missbrauch natürlich dann auch auf denjenigen zu-
rückfallen soll, der verantwortlich dafür war.

Somit:

Hiermit informiere ich Euch offiziell, dass sämtlicher Inter-
net Traffic und die Benutzung der Systeme (der Beklag-
ten) mitgelogged und dauerhaft gespeichert wird. Solltet
Ihr damit nicht einverstanden sein, bitte ich Euch mir die-
ses innerhalb dieser Woche mitzuteilen.

...

Bitte benutzt dieses Netzwerk für alles wie Spotify, YouTube, etc. um unser Hauptnetzwerk zu entlasten.

...“

In einer Unterweisung am 20. April 2015 wandte sich kein Arbeitnehmer 4
gegen die Absicht der Beklagten, den „Internettraffic“ und die Benutzung ihrer
Systeme zur Verhinderung von Missbrauch des Internetzugangs „mitzuloggen“.

Die Beklagte installierte sodann auf dem Dienst-PC des Klägers eine 5
Software, die ab dem 21. April 2015 alle Tastatureingaben protokollierte und
regelmäßig Screenshots fertigte (Keylogger). Nachdem die Beklagte die vom
Keylogger erstellten Dateien ausgewertet hatte, fand am 4. Mai 2015 ein Ge-
spräch mit dem Kläger statt, in dem dieser einräumte, seinen Dienst-Rechner
während der Arbeitszeit privat genutzt zu haben. Er gab an, ein Computerspiel
programmiert und E-Mail-Verkehr für das Logistikunternehmen seines Vaters
abgewickelt zu haben. Auf die Programmierung des Spiels habe er am Arbeits-
platz in der Zeit von Januar bis April 2015 ca. drei Stunden verwendet. Für die
Firma seines Vaters sei er - vorwiegend in seiner Freizeit - höchstens etwa
zehn Minuten täglich tätig gewesen.

Die Beklagte kündigte das Arbeitsverhältnis des Klägers mit Schreiben 6
vom 19. Mai 2015 außerordentlich fristlos, hilfsweise ordentlich zum nächstzu-
lässigen Termin.

Hiergegen hat sich der Kläger fristgerecht mit der vorliegenden Klage 7
gewandt. Er hat behauptet, die privaten Verrichtungen meist in den Pausen und
in Zeiten erledigt zu haben, in denen er keines der ihm zugewiesenen Projekte
bearbeiten können. Die Beklagte habe durch den Einsatz eines Keylog-
gers „hinterrücks“ und ohne jeden Anlass massiv in sein Grundrecht auf infor-
mationelle Selbstbestimmung eingegriffen. In der E-Mail vom 19. April 2015
habe sie den Eindruck vermittelt, es sollten nur die Internetaktivitäten über das
neue Netzwerk kontrolliert werden.

Der Kläger hat sinngemäß beantragt,

8

1. festzustellen, dass das Arbeitsverhältnis der Parteien nicht durch die außerordentliche Kündigung der Beklagten vom 19. Mai 2015 aufgelöst worden ist;
2. festzustellen, dass das Arbeitsverhältnis der Parteien nicht durch die ordentliche Kündigung der Beklagten vom 19. Mai 2015 aufgelöst worden ist;
3. hilfsweise für den Fall des Obsiegens mit den Feststellungsanträgen die Beklagte zu verurteilen, ihn bis zum rechtskräftigen Abschluss des Kündigungsverfahrens als Webentwickler weiterzubeschäftigen.

Die Beklagte hat beantragt, die Klage abzuweisen. Aus den vom Keylogger erstellten Dateien ergebe sich, dass der Kläger am 21. April 2015 weit- 9
aus länger mit der Entwicklung des Computerspiels beschäftigt gewesen sei, als er eingeräumt habe. Die Einträge in den Logdateien widerlegten zudem seine Behauptung, höchstens zehn Minuten täglich mit Aufgaben für die Firma seines Vaters befasst gewesen zu sein. Ausweislich von Screenshots der auf seinem Dienst-PC befindlichen Ordner habe der Kläger für dessen Unternehmen 5.221 E-Mails empfangen und 5.835 Nachrichten versandt. Der Einsatz eines Keyloggers sei ohne Weiteres rechtmäßig gewesen, weil dem Kläger jede außerdienstliche Nutzung der IT-Systeme untersagt und damit seine Privatsphäre nicht betroffen gewesen sei. Im Übrigen habe gegen ihn der Verdacht des Arbeitszeitbetrugs bestanden. Am 9. Februar 2015 habe eine Arbeitnehmerin im Vorbeigehen gesehen, dass der Kläger eine „stark bebilderte“ Webseite hastig „weggeklickt“ habe. Weitere Mitarbeiter hätten mitgeteilt, der Kläger gehe während seiner Arbeitszeit in erheblichem Umfang privaten Aktivitäten nach. Zudem habe er sich zu einem sehr unproduktiven Mitarbeiter entwickelt.

Die Vorinstanzen haben der Klage stattgegeben. Mit ihrer Revision ver- 10
folgt die Beklagte ihren Klageabweisungsantrag weiter.

Entscheidungsgründe

Die Revision ist unbegründet. Das Landesarbeitsgericht hat die Berufung der Beklagten gegen das der Klage stattgebende Urteil des Arbeitsgerichts zu Recht zurückgewiesen. Die dem Senat allein zur Entscheidung anfallenden Feststellungsanträge sind begründet. Die Kündigungen der Beklagten vom 19. Mai 2015 sind unwirksam. Nach dem verfahrensrechtlich verwertbaren Sachvortrag der Beklagten fehlt es sowohl an einem wichtigen Grund für die außerordentliche Kündigung (§ 626 Abs. 1 BGB) als auch an einer sozialen Rechtfertigung für die unter Geltung des Kündigungsschutzgesetzes (§ 1 Abs. 1, § 23 Abs. 1) erklärte ordentliche Kündigung (§ 1 Abs. 2 KSchG). 11

I. Die Würdigung des Berufungsgerichts, die vom Kläger zugestandenen Sachverhalte rechtfertigten die beiden Kündigungen nicht, ist revisionsrechtlich nicht zu beanstanden. 12

1. Das Landesarbeitsgericht ist davon ausgegangen, der Kläger habe in der Zeit von Januar bis April 2015 an seinem Dienst-Rechner ca. drei Stunden auf die Programmierung des Computerspiels verwendet, dies aber überwiegend während der Pausen. Darüber hinaus hat das Berufungsgericht zugunsten der Beklagten unterstellt, der Kläger habe während der Arbeitszeit täglich zehn Minuten mit Tätigkeiten für die Firma seines Vaters verbracht. Damit habe er seine vertraglichen Pflichten in erheblicher Weise verletzt. Allerdings rechtfertigten die Pflichtverletzungen mangels vorheriger Abmahnung keine - außerordentliche oder ordentliche - Kündigung. Zwar habe der Kläger Hard- und Software der Beklagten entgegen der von ihm zu Beginn des Arbeitsverhältnisses unterzeichneten Erklärung für außerdienstliche Zwecke eingesetzt. Die „minutenweise“ Privatnutzung über den Zeitraum eines Jahres habe sich zu einer Gesamtdauer von 36,66 Stunden summiert. Jedoch sei schon der E-Mail der Beklagten vom 19. April 2015 zu entnehmen, dass tatsächlich kein absolutes Verbot der privaten Nutzung betrieblicher IT-Einrichtungen gelebt worden sei. Die unzulässige Privatnutzung habe auch nur einen minimalen Bruchteil 13

(2,08 vH) der täglichen Arbeitszeit des Klägers ausgemacht. Die Beklagte habe schließlich nicht substantiiert dargetan, dass seine Arbeitsleistung durch die außerdienstlichen Aktivitäten beeinträchtigt worden sei. Insgesamt liege keine derart schwere Pflichtverletzung vor, dass selbst deren erstmalige Hinnahme der Beklagten nach objektiven Maßstäben unzumutbar und damit offensichtlich - auch für den Kläger erkennbar - ausgeschlossen gewesen sei. Es gebe auch keine Anhaltspunkte dafür, dass sich der Kläger in Zukunft nach einer Abmahnung in gleicher oder ähnlicher Weise pflichtwidrig verhalten hätte.

2. Mit dieser Würdigung hat das Berufungsgericht, dem bei der Prüfung und Interessenabwägung im Rahmen von § 626 Abs. 1 BGB, § 1 Abs. 2 KSchG ein Beurteilungsspielraum zukommt, alle vernünftigerweise in Betracht zu ziehenden Umstände widerspruchsfrei und ohne Verstoß gegen Denkgesetze oder allgemeine Erfahrungssätze berücksichtigt. Entgegen der Annahme der Revisi- on hat das Landesarbeitsgericht den „auf lange Sicht“ - möglicherweise - verursachten Schaden in seine Überlegungen einbezogen, indem es die „vertane“ Arbeitszeit auf einen Zeitraum von einem Jahr hochgerechnet hat. Zu einem über die Vergütung der nicht bestimmungsgemäß verbrachten Arbeitszeit hinausgehenden Schaden hat die Beklagte nicht substantiiert vorgetragen. Soweit sie rügt, das Berufungsgericht habe übersehen, dass der Kläger nicht um Erlaubnis gefragt habe, obgleich er nur ausnahmsweise am Arbeitsplatz für die Firma seines Vaters habe tätig werden wollen und man insoweit eine „adäquate Lösung“ hätte finden können, bestätigt die Beklagte letztlich nur die Einschätzung des Berufungsgerichts, es sei zumindest nicht ausgeschlossen gewesen, dass sie eine geringfügige Privatnutzung ihrer Betriebsmittel während der Arbeitszeit hinnehmen würde.

14

II. Das Landesarbeitsgericht ist zu Recht davon ausgegangen, es müsse bei seiner Entscheidung den Sachvortrag der Beklagten unberücksichtigt lassen, den sie nur aufgrund des von ihr eingesetzten Keyloggers in das Verfahren einführen konnte. Die Verwertung dieses Vorbringens bei der Urteilsfindung wäre mit dem Recht des Klägers auf informationelle Selbstbestimmung (*Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG*) unvereinbar.

15

1. Ein Sachvortrags- oder Beweisverwertungsverbot wegen einer Verletzung des gemäß Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG geschützten allgemeinen Persönlichkeitsrechts einer Partei (*vgl. auch Art. 8 Abs. 1 EMRK*) kann sich im arbeitsgerichtlichen Verfahren aus der Notwendigkeit einer verfassungskonformen Auslegung des Prozessrechts - etwa von § 138 Abs. 3, § 286, § 331 Abs. 1 Satz 1 ZPO - ergeben. Wegen der nach Art. 1 Abs. 3 GG bestehenden Bindung an die insoweit maßgeblichen Grundrechte und der Verpflichtung zu einer rechtsstaatlichen Verfahrensgestaltung (*BVerfG 13. Februar 2007 - 1 BvR 421/05 - Rn. 93, BVerfGE 117, 202*) hat das Gericht zu prüfen, ob die Verwertung von heimlich beschafften persönlichen Daten und Erkenntnissen, die sich aus diesen Daten ergeben, mit dem allgemeinen Persönlichkeitsrecht des Betroffenen vereinbar ist (*BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 21; 20. Oktober 2016 - 2 AZR 395/15 - Rn. 18; 22. September 2016 - 2 AZR 848/15 - Rn. 23, BAGE 156, 370; BGH 15. Mai 2013 - XII ZB 107/08 - Rn. 21*). Das Grundrecht schützt neben der Privat- und Intimsphäre und seiner speziellen Ausprägung als Recht am eigenen Bild auch das Recht auf informationelle Selbstbestimmung, das die Befugnis garantiert, selbst über die Preisgabe und Verwendung persönlicher Daten zu befinden (*BVerfG 11. März 2008 - 1 BvR 2074/05 ua. - Rn. 67, BVerfGE 120, 378; 23. Februar 2007 - 1 BvR 2368/06 - Rn. 37, BVerfGK 10, 330; 15. Dezember 1983 - 1 BvR 209/83 ua. - zu C II 1 a der Gründe, BVerfGE 65, 1*).

16

2. Die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) über die Anforderungen an eine zulässige Datenverarbeitung konkretisieren und aktualisieren den Schutz des Rechts auf informationelle Selbstbestimmung und am eigenen Bild (§ 1 Abs. 1 BDSG). Sie regeln, in welchem Umfang im Anwendungsbereich des Gesetzes Eingriffe durch öffentliche oder nicht-öffentliche Stellen iSd. § 1 Abs. 2 BDSG in diese Rechtspositionen zulässig sind. Sie ordnen für sich genommen jedoch nicht an, dass unter ihrer Missachtung gewonnene Erkenntnisse oder Beweismittel bei der Feststellung des Tatbestands im arbeitsgerichtlichen Verfahren vom Gericht nicht berücksichtigt werden dürften (*BAG 20. Oktober 2016 - 2 AZR 395/15 - Rn. 17; 22. September 2016 - 2 AZR 848/15 - Rn. 22, BAGE 156, 370*). Ist allerdings die Datenverarbeitung gegen-

17

über dem betroffenen Arbeitnehmer nach den Vorschriften des BDSG zulässig, liegt insoweit keine Verletzung seines Rechts auf informationelle Selbstbestimmung und am eigenen Bild vor (*BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 22*).

3. In Anwendung dieser Grundsätze hat sich das Landesarbeitsgericht zu Recht gehindert gesehen, seiner Entscheidung den streitigen Sachvortrag der Beklagten über die Nutzung des Dienst-PC durch den Kläger am 21. und 23. April 2015 zugrunde zu legen. Hierdurch hätte das Landesarbeitsgericht eine durch die Beklagte begangene Grundrechtsverletzung perpetuiert und vertieft. Die Datenerhebung durch den Keylogger griff in das Recht des Klägers auf informationelle Selbstbestimmung ein. Der Kläger hat in die Maßnahme nicht eingewilligt. Der Eingriff war nicht aufgrund überwiegender Interessen der Beklagten nach § 32 Abs. 1 oder § 28 Abs. 1 BDSG gerechtfertigt. Ebenso lagen keine weiteren, über das schlichte Beweisinteresse der Beklagten hinausgehenden Aspekte vor, die gerade die in Frage stehende verdeckte Informationsbeschaffung durch einen Keylogger als gerechtfertigt erscheinen lassen könnten. 18

a) Die Aufzeichnung und Speicherung der Tastatureingaben am Dienst-PC des Klägers sowie das Fertigen von Screenshots durch den Keylogger stellten Datenerhebungen iSv. § 3 Abs. 1, Abs. 2 Satz 1, Abs. 3 und Abs. 7 BDSG dar. Die Beklagte hat sich dadurch Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten natürlichen Person, nämlich des Klägers als dem Nutzer des ihm zugeordneten Rechners, verschafft. 19

b) Der Kläger hat in die Datenerhebungen nicht dadurch gemäß § 4a BDSG eingewilligt, dass er der Ankündigung der Beklagten nicht widersprochen hat. Allein in der Tatsache, dass ein Arbeitnehmer einer ihm mitgeteilten Maßnahme nicht entgegen tritt, liegt keine Einverständniserklärung in die Informationserhebung. Das Unterlassen eines Protests kann nicht mit einer Einwilligung gleichgesetzt werden (*für die Videoüberwachung im öffentlichen Raum: vgl. BVerfG 23. Februar 2007 - 1 BvR 2368/06 - Rn. 40, BVerfGK 10, 330; BVerwG 25. Januar 2012 - 6 C 9/11 - Rn. 25, BVerwGE 141, 329*). Das gilt insbesondere, wenn - wie vorliegend - eine vom Arbeitgeber gesetzte „Widerspruchsfrist“ 20

noch nicht abgelaufen ist. Im Übrigen hatte die Beklagte dem Kläger nicht eröffnet, es sollten alle Tastatureingaben an seinem Dienst-PC „mitgeloggt“ und regelmäßig Screenshots gefertigt werden. Auch konnte der Kläger nicht erkennen, zu welchem Zweck er überwacht wurde. Die E-Mail der Beklagten vom 19. April 2015 legte den Schluss nahe, dass allein eine etwaige Internetaktivität über das neue Netzwerk und diese auch „nur“ hinsichtlich der abgerufenen Inhalte („*Download von illegalen Filmen*“, „*Betreiber zur Verantwortung gezogen*“, „*rechtlicher Missbrauch*“) kontrolliert werden sollte. Das Landesarbeitsgericht hat nicht festgestellt, in der mündlichen Unterweisung am 20. April 2015 seien anderslautende oder weiter gehende Aussagen getroffen worden. Dementsprechend ließ die Beklagte dem Kläger in ihrem Schreiben vom 5. Mai 2015 lediglich mitteilen, sie habe „im Zuge der Umstellung des Internetanschlusses zur Vermeidung eines etwaigen Missbrauchs die Onlineaktivitäten, die über diesen Anschluss laufen, kontrolliert und diese Kontrolle im Vorfeld sowohl per E-Mail als auch im Rahmen einer Ansprache an die gesamte Belegschaft angekündigt.“

c) Mit der ohne Einwilligung des Klägers erfolgten Datenerhebung durch den Keylogger hat die Beklagte in dessen durch Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG geschütztes Recht auf informationelle Selbstbestimmung eingegriffen. 21

aa) Für einen Eingriff in den Schutzbereich dieses Grundrechts ist es ohne Bedeutung, ob die Datenerhebung in verdeckter Form oder für den Arbeitnehmer erkennbar erfolgt. 22

(1) Bei dem verdeckten Einsatz eines Keyloggers wird der betroffene Arbeitnehmer in der Befugnis, selbst über die Preisgabe und Verwendung persönlicher Daten zu befinden, beschränkt, indem er zum Ziel einer nicht erkennbaren - systematischen - Beobachtung durch den Arbeitgeber gemacht wird und dadurch auf sich beziehbare Daten über sein Verhalten preisgibt, ohne die Überwachung oder gar den mit ihr verfolgten Verwendungszweck zu kennen (*für die automatisierte Erhebung öffentlich zugänglicher Informationen vgl. BVerfG 11. März 2008 - 1 BvR 2074/05 ua. - Rn. 67, BVerfGE 120, 378; für die* 23

Observation durch einen Detektiv außerhalb des Betriebsgeländes vgl. BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 24).

(2) Wird der Keylogger offen eingesetzt, liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor, weil die Aufzeichnung und Speicherung sämtlicher Tastatureingaben und bestimmter Bildschirminhalte der Vorbereitung möglicher belastender Maßnahmen (Ermahnung, Abmahnung, Kündigung) dienen und zugleich abschreckend wirken und insoweit das Verhalten des Betroffenen lenken soll (*für die offene Videoüberwachung im öffentlichen Raum: vgl. BVerfG 23. Februar 2007 - 1 BvR 2368/06 - Rn. 38, BVerfGK 10, 330; BVerwG 25. Januar 2012 - 6 C 9/11 - Rn. 24, BVerwGE 141, 329*).

bb) Der Eingriff in den Schutzbereich von Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG entfällt nicht dadurch, dass lediglich Verhaltensweisen am Arbeitsplatz erfasst werden. Das allgemeine Persönlichkeitsrecht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen desjenigen Rechnung, der sich in die (Betriebs-)Öffentlichkeit begibt (*für die Videoüberwachung vgl. BVerfG 23. Februar 2007 - 1 BvR 2368/06 - Rn. 39, BVerfGK 10, 330; BVerwG 25. Januar 2012 - 6 C 9/11 - Rn. 25, BVerwGE 141, 329; für die Observation durch einen Detektiv vgl. BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 24*).

cc) Ein Eingriff in das Recht auf informationelle Selbstbestimmung setzt nicht voraus, dass der betroffene Arbeitnehmer das informationstechnische System, über das Daten erhoben werden, als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das System selbstbestimmt verfüge. Diese Einschränkung betrifft allein das ebenfalls von Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG geschützte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, dem ggf. eine lückenfüllende Funktion zukommt (*BVerfG 27. Februar 2008 - 1 BvR 370/07 ua. - Rn. 201 und Rn. 206, BVerfGE 120, 274*).

d) Der Einsatz des Keyloggers war der Beklagten nicht nach § 32 Abs. 1 BDSG erlaubt. Es fehlte bereits an dem insoweit erforderlichen, durch konkrete Tatsachen begründeten Anfangsverdacht einer Straftat oder einer anderen schweren Pflichtverletzung. Eine Maßnahme, die hinsichtlich der Intensität des durch sie bewirkten Eingriffs in das allgemeine Persönlichkeitsrecht des Arbeitnehmers mit einer (verdeckten) Videoüberwachung vergleichbar ist, stellt sich als unverhältnismäßig dar, wenn sie aufgrund bloßer Mutmaßungen ergriffen wird. 27

aa) Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses ua. dann erhoben, verarbeitet oder genutzt werden, wenn dies für dessen Durchführung oder Beendigung erforderlich ist. Zur Durchführung gehört die Kontrolle, ob der Arbeitnehmer seinen Pflichten nachkommt (*Gola/Schomerus BDSG 12. Aufl. § 32 Rn. 16; Grimm JM 2016, 17, 19*), zur Beendigung iSd. Kündigungsvorbereitung (*dazu Grimm, aaO*) die Aufdeckung einer Pflichtverletzung, die die Kündigung des Arbeitsverhältnisses rechtfertigen kann (*BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 26*). Sofern nach § 32 Abs. 1 Satz 1 oder Satz 2 BDSG zulässig erhobene Daten den Verdacht einer solchen Pflichtverletzung begründen, dürfen sie für die Zwecke und unter den Voraussetzungen des § 32 Abs. 1 Satz 1 BDSG auch verarbeitet und genutzt werden (*BAG 29. Juni 2017 - 2 AZR 597/16 - aaO; 20. Oktober 2016 - 2 AZR 395/15 - Rn. 40; 22. September 2016 - 2 AZR 848/15 - Rn. 37 f., BAGE 156, 370*). Der Begriff der Beendigung umfasst dabei die Abwicklung eines Beschäftigungsverhältnisses (*BT-Drs. 16/13657 S. 21*). Der Arbeitgeber darf deshalb alle Daten speichern und verwenden, die er benötigt, um die ihm obliegende Darlegungs- und Beweislast in einem potentiellen Kündigungsschutzprozess zu erfüllen (*BAG 29. Juni 2017 - 2 AZR 597/16 - aaO; Stamer/Kuhnke in Plath BDSG § 32 Rn. 149; HWK/Lembke 7. Aufl. § 32 BDSG Rn. 15*). 28

bb) § 32 Abs. 1 Satz 2 BDSG erlaubt die Datenerhebung, -verarbeitung und -nutzung in Fällen, in denen - unabhängig von den in § 32 Abs. 1 Satz 1 BDSG näher bestimmten Zwecken - Anhaltspunkte für den Verdacht einer im Beschäf- 29

tigungsverhältnis begangenen Straftat bestehen. Der Gesetzgeber geht davon aus, dass Maßnahmen, die vom Arbeitgeber ergriffen werden, um strafbares Verhalten eines Arbeitnehmers aufzudecken, in der Regel besonders intensiv in dessen allgemeines Persönlichkeitsrecht eingreifen (*BT-Drs. 16/13657 S. 21*). Das ist insbesondere bei einer zu diesem Zweck erfolgenden (verdeckten) Überwachung von Beschäftigten der Fall, weshalb die - von der Gesetzesbegründung in Bezug genommenen - restriktiven Grundsätze der hierzu ergangenen Rechtsprechung in § 32 Abs. 1 Satz 2 BDSG gesondert kodifiziert wurden. Die Vorschrift soll hinsichtlich der Eingriffsintensität damit vergleichbare Maßnahmen erfassen (*BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 27; 12. Februar 2015 - 6 AZR 845/13 - Rn. 75, BAGE 151, 1*). Diese sollen allenfalls dann zulässig sein, wenn der durch konkrete Tatsachen begründete „einfache“ Verdacht (*Anfangsverdacht, BAG 20. Oktober 2016 - 2 AZR 395/15 - Rn. 25*) einer im Beschäftigungsverhältnis begangenen Straftat besteht.

cc) § 32 Abs. 1 Satz 2 BDSG entfaltet keine „Sperrwirkung“ dergestalt, dass eine anlassbezogene Datenerhebung durch den Arbeitgeber ausschließlich zur Aufdeckung von Straftaten zulässig wäre und sie nicht nach § 32 Abs. 1 Satz 1 BDSG zulässig sein könnte (*ausführlich BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 28 ff.*). Allerdings muss der mit einer Datenerhebung verbundene Eingriff in das allgemeine Persönlichkeitsrecht des Arbeitnehmers auch im Rahmen von § 32 Abs. 1 Satz 1 BDSG einer Abwägung der beiderseitigen Interessen nach dem - dort gleichfalls verankerten - Grundsatz der Verhältnismäßigkeit standhalten (*BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 32; 17. November 2016 - 2 AZR 730/15 - Rn. 30; 7. September 1995 - 8 AZR 828/93 - zu II 2 c bb der Gründe, BAGE 81, 15; 22. Oktober 1986 - 5 AZR 660/85 - zu B I 2 a der Gründe, BAGE 53, 226*). Dieser verlangt, dass der Eingriff geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten Zweck zu erreichen (*BAG 29. Juni 2017 - 2 AZR 597/16 - aaO; 17. November 2016 - 2 AZR 730/15 - aaO; 15. April 2014 - 1 ABR 2/13 (B) - Rn. 41, BAGE 148, 26; 29. Juni 2004 - 1 ABR 21/03 - zu B I 2 d der Gründe, BAGE 111, 173*). Es dürfen keine anderen, zur Zielerreichung gleich wirksamen und das Persönlichkeitsrecht der Arbeitnehmer weni-

30

ger einschränkenden Mittel zur Verfügung stehen. Die Verhältnismäßigkeit im engeren Sinne (Angemessenheit) ist gewahrt, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht (*BVerfG 4. April 2006 - 1 BvR 518/02 - zu B I 2 b dd der Gründe, BVerfGE 115, 320; BAG 29. Juni 2017 - 2 AZR 597/16 - aaO; 15. April 2014 - 1 ABR 2/13 (B) - aaO*). Die Datenerhebung, -verarbeitung oder -nutzung darf keine übermäßige Belastung für den Arbeitnehmer darstellen und muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen. Danach muss im Falle einer der (verdeckten) Videoüberwachung vergleichbar eingriffsintensiven Maßnahme, die auf § 32 Abs. 1 Satz 1 BDSG gestützt werden soll, der auf konkrete Tatsachen begründete Verdacht einer schwerwiegenden, jedoch nicht strafbaren Pflichtverletzung bestehen. Eine entsprechende verdeckte Ermittlung „ins Blaue hinein“, ob ein Arbeitnehmer sich pflichtwidrig verhält, ist auch nach § 32 Abs. 1 Satz 1 BDSG unzulässig (*BAG 29. Juni 2017 - 2 AZR 597/16 - aaO*). Sie ist, ohne dass es noch darauf ankäme, ob mildere, gleich effektive Mittel vorhanden waren, jedenfalls unangemessen (nicht verhältnismäßig im engeren Sinne).

dd) Aus Vorstehendem folgt zugleich, dass weniger intensiv in das allgemeine Persönlichkeitsrecht des Arbeitnehmers eingreifende Datenerhebungen nach § 32 Abs. 1 BDSG ohne Vorliegen eines durch Tatsachen begründeten Anfangsverdachts - zumal einer Straftat oder anderen schweren Pflichtverletzung - zulässig sein können. Das gilt vor allem für nach abstrakten Kriterien durchgeführte, keinen Arbeitnehmer besonders unter Verdacht stellende offene Überwachungsmaßnahmen, die der Verhinderung von Pflichtverletzungen dienen sollen. Solche präventiven Maßnahmen können sich schon aufgrund des Vorliegens einer abstrakten Gefahr als verhältnismäßig erweisen, wenn sie keinen solchen psychischen Anpassungsdruck erzeugen, dass die Betroffenen bei objektiver Betrachtung in ihrer Freiheit, ihr Handeln aus eigener Selbstbestimmung zu planen und zu gestalten, wesentlich gehemmt sind (*dazu BAG 25. April 2017 - 1 ABR 46/15 - Rn. 20 und Rn. 28 ff.*). Dementsprechend kann die vorübergehende Speicherung und stichprobenartige Kontrolle der Verlaufsdaten eines Internetbrowsers zulässig sein, um die Einhaltung eines vom Ar-

31

beitgeber aufgestellten kompletten Verbots oder doch einer Beschränkung der Privatnutzung von IT-Einrichtungen zu kontrollieren. Dabei werden lediglich die Adressen und Titel der aufgerufenen Seiten und der Zeitpunkt des Aufrufs protokolliert und damit nicht mehr Daten gespeichert, als benötigt werden, um einen möglichen inhaltlichen oder zeitlichen Missbrauch der Nutzungsrechte festzustellen (*LAG Berlin-Brandenburg 14. Januar 2016 - 5 Sa 657/15 - zu B I 4 a aa (8) (d) der Gründe*). Würden die gespeicherten Verlaufsdaten nicht zumindest stichprobenartig überprüft, könnten Zuwiderhandlungen gegen das Verbot oder die Beschränkung der Privatnutzung von IT-Einrichtungen des Arbeitgebers nicht geahndet werden und könnte die Datenerhebung ihre verhaltenslenkende Wirkung nicht entfalten.

ee) Mit diesem Inhalt steht § 32 Abs. 1 BDSG im Einklang mit den Vorgaben der eine umfassende Harmonisierung (*zur Begrifflichkeit EuGH 6. November 2003 - C-101/01 - [Lindqvist] Rn. 96 f., Slg. 2003, I-12971*) vorsehenden Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (*RL 95/46/EG - ABI. L 281 vom 23. November 1995 S. 31*). Einerseits wird mit dem aus dem Grundsatz der Verhältnismäßigkeit abgeleiteten Erfordernis des auf konkrete Tatsachen gestützten Anfangsverdachts einer Straftat oder anderen schweren Pflichtverletzung für besonders eingriffsintensive Maßnahmen nicht entgegen Art. 5 der Richtlinie ein zusätzlicher, die Datenerhebung erschwerender Grundsatz eingeführt oder durch eine zusätzliche Bedingung die Tragweite eines der in Art. 7 der Richtlinie vorgesehenen Grundsätze verändert (*dazu EuGH 19. Oktober 2016 - C-582/14 - [Breyer] Rn. 57 ff.; 24. November 2011 - C-468/10 und C-469/10 - [ASNEF] Rn. 33, 34 und 36*). Andererseits genügt der vom Senat herangezogene Verhältnismäßigkeitsgrundsatz dem durch die Richtlinie sowie Art. 7 der Charta der Grundrechte der Europäischen Union (*dazu EuGH 11. Dezember 2014 - C-212/13 - [Ryneš] Rn. 28*) und Art. 8 EMRK (*dazu EuGH 9. November 2010 - C-92/09 und C-93/09 - [Volker und Markus Schecke] Rn. 52, Slg. 2010, I-11063; BAG 19. Februar 2015 - 8 AZR 1007/13 - Rn. 20 f.*) garantierten Schutzniveau für die von einer Datenerhebung Betroffenen (*BAG*

32

29. Juni 2017 - 2 AZR 597/16 - Rn. 38; EGMR 5. Oktober 2010 - 420/07 - EuGRZ 2011, 471).

ff) Bei dem (zeitlich nicht begrenzten) verdeckten Einsatz eines Keyloggers an einem Dienst-PC handelt es sich um eine Datenerhebung, die hinsichtlich der Intensität des mit ihr verbundenen Eingriffs in das allgemeine Persönlichkeitsrecht des Betroffenen mit einer - verdeckten - Videoüberwachung am Arbeitsplatz vergleichbar ist. Zwar berührt der Einsatz eines Keyloggers grundsätzlich nicht das Recht am eigenen Bild, insbesondere ist er regelmäßig nicht geeignet, Verhaltensweisen optisch zu erfassen, die von dem Betroffenen als peinlich empfunden werden. Jedoch wird mit der Datenerhebung durch einen Keylogger massiv in das Recht des Betroffenen auf informationelle Selbstbestimmung eingegriffen. Es werden - für den Benutzer irreversibel - alle Eingaben über die Tastatur eines Computers einschließlich des Zeitpunkts der Eingabe sowie des zeitlichen Abstands zwischen zwei Eingaben erfasst und gespeichert. Die auf diese Weise gewonnenen Daten ermöglichen es, ein nahezu umfassendes und lückenloses Profil sowohl von der privaten als auch dienstlichen Nutzung durch den Betroffenen zu erstellen. Dabei werden nicht nur gespeicherte Endfassungen und ggf. Zwischenentwürfe bestimmter Dokumente sichtbar, sondern es lässt sich jeder Schritt der Arbeitsweise des Benutzers nachvollziehen. Darüber hinaus können besondere Arten personenbezogener Daten iSv. § 3 Abs. 9 BDSG oder - so im Streitfall - andere hochsensible Daten wie zB Benutzernamen, Passwörter für geschützte Bereiche, Kreditkartendaten, PIN-Nummern etc. protokolliert werden, ohne dass dies für die verfolgten Kontroll- und Überwachungszwecke erforderlich wäre. Ebenso hat der betroffene Arbeitnehmer weder Veranlassung noch die Möglichkeit, bestimmte Inhalte als privat oder gar höchstpersönlich zu kennzeichnen und damit ggf. dem Zugriff des Arbeitgebers zu entziehen. Dieser ohnehin schon weit überschießende Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen wird noch verstärkt, wenn - wie hier - regelmäßig Screenshots gefertigt werden.

33

gg) Die Würdigung des Berufungsgerichts, die Beklagte habe keine Tatsachen dargelegt, die vor dem Einsatz des Keyloggers den Anfangsverdacht einer

34

Straftat oder schweren Pflichtverletzung begründet hatten, ist revisionsrechtlich nicht zu beanstanden.

(1) Das Landesarbeitsgericht hat angenommen, die Beklagte habe lediglich einen Vorfall konkret beschrieben. Das von einer Arbeitnehmerin mitgeteilte einmalige hastige „Wegklicken“ einer „stark bebilderten“ Webseite sei aber nicht geeignet, den konkreten Verdacht einer exzessiven Privatnutzung des Dienst-PC zu begründen. Im Weiteren sei der Vortrag der Beklagten substanzlos geblieben. Das gelte zum einen für die einer Beweisaufnahme nicht zugängliche Behauptung, auch andere Mitarbeiter hätten angegeben, der Kläger gehe während seiner Arbeitszeit in erheblichem Umfang außerdienstlichen Aktivitäten nach. Zum anderen habe die Beklagte nicht substantiiert dargetan, dass die Leistungen des Klägers erheblich nachgelassen hätten. 35

(2) Diese Ausführungen lassen keinen materiellen Rechtsfehler erkennen. Die Revision zeigt auch keinen Fehler bei der Anwendung des Prozessrechts auf. 36

(a) Das Berufungsgericht hat es - stillschweigend - zu Recht als unmaßgeblich angesehen, dass die Beklagte die tatsächlichen Anhaltspunkte, die aus ihrer Sicht den Verdacht strafbaren Verhaltens des Klägers begründeten, nicht iSv. § 32 Abs. 1 Satz 2 BDSG dokumentiert hat. Ein solches Versäumnis führt weder zu einer Präklusion mit Vortrag zu den Verdachtsmomenten im Prozess noch begründet es für sich genommen die Unverwertbarkeit der aus der Maßnahme gewonnenen Erkenntnisse. Die Vorgabe, die Tatsachen zu dokumentieren, auf die sich ein Anfangsverdacht gründet, verfolgt den Zweck, dem hiervon erfassten Personenkreis die nachträgliche Rechtmäßigkeitskontrolle zu erleichtern. Aus ihr kann ein prozessuales Verwertungsverbot jedenfalls dann nicht abgeleitet werden, wenn der Arbeitgeber den Verdacht von Straftaten spätestens im Rechtsstreit durch konkrete Tatsachen untermauert und dadurch eine Rechtmäßigkeitskontrolle gesichert ist (*BAG 20. Oktober 2016 - 2 AZR 395/15 - Rn. 33*). 37

(b) Das Landesarbeitsgericht hat die Darlegungslast der Beklagten nicht überspannt. Auch bei vermeintlich kreativ tätigen Arbeitnehmern lässt sich anhand objektiver Tatsachen feststellen, inwieweit sie die ihnen übertragenen Aufgaben fristgerecht und entsprechend den inhaltlichen Vorgaben erledigt haben. Keinesfalls reicht es aus, sich im Rechtsstreit auf einen nicht näher begründeten Eindruck eines Vorgesetzten oder des Geschäftsführers zurückzuziehen. 38

(c) Die von der Beklagten erhobene Rüge, das Berufungsgericht habe sie gemäß § 139 ZPO darauf hinweisen müssen, dass ihr Vortrag zum Vorliegen eines durch konkrete Tatsachen begründeten Anfangsverdachts unzureichend sei, ist unzulässig. Die Revision legt nicht dar, warum die Vorinstanz einem gewissenhaften und kundigen Prozessbeteiligten in der konkreten Lage des Prozesses, insbesondere nach den Einlassungen des Klägers den von ihr vermissen Hinweis hätte erteilen müssen. Überdies fehlte es nach dem eigenen Vorbringen der Beklagten an der Entscheidungserheblichkeit einer Verletzung der richterlichen Hinweispflicht. Sie räumt selbst ein, es sei ihr nicht möglich gewesen, ihr Vorbringen zu ergänzen. 39

e) § 28 Abs. 1 BDSG schied als Erlaubnisnorm aus. Die Vorschrift findet im Beschäftigungsverhältnis nur Anwendung, wenn nicht - wie hier - die Zwecke des § 32 Abs. 1 BDSG betroffen sind (*BT-Drs. 16/13657 S. 20 f.*). Demgegenüber kann eine Datenerhebung, die weder der Aufdeckung von Straftaten iSd. § 32 Abs. 1 Satz 2 BDSG noch sonstigen Zwecken des Beschäftigungsverhältnisses iSv. § 32 Abs. 1 Satz 1 BDSG dient, „zur Wahrung berechtigter Interessen“ iSv. § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig sein (*BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 25; Gola/Schomerus BDSG 12. Aufl. § 32 Rn. 2, 45 f.*). 40

f) Es kann dahinstehen, ob Erkenntnisse, die der Arbeitgeber im Anwendungsbereich des § 32 Abs. 1 BDSG unter Verletzung des Rechts auf informationelle Selbstbestimmung gewonnen hat, ausnahmsweise im Rechtsstreit verwertet werden dürfen. Das könnte nur dann in Betracht kommen, wenn weitere, über das schlichte Beweisinteresse hinausgehende Aspekte hinzutreten und diese besonderen Umstände gerade die in Frage stehende Informationsbe- 41

schaffung als gerechtfertigt ausweisen (*BAG 22. September 2016 - 2 AZR 848/15 - Rn. 24, BAGE 156, 370; 20. Juni 2013 - 2 AZR 546/12 - Rn. 29, BAGE 145, 278*). Im Streitfall fehlt es schon an erstem. Ein Arbeitgeber, der - wie hier die Beklagte - eine Überwachungsmaßnahme „ins Blaue hinein“ veranlasst, befindet sich weder in einer Notwehr- oder notwehrrähnlichen Situation gemäß § 227 BGB bzw. § 32 StGB noch in einer Notstandslage iSv. § 34 StGB (*dazu BAG 13. Dezember 2007 - 2 AZR 537/06 - Rn. 36; BGH 15. Mai 2013 - XII ZB 107/08 - Rn. 23 f.*).

4. Das Landesarbeitsgericht hat zu Recht angenommen, die Kündigungen seien auch als Verdachtskündigungen unwirksam. Es musste den Sachvortrag der Beklagten, mit dem sie die durch den Keylogger gewonnenen Erkenntnisse in den Rechtsstreit eingeführt hat, auch bei der Würdigung außer Acht lassen, ob gegen den Kläger der dringende Verdacht eines Verhaltens bestand, das, wäre es erwiesen, eine außerordentliche, fristlose Kündigung gerechtfertigt hätte (*dazu, dass dies auch für eine ordentliche Verdachtskündigung erforderlich ist, BAG 18. Juni 2015 - 2 AZR 256/14 - Rn. 22*). 42

III. Die Sache ist nicht deshalb an das Berufungsgericht zurückzuverweisen, weil es Sachvortrag der Beklagten übergegangen hätte, der möglicherweise keinem Verwertungsverbot unterläge. Die dahingehende Rüge der Beklagten greift nicht durch. 43

1. Das Landesarbeitsgericht hat angenommen, die von der Beklagten in Bezug genommenen Screenshots der E-Mail-Ordner auf dem Dienst-Rechner des Klägers seien vom Keylogger gefertigt worden. Einen Tatbestandsberichtigungsantrag der Beklagten (§ 320 ZPO), mit dem sie geltend gemacht hatte, ihr ersinstanzlicher, auf Seite 10 des amtlichen Umdrucks des Berufungsurteils wiedergegebener Vortrag sei dahin gegangen, dass diese Bildschirmfotos bei einer vom Keylogger unabhängigen Einsichtnahme in das E-Mail-Programm auf dem Dienst-PC des Klägers gemacht worden seien, hat es als unbegründet zurückgewiesen. 44

2. Die darauf bezogene Verfahrensrüge ist unzulässig. 45
- a) Es kann dahinstehen, ob dies schon deshalb der Fall ist, weil die Beklagte sich mit dieser Rüge gegen die nicht mit einem Berichtigungsantrag angegriffene tatbestandliche Feststellung wendet, ihr *zweif*instanzlicher - möglicherweise „überholender“ - Vortrag sei dahin gegangen, dass die Screenshots vom Inhalt der E-Mail-Ordner auf dem Rechner des Klägers vom Keylogger „geschossen“ wurden (*Seite 12 und 22 des amtlichen Umdrucks*). Auch bedarf keiner Entscheidung, ob die Beklagte nach abgelehnter Tatbestandsberichtigung mit einer Verfahrensrüge nach § 551 Abs. 3 Satz 1 Nr. 2 Buchst. b ZPO erfolgreich allenfalls hätte geltend machen können, das Berufungsgericht habe ihr Vorbringen bewusst missverstanden und damit übergangen, oder es habe den Vortrag zumindest als missverständlich ansehen müssen und deshalb die angegriffene tatbestandliche Feststellung nicht ohne vorherigen Hinweis gemäß § 139 ZPO treffen dürfen. 46
- b) Jedenfalls legt die Beklagte die Erheblichkeit ihres „richtig“ verstandenen Vorbringens nach der maßgeblichen Begründungslinie der angefochtenen Entscheidung nicht dar. Sie zeigt nicht auf, dass das Landesarbeitsgericht anhand der bloßen Anzahl der in den E-Mail-Ordern befindlichen Nachrichten zu der Überzeugung gelangt wäre, der Kläger sei in einem exzessiven, eine vorherige Abmahnung entbehrlich machenden Umfang während seiner Arbeitszeit privaten Aktivitäten nachgegangen. Solchen Vortrags hätte es insbesondere deshalb bedurft, weil unstreitig zumindest ein Teil der E-Mails betreffend die Firma seines Vaters automatisch und ohne aktives Zutun des Klägers generiert worden ist. 47

Koch

Berger

Niemann

Niebler

Löllgen