Arbeitnehmerüberwachung und Compliance unter Berücksichtigung der Cybercrime-Konvention*

Von Prof. Dr. **Jörg Eisele**, Konstanz

I. Einführung

Die Arbeitnehmerüberwachung und ihre strafrechtlichen Grenzen sind erst in jüngerer Zeit in das Blickfeld der Strafrechtswissenschaft getreten. Anlass hierfür waren einige spektakuläre Fälle unzulässiger Überwachung von Beschäftigten durch große deutsche Unternehmen, die eine breite gesellschaftliche und rechtspolitische Diskussion ausgelöst haben. So wurde etwa bei der Deutschen Bahn AG in den Jahren 2006 und 2007 der gesamte E-Mail-Verkehr massiv überwacht und nach bestimmten Schlagworten gefiltert (Logfile-Filterung); der Inhalt der E-Mails soll jedoch nicht überprüft worden sein. In einem weiteren Fall wurde eine Massen-Mail der Gewerkschaft Deutscher Lokomotivführer (GDL), die einen Streikaufruf enthielt, den Beschäftigten nicht zugestellt. Die Deutsche Bahn führte zu ihrer Verteidigung an, dass diese E-Mail mit einer weiteren internen Massen-Mail zur Überlastung und zum Zusammenbruch des Mailservers geführt habe. Im Zuge des Wiederhochfahrens des Servers sei dann entschieden worden, die E-Mail zu löschen, weil das Verschicken über das E-Mail-System der Bahn rechtswidrig gewesen sei. Schließlich wurden auch im Zuge eines sog. Screenings ohne konkreten Verdacht verschiedene Daten – wie Anschriften, Telefonnummern und Bankverbindungen – einer großen Zahl von Mitarbeitern mit Daten Angehöriger von Lieferanten abgeglichen, um so Korruptionsfällen auf die Spur zu kommen. Die Deutsche Bahn hat für die in diesem Zusammenhang begangenen Ordnungswidrigkeiten einen Bußgeldbescheid des Berliner Beauftragten für Datenschutz und Informationsfreiheit v. 16.10.2009 mit einem Bußgeld in Höhe von mehr als 1,1 Millionen Euro akzeptiert.[1] Im Folgenden möchte ich exemplarisch untersuchen, ob in Fällen der Arbeitnehmerüberwachung neben Ordnungswidrigkeiten wegen Verstößen gegen das Bundesdatenschutzgesetz auch „klassische Straftatbestände" zur Anwendung gelangen können.

II. Ausgangspunkt: Datenschutz und Compliance

Die Arbeitnehmerüberwachung betrifft den in jüngerer Zeit vieldiskutieren Bereich der sog. Compliance.[2] Von diesem Blickwinkel aus greifen Überwachungsmaßnahmen nicht nur in die Rechte des Arbeitnehmers ein, sondern können zugleich schutzwürdigen Interessen des Arbeitgebers dienen. So werden in der Praxis Überwachungsmaßnahmen zur Verhinderung oder Aufdeckung von Straftaten der Arbeitnehmer – wie z.B. Diebstahl, Bestechung, Untreue oder Verrat von Betriebsgeheimnissen u.s.w. – durchgeführt. Soweit die mit datenschutzrechtlichen Fragen im Unternehmen befassten Personen – insbesondere ein Datenschutzbeauftragter oder Compliance Officer, aber auch Rechtsabteilungen, Innenrevisionen, Vorstände, Geschäftsführer und Aufsichtsräte[3] – untätig bleiben, steht aufgrund neuerer Rechtsprechung des Bundesgerichtshofs zumindest eine Strafbarkeit wegen Beihilfe durch Unterlassen zu der von dem Beschäftigten begangenen Tat im Raum.[4] Diesbezüglich muss man also sehen, dass die Arbeitnehmerüberwachung dazu dienen kann, Compliance-Anforderungen im Unternehmen umzusetzen. Andererseits ist zu beachten, dass Compliance-Maßnahmen ihrerseits überhaupt nur zulässig sind, soweit sie nicht gegen Regelungen verstoßen, die den Arbeitnehmer schützen.[5]

III. Überwachung des E-Mail-Verkehrs

Im Folgenden möchte ich im Wesentlichen auf Fragen der Überwachung des E-Mail-Verkehrs eingehen. Die Überwachung des E-Mail-Verkehrs, die technisch problemlos möglich ist, erlangt schon deshalb zentrale Bedeutung, weil heute große Teile der Kommunikation eines Unternehmens per E-Mail erfolgen. Ausgeklammert bleiben daher im Wesentlichen – im Einklang mit dem Thema unseres Rechtsdialogs – insbesondere die Überwachung des Briefverkehrs, das Abhören des gesprochenen Wortes sowie unbefugte Bildaufnahmen mithilfe von installierten Kameras.

1. Verletzung des Fernmeldegeheimnisses nach § 206 StGB

Im Fokus meiner Ausführungen steht zunächst § 206 StGB, der dem Schutz des Post- und Fernmeldegeheimnisses dient. In den Schutzbereich einbezogen sind nach § 206 Abs. 5 S. 2 StGB der Inhalt der Telekommunikation sowie ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Erfasst ist damit der Inhalt jeder Art individueller Nachrichtenübermittlung, also auch per E-Mail oder Internettelefonie; dies gilt insbesondere auch für Verbindungsdaten – wie Rufnummern,

---

* Der folgende Vortrag beruht auf dem Manuskript meiner inzwischen erschienenen Monografie Compliance und Datenschutzstrafrecht, Strafrechtliche Grenzen der Arbeitnehmerüberwachung, 2012.

[1] Vgl. dazu näher Pressemitteilung v. 23.9.2009 des Berliner Beauftragten für Datenschutz und Informationsfreiheit unter http://www.datenschutz-berlin.de/attachments/627/PE_DB_AG.pdf?1256283223 sowie https://www.datenschutzzentrum.de/presse/20080911-bw-lidl-bussgeldverfahren.pdf (Stand: 20.8.2011).

[2] BT-Drs. 17/4230, S. 1 und S. 12; *Forst*, DuD 2010, 160 (161); *Salvenmoser/Hauschka*, NJW 2010, 331.

[3] *Wybitul*, BB 2009, 2590 (2591).

[4] BGHSt 54, 44 (Leiter der Innenrevision einer Anstalt des öffentlichen Rechts). Dazu *Rotsch*, ZJS 2009, 712, und jüngst *ders.*, in: Schulz/Reinhart/Sahan (Hrsg.)., Festschrift für Imme Roxin, 2012, S. 485 m.w.N.

[5] *Forst*, DuD 2010, 160 (161); *Kamp/Körffer*, RDV 2010, 72 (75); *Rübenstahl*, NZG 2009, 1341 (1342); unklar *Behling*, BB 2010, 892 (893 f.). Zu diesem Spannungsverhältnis auch ArbG Berlin ZIP 2010, 1191, wonach eine verhaltensbedingte Kündigung wegen eines leitenden Mitarbeiters im Bereich „Compliance" wegen Überwachungsmaßnahmen zur Korruptionsbekämpfung nur in engen Grenzen zulässig ist.

IP-Adresse, Zeit, Ort oder Gesprächsdauer eines Telekommunikationsvorgangs.

a) Was die Tathandlungen anbelangt, so ist für den hier vorliegenden Zusammenhang die Weitergabe von Informationen nach Abs. 1 und das Unterdrücken von E-Mails nach Abs. 2 Nr. 1 von Belang. Solange der E-Mail-Verkehr nur überwacht, protokolliert, nach bestimmten Begriffen gefiltert oder auch eingesehen wird, ohne dass Informationen an Dritte weitergeleitet werden, ist der Tatbestand von vornherein zu verneinen.[6] Hier kommen regelmäßig nur Ordnungswidrigkeiten nach § 43 BDSG, im Falle des Handelns gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, auch eine Straftat nach § 44 BDSG in Betracht. Die Frage der Anwendbarkeit des Tatbestands erlangt neben Fällen des Nichtzustellens von E-Mails vor allem hinsichtlich der Weitergabe von Informationen an Externe – wie etwa Detektive oder Sicherheitsunternehmen –, die in die Überwachung eingeschaltet sind, sowie an Strafverfolgungsbehörden oder Gerichte in Kündigungsschutzprozessen Bedeutung.[7]

b) Als Täter des Delikts kommen aber nur Inhaber oder Beschäftigte eines Unternehmens in Betracht, das geschäftsmäßig Telekommunikationsdienste erbringt. Damit scheint der Anwendungsbereich auf den ersten Blick auf typische Telekommunikationsunternehmen und Internetprovider begrenzt zu sein. Die h.M. versteht diese Voraussetzung jedoch weiter und orientiert sich bei ihrer Auslegung an den einschlägigen Regelungen des Telekommunikationsgesetzes.[8] Unter dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten wird nach § 3 Nr. 10 TKG das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht verstanden. Damit wird das *Angebot für Dritte* zum entscheidenden Kriterium erhoben. In Folge dessen soll dann jeder Unternehmer, der Telekommunikationseinrichtungen für seine Mitarbeiter zur privaten Nutzung zur Verfügung stellt, vom Tatbestand erfasst sein.[9] Zur Begründung wird u.a. angeführt, dass es auf eine Gewinnerzielungsabsicht nicht ankomme und so das unentgeltliche Bereitstellen erfasst werde.[10] Zudem wird auf die Gesetzesbegründung zu § 88 Abs. 2 TKG verwiesen, wonach auch Nebenstellenanlagen in Betrieben und Behörden einbezogen sein sollten.[11] Letztlich kann man auch noch anführen, dass es für die Schutzwürdigkeit des Arbeitnehmers unerheblich ist, ob er seine privaten E-Mails über das Webmail-Programm des Arbeitgebers oder einen allgemeinen Internetprovider versendet. Diese Ansicht hat zur Folge, dass das TKG nur dann nicht anwendbar ist, wenn eine rein betriebliche Nutzung der Telekommunikation erfolgt, d.h. die Privatnutzung verboten ist, weil dann kein Angebot an Dritte vorliegt; dabei bleibt es auch, wenn der Arbeitnehmer ein solches Verbot des Arbeitgebers missachtet.[12] Dabei ist zu beachten, dass der Arbeitnehmer grundsätzlich kein Recht auf die Inanspruchnahme der Kommunikationsmittel zur privaten Nutzung hat, so dass der Arbeitgeber prinzipiell frei entscheiden kann.

c) Die Gegenansicht wendet ein, dass Zweck des Telekommunikationsgesetzes nach dessen § 1 sei, den Wettbewerb und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten, was jedoch auf den Arbeitgeber, der nur die Privatnutzung gestatte, nicht zutreffe.[13] Freilich überzeugt dieses Argument jedenfalls im Rahmen des § 206 StGB nicht, weil dieser Vorschrift ein anderer Schutzzweck zu Grunde liegt und Wettbewerbsaspekte von vornherein keine Rolle spielen.

Entscheidender ist aber, dass die Kontrollmöglichkeiten des Arbeitgebers stark eingeschränkt werden, wenn er als Telekommunikationsanbieter qualifiziert wird. Dann gelten für ihn nämlich auch bei der Kontrolle dienstlicher Tätigkeiten die strengen Vorgaben des TKG, wobei jedoch aufgrund seines Direktionsrechts im Ergebnis weitergehende Kontrollmaßnahmen als bei einer Privatnutzung möglich sind.[14] Würde der Arbeitgeber hingegen von vornherein die Privatnutzung von E-Mails verbieten, unterläge er insgesamt nur den weniger strengen Vorschriften des Bundesdatenschutzgesetzes. Auf weitere komplizierte Abgrenzungsfragen im Hinblick auf Telemedien soll hier nicht eingegangen werden. Entscheidende Strafbarkeitslücken wären mit einer Verneinung der Eigenschaft als Telekommunikationsanbieter und damit zugleich des Tatbestandes des § 206 StGB jedoch nicht verbunden. Da die Tathandlung des Unterdrückens auch von § 303a StGB erfasst wird, ginge es im Wesentlichen nur noch um die Mitteilung von Tatsachen durch den Arbeitgeber gegenüber Dritten. Dabei würde es sich freilich nicht um eine gravierende Strafbarkeitslücke handeln, da z.B. auch bei Schriftstü-

[6] Siehe *Altenburg/Reinersdorff/Leister*, MMR 2005, 135 (138); *Barton*, CR 2003, 839 (843); *Hoppe*, Private Nutzung betrieblicher Informations- und Kommunikationsmittel am Arbeitsplatz, 2010, S. 182; *Schuster*, ZIS 2010, 68 (72).

[7] Vgl. nur *Gola*, Datenschutz und Multimedia am Arbeitsplatz, 3. Auflage, 2010, Rn. 104; *Thüsing*, Arbeitnehmerdatenschutz und Compliance, Effektive Compliance im Spannungsfeld von reformiertem BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, 2010, Rn. 314.

[8] Vgl. § 88 Abs. 2 i.V.m. § 3 Nr. 6 TKG; dazu *Altvater*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 5, 12. Aufl. 2005, § 206 Rn. 11; *Altenhain*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 2003, § 206 Rn. 15 ff.

[9] *Heidrich/Tschoepe*, MMR 2004, 75 (76); *Altvater* (Fn. 8), § 206 Rn. 12; *Altenhain* (Fn. 8), § 206 Rn. 18; *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 3. Aufl. 2010, § 206 Rn. 10; offen gelassen von VG Frankfurt a.M. CR 2009, 125 (126), und VGH Hessen NJW 2009, 2470 (2471 f.).

[10] *Elschner*, Handbuch Multimedia-Recht, Teil 22.1 Rn. 80; *Kalf/Papsthart*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 188. Lfg., Stand: Januar 2012, § 85 Rn. 8.

[11] BT-Drs. 13/3609, S. 53.

[12] *Härting*, CR 2007, 311 (316); *Heidrich/Tschoepe*, MMR 2004, 75 (76); *Sassenberg/Lammer*, DuD 2008, 461 (463 f.); *Sauer*, K&R 2008, 399 (400); *Schuster*, ZIS 2010, 68 (71).

[13] So *Haussmann/Krets*, NZA 2005, 259 (260); *Thüsing* (Fn. 7), Rn. 240 f.

[14] *Thüsing* (Fn. 7), Rn. 237.

cken die Weitergabe des Inhalts nicht von der Strafvorschrift des § 202 StGB sanktioniert wird. Im Übrigen muss man sehen, dass auch die Weitergabe anderer (privater) Informationen durch den Arbeitgeber grundsätzlich nur als Ordnungswidrigkeit nach Datenschutzrecht sanktioniert werden kann.[15]

d) Angesichts der hier vertretenen Ansicht möchte ich nur noch zwei wichtige Aspekte aus der großen Anzahl der im Rahmen des Tatbestandes diskutierten Problemfelder hervorheben, die es aus dem Blickwinkel der h.M. zu beachten gilt.

aa) Zunächst muss man sehen, dass der Tatbestand beim Unterdrücken nach Abs. 2 Nr. 2 nur dem Unternehmen anvertraute Sendungen erfasst; der Schutz beginnt damit erst, wenn der versendende Rechner die Daten dem empfangenden Server des Unternehmens übermittelt hat.[16] Noch nicht anvertraut ist eine E-Mail daher, wenn das Unternehmen diese – z.B. bei Spam-Mails – von vornherein mittels sog. „Blacklists" aufgrund der IP- oder E-Mail-Adresse des Absenders ablehnt.[17] Andererseits fallen aber auch E-Mails, die vom Arbeitnehmer bereits vom Server des Unternehmens abgerufen und wie andere Dateien auf dem Rechner archiviert worden sind, nicht mehr in den tatbestandlichen Schutzbereich,[18] weil vom Fernmeldegeheimnis nur die Phase des Übertragungsvorgangs erfasst ist.[19] Hingegen werden nach h.M. E-Mails, die auf dem Server verbleiben und per Internetverbindung durch lokale Rechner, Notebooks, Mobiltelefone usw. abgerufen werden können, vom Schutzbereich umfasst.[20] Das Unternehmen erbringt demnach auch in dieser Phase weiterhin Telekommunikationsleistungen und wird nicht nur als Arbeitgeber tätig, der den Mitarbeitern IT-Einrichtungen zur Speicherung zur Verfügung stellt.[21] Auch die bloße Möglichkeit des Arbeitnehmers, darüber zu entscheiden, ob die E-Mail nach Kenntnisnahme im System verbleibt oder gelöscht wird, vermag daran nichts zu ändern, wenn diese weiterhin abrufbar bleibt.

bb) Hinsichtlich einer möglichen Rechtfertigung des Arbeitgebers ist die Regelung des § 88 Abs. 3 TKG zu beachten. Demnach ist es den Verpflichteten untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an Dritte wie Strafverfolgungsbehörden, ist nur zulässig, soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei *ausdrücklich* auf Telekommunikationsvorgänge bezieht. Daraus wird überwiegend gefolgert, dass auch für die strafrechtliche Rechtfertigung nur solche Vorschriften in Betracht kommen, die sich nach ihrem Wortlaut ausdrücklich auf Telekommunikationsvorgänge beziehen,[22] was vor allem bei Notwehr (§ 32 StGB) und Notstand (§ 34 StGB) nicht der Fall ist. Andere möchten die Notstandsvorschrift des § 34 StGB zumindest im Falle des Unterdrückens anwenden, weil § 88 Abs. 3 S. 3 TKG nur an die Verwendung der Kenntnisse anknüpft, das Unterdrücken aber unerwähnt lässt; dem durch Art. 10 GG geschützten Fernmeldegeheimnis soll dann im Rahmen der bei § 34 StGB vorzunehmenden Abwägung freilich entsprechendes Gewicht einzuräumen sein.[23] Für die restriktive Ansicht der h.M. spricht jedoch, dass sich der Gesetzgeber die Entscheidung darüber vorbehalten wollte, wann ein Eingriff in das besonders schützenswerte Fernmeldegeheimnis als erlaubt anzusehen ist,[24] so dass sich dies grundsätzlich nach den speziellen Datenschutzvorschriften der §§ 91 ff. TKG richten soll. Unberührt von dieser Sperre bleibt lediglich die Einwilligung, weil hier der Betroffene selbst über das Rechtsgut disponieren kann.[25] Werden virenverseuchte E-Mails in einem Unternehmen durch Filter zurückgehalten und dem Adressaten deshalb nicht zugestellt, bieten übrigens § 88 Abs. 3 S. 2 TKG und § 109 TKG hierfür eine spezielle Befugnis.[26] Anders ist hingegen bei Spam-Mails zu entscheiden, weil diese nicht per se zur Schädigung oder Störung geeignet sind und automatisiert in einen gesonderten Spam-Ordner, der dem Arbeitnehmer zugänglich ist, verschoben werden können, so dass ein Unterdrücken nicht erforderlich

[15] Speziell zu § 44 BDSG *Wybitul/Reuling*, CR 2010, 829 (830 ff.).

[16] OLG Karlsruhe MMR 2005, 178 (180); *Heidrich/Tschoepe*, MMR 2004, 75 (78).

[17] Zur technischen Seite *Heidrich*, CR 2009, 168.

[18] Siehe VG Frankfurt a.M. CR 2009, 125 f.; *Behling*, BB 2010, 892 (893).

[19] BVerfGE 115, 166 (183 f.), 120, 274 (307 f.); 124, 43 (54); *Hauschild*, NStZ 2005, 337 (340); *Welp*, NStZ 1994, 294 (295). Zu den einzelnen Phasen der E-Mail-Kommunikation *Brodowski*, JR 2009, 402.

[20] Nach *Hoppe/Braun*, MMR 2010, 80 (82) gilt dies auch für Sicherungskopien des E-Mail-Verkehrs.

[21] So aber VGH Hessen NJW 2009, 2470 (2471); vgl. auch die Vorinstanz VG Frankfurt a.M. CR 2009, 125.

[22] *Bock*, in: Beck'scher Onlinekommentar, Telekommunikationsgesetz, Stand: 3. Aufl. 2006, § 88 Rn. 28; *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 27. Aufl. 2011, § 206 Rn. 15; *Altenhain* (Fn. 8), § 206 Rn. 68; *Kargl* (Fn. 9), § 206 Rn. 47; *Lenckner/Eisele*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, § 206 Rn. 14; *Schuster*, ZIS 2010, 68 (75); *Hoyer*, in: Rudolphi u.a. (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, 56. Lfg., Stand: Mai 2003, § 206 Rn. 35; *Bosch*, in: Satzger/Schmitt/Widmaier (Hrsg.), Strafgesetzbuch, Kommentar, 2009, § 206 Rn.14; *Thüsing* (Fn. 7), Rn. 316; and. *Altvater* (Fn. 8), § 206 Rn. 80; krit. auch *Barton*, CR 2003, 839 (844).

[23] *Altvater* (Fn. 8), § 206 Rn. 80.

[24] BR-Drs. 147/97, S. 46; ferner BT-Drs. 13/ 3609, S. 53.

[25] *Bock* (Fn. 22), § 88 Rn. 56; *Eckhardt*, in: Spindler/Schuster, Recht der elektronischen Medien, 2008, § 88 Rn. 15; *Hanau/Hoeren*, Fundstelle, S. 56; *Lenckner/Eisele* (Fn. 22), § 206 Rn. 14; *Hoyer* (Fn. 22), § 206 Rn. 39; and. aber *Altenhain* (Fn. 8), § 206 Rn. 68.

[26] Vgl. auch *Gola* (Fn. 7), Rn. 110; *Heidrich/Tschoepe*, MMR 2004, 75 (78); *Altvater* (Fn. 8), § 206 Rn. 73; *Schmidl*, MMR 2005, 343 (344). Zum Erkennen, Eingrenzen und Beseitigen aktueller Störungen können auch nach § 100 Abs. 1 TKG Bestands- und Verkehrsdaten erhoben und verwendet werden.

ist.[27] Hier muss man sich ggf. mit Einwilligungslösungen behelfen.

2. Ausspähen von Daten nach § 202a StGB

a) Bedeutung erlangt in diesem Zusammenhang auch die Vorschrift des § 202a StGB. Diese wurde durch das StrafrechtsänderungsG zur Bekämpfung der Computerkriminalität modifiziert und dadurch den Vorgaben der jeweiligen Art. 2 des Rahmenbeschlusses der EU über Angriffe auf Informationssysteme und des Übereinkommens des Europarates über Computerkriminalität (Cybercrime-Konvention, Nr. 185) angepasst.[28] § 202a StGB betrifft dabei nicht nur den Telekommunikationsverkehr, sondern prinzipiell alle Daten, die auf dem Rechner des Arbeitnehmers gespeichert werden. Der Tatbestand setzt nunmehr voraus, dass der Täter sich oder einem anderen den Zugang zu Daten verschafft, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind.

b) Entscheidende Bedeutung erlangt damit die Frage, für wen die Daten bestimmt sind. Da geschütztes Rechtsgut die Verfügungsbefugnis des Berechtigten an dem gedanklichen Inhalt der Daten ist,[29] ist insoweit anerkannt, dass es auf die Eigentümerposition am Datenträger nicht ankommen kann.[30] Speichert der Arbeitnehmer private Daten, so erlangt er hierüber die alleinige Verfügungsbefugnis.[31] Dies gilt auch, wenn die Privatnutzung des Computers nicht gestattet war, weil das bloß weisungswidrige Verhalten im Innenverhältnis keinen Einfluss auf die Verfügungsbefugnis hat.[32] Das insoweit gegenüber § 206 StGB abweichende Ergebnis lässt sich mit dem unterschiedlichen Rechtsgut erklären. Dienstlich veranlasste Datenspeicherungen sind hingegen dem Arbeitgeber zuzurechnen, da solche aufgrund des Weisungsrechts und mit Veranlassung des Arbeitgebers vorgenommen werden.[33] Soweit es speziell um den E-Mail-Verkehr geht, sind Daten, die für den Empfänger auf einem E-Mail-Server zum Abruf bereitgehalten werden, für diesen bestimmt.[34] Daraus folgt wiederum, dass dienstliche E-Mails regelmäßig für den Arbeitgeber,[35] private E-Mails hingegen für den Arbeitnehmer bestimmt sind. Was die Abgrenzung anbelangt, kann es sich insbesondere um private Nachrichten handeln, wenn dem Arbeitnehmer für diesen Zweck eine gesonderte E-Mail-Adresse mit eigenem Passwort zur Verfügung steht. Umgekehrt wird zumeist Geschäftspost vorliegen, wenn die E-Mail an eine allgemeine dienstliche E-Mail-Adresse gerichtet ist. Wie beim Brief kann im Einzelfall etwa anderes gelten, wenn ein Vermerk persönlich, vertraulich oder privat angebracht ist. Soweit der Arbeitgeber private Nachrichten des Arbeitnehmers kontrolliert, kann er sich also unter den weiteren Voraussetzungen strafbar machen.

c) § 202a StGB erfordert weiterhin, dass der Täter sich den Zugang zu den Daten durch Überwindung einer Zugangssicherung verschafft. Zugangssicherungen können insbesondere Passworte oder Verschlüsselungen sein.[36] Eine besondere Sicherung und damit eine Strafbarkeit nach § 202a StGB ist daher etwa zu verneinen, wenn unverschlüsselte E-Mails im Unternehmen anhand bestimmter Schlagworte gefiltert werden.[37] Die Zugangsverschaffung muss zudem gerade unter Überwindung der Zugangssicherung erfolgen. Bei einem Passwort kommt es daher darauf an, ob dieses auch zugunsten des Arbeitnehmers gegenüber dem Arbeitgeber Zugangssicherung bildet oder lediglich den Zugriff von anderen Arbeitnehmern und außenstehenden Dritten verhindern soll.[38] Entscheidend ist damit die Zweckbestimmung, die mit dem Passwort verfolgt wird.[39] Teilt der Arbeitgeber den einzelnen Arbeitnehmern verschiedene Passwörter zu, behält sich aber selbst eine Zugriffsmöglichkeit auf die Verzeichnisse der Mitarbeiter vor, so ist der Tatbestand nicht verwirklicht.[40] Auch kann er im Bereich der dienstlichen E-Mails aufgrund seines Direktionsrechts grundsätzlich die Mitteilung des

[27] *Gola* (Fn. 7), Rn. 118; *Heidrich/Tschoepe*, MMR 2004, 75 (78); *Schmidl*, MMR 2005, 343 (344). Vgl. aber auch *Bock* (Fn. 22), § 88 Rn. 26, wonach eine Rechtfertigung bei Viren- und Spam-Mails in Betracht kommen soll.

[28] ABl. EU 2005 Nr. L 69, S. 67; zur Umsetzung BT-Drs. 16/3656, S. 1; BT-Drs. 16/5449, S. 1; BT-Drs. 16/5486, S. 1. Dazu *Borges/Stuckenberg/Wegener*, DuD 2007, 275.

[29] OLG Köln JMBl NW 2008, 238 (239); *Lackner/Kühl* (Fn. 22), § 202a Rn. 1; *Rengier*, Strafrecht, Besonderer Teil, Bd. 2, 13. Aufl. 2012, § 31 Rn. 24; *Lenckner*, in: Schönke/Schröder (Fn. 22), § 202a Rn. 1.

[30] *Lackner/Kühl* (Fn. 22), § 202a Rn. 3; *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Fn. 8), § 202a Rn. 26; *Graf*, in: Joecks/Miebach (Fn. 8), § 202a Rn. 17; *Möhrenschlager*, wistra 1986, 128 (140); *Weidemann*, in: Beck'scher Onlinekommentar, Strafgesetzbuch, Stand: 15.6.2012, § 202a Rn. 4.

[31] *Mattl*, Die Kontrolle der Internet- und E-Mail-Nutzung am Arbeitsplatz unter besonderer Berücksichtigung der Vorgaben des Telekommunikationsgesetzes, 2008, S. 161; *Weißgerber*, NZA 2003, 1005 (1008).

[32] *Schuster*, ZIS 2010, 68 (70); *Weißgerber*, NZA 2003, 1005 (1008). Vgl. aber *Gola* (Fn. 7), Rn. 54.

[33] *Graf* (Fn. 30), § 202a Rn. 17; *Schuster*, ZIS 2010, 68 (69); ferner *Hilgendorf*, JuS 1996, 890 (893) zu § 303a StGB.

[34] *Lenckner/Eisele* (Fn. 22), § 202a Rn. 6.

[35] Vgl. auch *Jofer/Wegerich*, K&R 2002, 235 (238).

[36] BT-Drs. 16/3656, S. 11; *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 176; *Graf* (Fn. 30), § 202a Rn. 38; *Kargl* (Fn. 9), § 202a Rn. 10; *Hoyer* (Fn. 22) § 202a Rn. 5; and. aber *Dornseif/Schumann/Klein*, DuD 2002, 226 (229 f.).

[37] Siehe auch *Spindler/Ernst*, CR 2004, 437 (439).

[38] LAG Köln NZA-RR 2004, 527 (528); *Barton*, CR 2003, 839 (842).

[39] *Barton*, CR 2003, 839 (842); *Hoppe* (Fn. 6), S. 178.

[40] LAG Köln NZA-RR 2004, 527 (528); in dem zugrunde liegenden Sachverhalt mussten alle Arbeitnehmer bei Einrichtung der Computeranlage ihr persönliches Passwort dem Netzwerkadministrator bekannt geben; *Schuster*, ZIS 2010, 68 (70).

Passworts an andere Mitarbeiter zur Urlaubs- oder Krankheitsvertretung verlangen.[41]

d) Was Rechtfertigungsfragen anbelangt, ist bei Telekommunikationsvorgängen wiederum die Sperre des § 88 Abs. 3 TKG zu berücksichtigen. Ansonsten kann § 32 StGB im Einzelfall zu einer Rechtfertigung führen, wenn private Dateien auf Servern oder Rechnern des Arbeitgebers abgelegt werden, so dass das System aufgrund der Menge der Daten oder aufgrund von Viren, Trojanern usw. beeinträchtigt wird.[42] Soweit mit dem Zugang Beweise für zivilrechtliche, arbeitsrechtliche oder strafrechtliche Verfahren gesammelt werden sollen, ist zu beachten, dass für eine Rechtfertigung kraft Notstand (§ 34 StGB) die bloße Beweisnot nicht genügt.[43]

3. Abfangen von Daten nach § 202b StGB

Die aufgrund der Vorgaben des Art. 3 der Cybercrime-Konvention eingefügte Vorschrift des § 202b StGB ist hingegen verwirklicht, wenn der Täter sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft. Für wen die Daten bestimmt sind und wer daher Verfügungsberechtigter im Verhältnis von Arbeitgeber und Arbeitnehmer ist, ist wie bei § 202a StGB zu bestimmen.

a) Anders als bei § 202a StGB müssen die Daten nicht besonders gesichert sein, so dass alle Formen der elektronischen Datenübermittlung durch den Arbeitnehmer erfasst werden. Zu erwähnen sind etwa E-Mail-Verkehr, Internettelefonie und auch Übertragungen innerhalb kleiner Netzwerke. Bei Var. 1 muss es sich um Daten in einem Übermittlungsvorgang handeln; nicht erfasst wird daher der Fall, dass der Arbeitgeber auf E-Mails zugreift, die bereits auf dem Rechner des Arbeitnehmers abgelegt sind. Anderes gilt nach h.M. jedoch auch hier, wenn diese noch auf dem Server zum Abruf durch den Adressaten bereitgehalten werden.[44]

b) Die Datenübermittlung muss ferner nichtöffentlich sein. Entscheidend ist, dass sich die Datenübermittlung nach Zielsetzung des Übermittelnden nicht an die Allgemeinheit, sondern an einen nur beschränkten Adressatenkreis richtet. Die Übermittlung ist daher nicht schon deshalb für die Öffentlichkeit bestimmt, weil keine Verschlüsselung benutzt wird.[45] Soweit sich die Kommunikation nur an Angehörige des Unternehmens richtet,[46] ist sie ebenfalls nichtöffentlich. Var. 2 schützt hingegen elektromagnetische Abstrahlungen einer Datenverarbeitungsanlage (insb. eines WLAN-Routers).[47] Da es hier nicht um einen Übermittlungsvorgang geht, ist auch die Abstrahlung bereits gespeicherter Daten geschützt.[48]

c) Schließlich muss sich der Täter anders als bei § 202a StGB nicht nur den Zugang zu den Daten, sondern die Daten selbst verschaffen. Ungeachtet dieser im Einzelnen umstrittenen Feinheiten soll bei E-Mails die bloße Kenntnisnahme und im Übrigen auch das Speichern und Kopieren von Daten genügen.[49]

4. Vorbereiten des Ausspähens und Abfangens von Daten nach § 202c StGB

§ 202c StGB, der auf Art. 6 Abs. 1 lit. a der Cybercrime-Konvention zurückgeht, stellt auch Vorbereitungshandlungen zu § 202a StGB und § 202b StGB unter Strafe. Tatgegenstände sind Passwörter und sonstige Sicherungscodes, die den Zugang zu Daten, d.h. ein Ausspähen nach § 202a oder ein Abfangen nach § 202b StGB ermöglichen (Nr. 1). Ferner sind Computerprogramme erfasst, deren Zweck die Begehung einer Tat nach §§ 202a, 202b StGB ist (Nr. 2). Strafbar nach dieser Vorschrift ist der Arbeitgeber etwa, wenn er Passwörter des Arbeitnehmers ausspäht, um so später Zugang zu den E-Mails zu erlangen.

5. Datenveränderung und Computersabotage nach §§ 303a, 303b StGB

a) Beim Abfangen von E-Mails und Eingreifen in Datenbestände ist ferner an eine Strafbarkeit nach § 303a StGB und auch § 303b StGB zu denken. Die Vorschriften wurden aufgrund von Art. 4 und Art. 5 der Cybercrime-Konvention sowie Art. 3 und 4 des Rahmenbeschlusses über Angriffe auf Informationssysteme modifiziert.[50] Für die Vorbereitung der §§ 303a, 303b StGB wird jeweils auf den eben angesprochenen § 202c StGB verwiesen. In unserem Zusammenhang erlangt insbesondere § 303a StGB Bedeutung, der das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen sowie Verändern von Daten sanktioniert.

b) Rechtswidrig ist eine solche Handlung aber nur, wenn sie sich auf Daten bezieht, über die der Täter nicht die alleinige Verfügungsbefugnis besitzt. Wie bei § 202a StGB kommt es nicht auf das Eigentum am Datenträger an, sondern darauf, dass das Verfügungsrecht eines anderen,[51] der ein unmittelba-

[41] *Barton*, CR 2003, 839 (842).
[42] Vgl. auch *Weißgerber*, NZA 2003, 1005 (1008).
[43] *Weißgerber*, NZA 2003, 1005 (1008).
[44] *Schumann*, NStZ 2007, 675 (677); *Hoyer* (Fn. 22), § 202b Rn. 7; *Weidemann* (Fn. 30), § 202b Rn. 5.
[45] *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 59. Aufl. 2012, § 202b Rn. 4; *Hilgendorf* (Fn. 30), § 202b Rn. 9; *Weidemann* (Fn. 30), § 202b Rn. 6. Siehe aber auch *Schumann*, NStZ 2007, 675 (677).
[46] Vgl. auch *Kargl* (Fn. 9), § 202b Rn. 5.
[47] Einbezogen sind also Fälle, in denen aus Abstrahlungen (keine Daten i.S.d. § 202a Abs. 2 StGB) Daten wiederhergestellt werden; vgl. BT-Drs. 16/3656, S. 11.
[48] *Hilgendorf* (Fn. 30), § 202b Rn. 12.
[49] Siehe BT-Drs. 16/3656, S. 11; *Kargl* (Fn. 9), § 202b Rn. 6; nach AG Kamen SchAZtg 2008, 229, wird auch das Umleiten und Aufnehmen des Chat-Verkehrs erfasst. Enger hingegen *Hoyer* (Fn. 22), § 202b Rn. 6, der ein Verschaffen in der Absicht, die mit Hilfe der Daten ausgedrückten Informationen in Erfahrung zu bringen, verlangt.
[50] ABl. Nr. L 69 v. 16.3.2005, S. 67.
[51] Siehe *Lackner/Kühl* (Fn. 22), § 303a Rn. 4; *Wieck-Noodt*, in: Joecks/Miebach (Fn. 8), § 303a Rn. 9; *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen (Fn. 9), § 303a Rn. 4; *Stree/*

res Interesse an dem Bestand bzw. der Unversehrtheit der Daten hat, verletzt wird. Insoweit ist auch hier zu klären, wem die Verfügungsberechtigung im Verhältnis zwischen Arbeitgeber und Arbeitnehmer zukommt. Entscheidende Bedeutung erlangt wiederum die Unterscheidung zwischen dienstlicher und privater Nutzung.

IV. Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes

1. Bezug zum Strafrecht

Ein Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes sieht spezifische Regelungen zur Arbeitnehmerüberwachung vor, die in das Bundesdatenschutzgesetz eingestellt werden sollen.[52] Solche Vorschriften hätten auch für den Bereich des Strafrechts Bedeutung. Zum ersten, weil Verstöße gegen diese Vorschriften Ordnungswidrigkeiten i.S.d. § 43 BDSG und ggf. auch Straftaten nach § 44 BDSG begründen würden. Zum zweiten, weil diese Vorschriften als Compliance-Maßnahmen Bedeutung erlangen sollen; so sieht etwa § 32d Abs. 3 des Vorschlags vor, dass zur Aufdeckung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen, insbesondere Straftaten nach §§ 266, 299, 331 bis 334 StGB, ein automatisierter Datenabgleich vorgenommen werden darf.[53] Zum dritten würden solche Regelungen aber auch auf Rechtswidrigkeitsebene zu beachten sein, da es wenig einleuchtend wäre, wenn ein datenschutzrechtlich zulässiges Verhalten strafbares Unrecht wäre.

2. Verhältnis zum TKG

Der Entwurf möchte am Verhältnis zwischen TKG und BDSG nichts ändern, so dass die Regelungen des BDSG mit der h.M. nur gelten sollen, wenn eine Privatnutzung nicht gestattet ist.[54] Bei gestatteter Privatnutzung richten sich die Maßnahmen dann weiter nach dem TKG. Entscheidend soll dabei die abstrakte Erlaubnis zur Privatnutzung und nicht die tatsächliche Nutzung sein.[55] Dies begegnet erneut Bedenken: Denn damit würden die geplanten Vorschriften, die detailliert die Arbeitnehmerüberwachung bei Telefon-, E-Mail- und Internetnutzung regeln, häufig nicht zur Anwendung gelangen, so dass nur die engen Überwachungsmöglichkeiten nach TKG in Betracht kommen, die jedoch nicht auf die Arbeitnehmerüberwachung zugeschnitten sind. Der Gesetzgeber würde daher dieses wichtige Problemfeld nur teilweise regeln. Im Ergebnis ist damit der Arbeitgeber, der seinen Mitarbeitern auch in deren Interesse die Privatnutzung gestattet, hinsichtlich der Wahrung seiner schutzwürdigen Interessen selbst bei der Kontrolle dienstlicher E-Mails stark eingeschränkt.

3. Exemplarisch: E-Mail-Kontrolle

a) Nach § 32i Abs. 3 des Vorschlags darf der Arbeitgeber Inhalte bei E-Mails erheben, verarbeiten und nutzen, soweit dies zur Gewährleistung des ordnungsgemäßen Betriebs von Telekommunikationsnetzen oder Telekommunikationsdiensten, einschließlich der Datensicherheit oder zu einer stichprobenartigen oder anlassbezogenen Leistungs- oder Verhaltenskontrolle erforderlich ist und keine Anhaltspunkte dafür bestehen, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt. Dies gilt auch, soweit es für den ordnungsgemäßen Dienst- oder Geschäftsbetrieb des Arbeitgebers in den Fällen einer Versetzung, Abordnung oder Abwesenheit (z.B. Urlaub) erforderlich ist.

b) Die Telekommunikation soll im Übrigen mit dem Empfang der übermittelten Signale – bei E-Mails mit Eingang auf dem „Arbeitsplatzcomputer" – abgeschlossen sein.[56] Dies überzeugt so allerdings nicht ohne weiteres, da E-Mails häufig auf dem Server des Arbeitgebers verbleiben.[57] Der Gesetzgeber jedenfalls hat dieses Problem in seiner Dimension vollständig verkannt. Der Arbeitgeber darf nach diesem Vorschlag erkennbar[58] private Daten und Inhalte nur erheben, verarbeiten und nutzen, wenn dies zur Durchführung des ordnungsgemäßen Dienst- oder Geschäftsbetriebes unerlässlich ist und er den Beschäftigten hierauf schriftlich hingewiesen hat. Die Begründung nennt den Fall, dass der Beschäftigte erkrankt ist und zur Bearbeitung dienstlicher E-Mails die gesamte elektronische Post samt privater Nachrichten gesichtet werden muss. Freilich muss man sehen, dass bei erlaubter privater Nutzung das BDSG ja auch nach Ansicht des Gesetzgebers gar nicht anwendbar sein soll,[59] so dass der Anwendungsbereich auch dieser Vorschrift beschränkt wäre.

V. Europäischer Kontext

Ein aktueller Vorschlag der EU für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), die die bisher geltende Datenschutzrichtlinie 95/46/EG ersetzen soll, sieht vor allem die Einwilligung des Arbeitnehmers kritisch: „Die Einwilligung liefert keine rechtliche Handhabe für die Verarbeitung personenbezogener

Hecker, in: Schönke/Schröder (Fn. 22), § 303a Rn. 3; *Hoyer* (Fn. 22), § 303a Rn. 5; *Hilgendorf*, in: Satzger/Schmitt/Widmaier (Fn. 22), § 303a Rn. 5.

[52] BT-Drs. 17/4230. Vgl. den Diskussionsentwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis des Bundesministeriums für Arbeit und Soziales v. August 2009; siehe ferner den Referentenentwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes des Bundesministerium des Innern v. 28.5.2010; Hintergrundpapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, Kabinettsbeschluss v. 25.8.2010.

[53] BT-Drs. 17/4230, S. 18.

[54] BT-Drs. 17/4230, S. 21 und S. 42; Hintergrundpapier zum Gesetzentwurf Beschäftigtendatenschutz v. 25.8.2010, S. 6; *Beckschulze/Natzel*, BB 2010, 2368 (2374); *Vietmeyers/Bryers*, MMR 2010, 807.

[55] Zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes BT-Drs. 17/4230, S. 42.

[56] BT-Drs. 17/4230, S. 22.

[57] Siehe auch *Vietmeyer/Byers*, MMR 2010, 807 (809 f.).

[58] BT-Drs. 17/4230, S. 22.

[59] BT-Drs. 17/4230, S. 42.

Daten, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein klares Ungleichgewicht besteht. Dies ist vor allem dann der Fall, wenn sich die betroffene Person in einem Abhängigkeitsverhältnis von dem für die Verarbeitung Verantwortlichen befindet, zum Beispiel dann, wenn personenbezogene Daten von Arbeitnehmern durch den Arbeitgeber im Rahmen von Beschäftigungsverhältnissen verarbeitet werden."[60] Eine solche Regelung würde Compliance- Maßnahmen gegenüber der geltenden Rechtslage eine weitere empfindliche Grenze setzen. Im Übrigen möchte der Vorschlag den Mitgliedstaaten die Regelung der Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext jedoch in den von der geplanten Verordnung gezogenen Grenzen weiterhin überlassen.

[60] Erwägungsgrund 34 des Vorschlags; vgl. KOM(2012) 11 endg.