IT-gestützte interne Ermittlungen in Unternehmen – Strafbarkeitsrisiken nach den §§ 202a, 206 StGB

Von Akad. Rat Dr. **Frank Peter Schuster**, Mag. iur., Mainz

Unternehmensinterne Ermittlungen werden als Dienstleistung angesichts stetig steigender Ansprüche an „Corporate Compliance" zunehmend auch in Deutschland nachgefragt – vor allem in Zusammenhang mit der Aufklärung von Korruptions-, Untreue- und Betrugsvorwürfen. Äußerst praxisrelevant ist dabei die Sichtung von Computerdateien, insbesondere E-Mails, auf firmeneigenen Datenträgern. Negativ-Schlagworte wie „Mitarbeiterüberwachung", „Datenskandal" und „Spitzelaffäre" beschreiben allerdings die Kehrseite solcher Maßnahmen. Dieser Beitrag beschäftigt sich mit möglichen Strafbarkeitsrisiken nach den §§ 202a, 206 StGB für Ermittler und ihre Auftraggeber. Insofern ist bisher noch keine strafgerichtliche Rechtsprechung ergangen.

I. Einleitung

Der Trend zum „papierlosen Arbeitsplatz" macht die Datenbestände eines Unternehmens zu einer herausragenden Erkenntnisquelle, denn dolose Handlungen der Mitarbeiter hinterlassen vielfältig Spuren auf den Computersystemen.[1] Dabei kann es sich u.a. um abgespeicherte Geschäftsbriefe, (verworfene) Geschäftberichte, Bilanzen, Kalkulationen, Scheinrechnungen, interne Vereinbarungen, Vertragsentwürfe, Memos oder Meeting-Protokolle handeln. Fast alle Dokumente werden heutzutage elektronisch erstellt, weniger als die Hälfte jemals ausgedruckt.[2] Zentrale Bedeutung haben aber vor allem E-Mails, die bei mittelständischen Betrieben und Konzernen mittlerweile zum wichtigsten Kommunikationsmittel geworden sind.[3] Einzelne Datenbestände lassen sich technisch unter Zuhilfenahme forensischer Software auf bestimmte Inhalte, Namen, E-Mail-Adressen oder Stichworte filtern. Hinsichtlich einzelner verdächtiger Mitarbeiter lässt sich prüfen, welche Dateien von ihnen angelegt, ggf. manipuliert oder unrechtmäßig kopiert[4] wurden, aber auch welche Nachrichten sie in einem gewissen Zeitraum erhalten und versendet haben. Selbst die Wiederherstellung von gelöschten Dateien ist erstaunlich oft möglich, nicht nur, wenn die Firma über funktionierende Backup-Systeme verfügt. Daten sind nämlich auch nach Löschen oder Formatieren noch so lange auf dem Speichermedium vorhanden, bis neue an dieselbe Stelle geschrieben werden. Die für die Ermittler interessanten Dateien sind meist auf einem zentralen Server, also einem externen Speichermedium im Intra- oder Internet, seltener direkt auf dem Arbeits-PC oder firmeneigenen Notebook einzelner Mitarbeiter gespeichert. Vor der Sichtung wird zunächst ein identisches (bit-genaues) Abbild des Datenträgers erstellt. Nur dieses exakte Abbild wird untersucht, äußerst selten der Original-Datenträger, da dieser als Beweisstück verfügbar bleiben muss.[5]

Die Ermittlungsteams so genannter „internal investigations" werden entweder aus Angehörigen des eigenen Unternehmens oder solchen eigens beauftragter Rechtsanwaltskanzleien und Wirtschaftsprüfungsgesellschaften[6] gebildet, die sich ihrerseits externer IT-Dienstleister bedienen. Gegenüber Arbeitgeber und Ermittlern gelten bei all diesen Maßnahmen weder die Vorschriften der Strafprozessordnung noch irgendeine andere Verfahrensordnung. Sie bewegen sich dabei jedoch in keinem rechtsfreien Raum: Ein spezielles Beschäftigtendatenschutzgesetz[7] wird es zwar auf absehbare Zeit nicht geben, auch die Überlegungen zu einem eigenen Kapitel im Bundesdatenschutzgesetz, so wie es der Koalitionsvertrag der neuen Regierungsparteien vorsieht,[8] stehen wohl noch am Anfang. Schon heute stellt aber neben dem am 1. September 2009 in Kraft getretenen § 32 BDSG, dessen Auslegung noch viele Probleme bereitet,[9] dem Individual-

---

* Der Beitrag beruht auf einem Referat, das der *Verf.* auf einer Vortragsveranstaltung der Wirtschaftsstrafrechtlichen Vereinigung e.V. (WisteV) zum Thema „Technische Möglichkeiten und rechtliche Rahmenbedingungen für IT-gestützte interne Ermittlungen in Unternehmen" in Frankfurt am Main gehalten hat.

[1] *Salvenmoser/Schreier*, in: Achenbach/Ransiek (Hrsg.), Handbuch Wirtschaftsstrafrecht, 2. Auflage 2008, Kap. XV, Rn. 93.

[2] Vgl. die Broschüre der Firma Kroll Ontrack Inc. (Hrsg.), Whitepaper Forensik, S. 6.

[3] Laut Computerwoche 20/2006 („Das ungeliebte Kind E-Mail-Archivierung") machen E-Mails etwa 60-70% der geschäftlichen Kommunikation aus.

[4] Etwa auf USB-Stick, CD-ROM, DVD oder externe Festplatte, aber auch MP3-Player, PDA, Mobiltelefon etc.

[5] Vgl. Kroll Ontrack Inc. (Fn. 2), S. 15. Für das Abbild wird eine so genannte hexdezimale MD5-Prüfsumme errechnet, die dann spätere Abweichungen vom Original (und damit eventuelle Manipulationen) auf einen Blick feststellbar machen würde.

[6] Anders als eigene Mitarbeiter oder solche normaler Wirtschaftsdetekteien haben Rechtsanwälte und Wirtschaftsprüfer den Vorteil, dass diese der Verschwiegenheit unterliegen, was durch § 203 Abs. 1 Nr. 3, Abs. 3 StGB, §§ 53 Abs. 1 Nr. 3, 53a StPO; § 43a Abs. 2 BRAO; § 43 Abs. 1 WPO umfassend gewährleistet wird.

[7] Ein solches wurde noch kurz vor der Bundestagswahl 2009 vom Bundesministerium für Arbeit und Soziales unter Olaf Scholz (SPD) als Diskussionsentwurf vorgestellt.

[8] Vgl. Koalitionsvertrag zwischen CDU, CSU und FDP („Wachstum, Bildung, Zusammenhalt"), S. 106.

[9] Vgl. dazu etwa *Beckschulze*, BB 2009, 2097 (2099); *Erfurth*, NJOZ 2009, 2914; *Gola/Klug*, NJW 2009, 2577 (2580); *Hanloser*, MMR 2009, 594 (597); *Schmidl*, ZJS 2009, 453; *Thüsing*, NZA 2009, 865; *Vogel/Glas*, DB 2009, 1747; *Wybitul*, BB 2009, 1582; *Wuermeling*, NJW-Editorial, Heft 37/2009. Die neue Vorschrift, die § 28 Abs. 1 Nr. 1 BDSG im Hinblick auf Beschäftigungsverhältnisse verdrängt, sollte die von der Rechtsprechung bisher erarbeiteten Grundsätze lediglich zusammenfassen (BT-Drs. 16/13657, S. 20 f.). Dennoch wirft sie viele neue Fragen auf: Nach § 32 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten für Zwecke des Beschäfti-

und Kollektivarbeitsrecht[10] vor allem auch das materielle Strafrecht zahlreiche Hürden auf. Während die Ermittler z.B. im Rahmen von Mitarbeiter-„Interviews" § 240 StGB (und erst recht § 132 StGB)[11] zu beachten haben, das Abhören von Telefonaten nach § 201 Abs. 2 S. 1 Nr. 1 StGB[12] strafbar ist, kommen bei der elektronischen Beweissicherung insbesondere Strafbarkeiten nach den §§ 202a, 206 StGB in Betracht, die die Ermittler selbst, aber vor allem auch ihre Auftraggeber treffen könnten. Dies gilt selbst dann, wenn die Daten physikalisch auf Servern im Ausland lagern.[13]

II. Strafbarkeitsrisiken nach § 202a StGB bei der Kontrolle von Computerdateien im Allgemeinen

Nach § 202a StGB macht sich strafbar, wer sich unbefugt Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft. Unzweifelhaft fallen alle hier relevanten Dateien, auch E-Mails, unter den Datenbegriff des § 202a Abs. 2 StGB.

1. Verfügungsberechtigung bei dienstlichen und privaten Dateien auf firmeneigenen Speichermedien

Erste Voraussetzung für eine mögliche Strafbarkeit des Arbeitgebers oder von ihm beauftragter Ermittler ist die fehlende Verfügungsbefugnis des Arbeitgebers. Die Verfügungsbefugnis hängt nicht vom Eigentum am Datenträger ab.[14] Vielmehr geht man davon aus, dass grundsätzlich derjenige verfügungsberechtigt ist, durch den die Daten erstellt und abgespeichert wurden.[15]

a) Auch bei dienstlichen Dateien erfolgt die unmittelbare Ausführung des Erstellens und Speicherns durch die Arbeitnehmer. Diese sind dabei allerdings den Weisungen des Arbeitgebers unterworfen; alle dienstlichen Vorgänge erfolgen auf seine Veranlassung.[16] Deshalb wird man den Arbeitgeber als eigentlichen Urheber ansehen müssen; ihm ist der Skripturakt zuzurechnen.[17] Derselbe Rechtsgedanke findet sich bei § 69b UrheberG und i.w.S. auch bei den §§ 267 ff. StGB.[18] Da der Arbeitgeber damit selbst verfügungsbefugt ist, ist die Kontrolle dienstlicher Dateien in Hinblick auf den Tatbestand des § 202a StGB an sich unproblematisch.[19]

---

gungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies zur Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses *erforderlich* ist. Dies ist wohl weiterhin dann der Fall, wenn die berechtigten Interessen des Unternehmens auf andere Weise nicht oder nicht angemessen gewahrt werden können. Zur Aufklärung von Straftaten soll jedoch nach § 32 Abs. 1 S. 2 BDSG ein strengerer Maßstab gelten: Eine Datenerhebung, -verarbeitung und -nutzung ist nur dann zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte bereits den Verdacht begründen, dass der Betroffene eine Straftat begangen hat. Darüber hinaus gilt eine qualifizierte Abwägungs- und Verhältnismäßigkeitsklausel. Das handschriftliche Dokumentieren erster Verdachtsmomente wäre allerdings demnach schon selbst Datenerhebung. Zudem kann eine Straftat freilich (wie reine Vertragsverletzungen und Ordnungswidrigkeiten) auch für die Beendigung des Beschäftigungsverhältnisses relevant werden, so dass insofern das Verhältnis zu § 32 Abs. 1 S. 1 BDSG einer Klärung bedarf. Abgrenzungsprobleme gibt es auch zu präventiven Maßnahmen zwecks *Verhinderung* von Straftaten, die ebenfalls nur unter § 32 Abs. 1 S. 1 BDSG fallen sollen. Ungeklärt ist schließlich das Verhältnis zu § 28 Abs. 1 S. 1 Nr. 2 BDSG, der nicht zu den von § 32 BDSG verdrängten Erlaubnistatbeständen gehört. Interne Ermittlungen (auch „gegen Unbekannt") für beschäftigungsfremde Zwecke (Verteidigung des Unternehmens im Fall des §§ 30, 130 OWiG, Abwehr von Schadensersatzansprüchen, Geltendmachung ebensolcher gegen Dritte etc.) lassen sich wohl auf diese Vorschrift stützen, die zwar eine Interessenabwägung vorsieht, aber keinen auf einzelne Betroffene konkretisierten Verdacht verlangt.

[10] Vgl. *Beckschulze*, BB 2009, 2097; *Wolf/Mulert*, BB 2008, 442; *Lindemann/Simon*, BB 2001, 1950; *Däubler*, Internet und Arbeitsrecht, 3. Aufl. 2004. Relevante Vorschriften sind z.B. § 87 Abs. 1 Nr. 6 BetrVG, § 75 Abs. 3 Nr. 17 BPersVG und Nr. 22 des Anhangs der Bildschirmarbeitsverordnung.

[11] *Klengel/Mückenberger*, CCZ 2009, 81 (82); *Knierim*, StV 2009, 324 (325, 329).

[12] *Graf*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, 2003, § 201 Rn. 11, 18. Das Mitlesen von geschriebenen Mitteilungen fällt dagegen nicht darunter, auch wenn der Meinungsaustausch „live" erfolgt (etwa im Rahmen eines nicht-öffentlichen Chats).

[13] Auf Strafanwendungsebene (vgl. §§ 3-7 und 9 StGB) gilt insofern: Für die Haupttat greift deutsches Strafrecht bereits dann, wenn der Täter z.B. gem. §§ 3, 9 Abs. 1 StGB in Deutschland gehandelt hat oder der zum Tatbestand gehörende Erfolg im Inland eingetreten ist. Selbst wenn nach diesem Kriterium eine reine Auslandstat vorliegt, kommt für inländische Teilnahmehandlungen § 9 Abs. 2 S. 2 StGB zur Anwendung. Auf Tatbestandsebene gilt: Bei Strafnormen, die ausschließlich (§ 202a StGB) oder mitunter (§ 206 StGB) dem Schutz von Individualrechtsgütern dienen, kann vermutet werden, dass es auf die Belegenheit des Gutes oder die Nationalität des Inhabers nicht ankommt. Vgl. *Ambos*, in: Joecks/Miebach (Fn. 12), Bd. 1, 2003, Vor §§ 3-7 StGB Rn. 81; *Eser*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 27. Aufl., 2006, Vor §§ 3-7 StGB Rn. 15; *Satzger*, in: Ders./Schmitt/Widmaier, Strafgesetzbuch, Kommentar, 2009, Vor §§ 3-7 StGB Rn. 8 f.; *Werle/Jeßberger*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 1, 12. Aufl. 2007, Vor § 3 StGB Rn. 274.

[14] *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 57. Aufl., 2010, § 202a StGB Rn. 7; *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 26. Aufl. 2007, § 202a StGB Rn. 3; *Weißgerber*, NZA 2003, 1005 (1007).

[15] *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 6, 13. Aufl. 2010, § 202a StGB, Rn. 26.

[16] *Graf* (Fn. 12), § 202a Rn. 17.

[17] *Hilgendorf*, JuS 1996, 890 (893) zu § 303a StGB.

[18] Vgl. *Erb*, in: Joecks/Miebach (Fn. 12), Bd. 4, 2006, § 267 Rn. 123 ff., 166 ff. zum „geistigen" Aussteller.

[19] *Salvenmoser/Schreier* (Fn. 1), Kap. XV Rn. 96.

b) Auf firmeneigenen Datenträgern befinden sich in der Praxis allerdings doch recht häufig auch private Dateien der Arbeitnehmer. Insbesondere forensische Filterprogramme werden diese kaum äußerlich von dienstlichen unterscheiden können. Private Dateien können dabei sehr wohl dem Schutz des § 202a StGB unterfallen, auch dann, wenn die private Nutzung des PCs eigentlich gänzlich verboten wurde. Dass sich der Arbeitnehmer weisungswidrig verhält, hat nämlich keine Auswirkungen auf die Urheberschaft, die der Verfügungsbefugnis zugrunde liegt.[20] Ein Verbot durch den Arbeitgeber wird allenfalls beim Vorsatz (ggf. auch bei einer Rechtfertigung[21]) des Arbeitgebers relevant werden.

2. Zugangssicherung bei privaten Dateien auf firmeneigenen Speichermedien

Weitere Voraussetzung des § 202a StGB ist jedoch, dass die privaten Dateien gegen unberechtigten Zugang besonders gesichert sind. Unzweifelhaft fällt die Einsichtnahme in einzelne kennwortgeschützte private Dateien oder ein kennwortgeschütztes privates Unterverzeichnis darunter.[22] Der Kennwortschutz verhindert den ungehinderten Zugriff und bringt gleichzeitig den Geheimhaltungswillen des Berechtigten unmissverständlich zum Ausdruck.

Bei lebensnaher Betrachtung wird der Arbeitnehmer in aller Regel einen solchen separaten Kennwortschutz jedoch nicht einrichten. Er wird seine privaten Dateien neben den dienstlichen in seinem Heimverzeichnis, also seinem personalisierten virtuellen Laufwerk, abspeichern. Dieses verfügt schließlich selbst über Passwortschutz; um darauf zugreifen zu können, muss man sich mit Benutzernamen und persönlichem Passwort anmelden. Ein Dritter, der so geschützte Dateien, auch E-Mails, in Überwindung des Kennwortschutzes unerlaubt durchsucht, macht sich deshalb ganz ohne Frage nach § 202a StGB strafbar.

Problematisch ist jedoch, ob das allgemeine Benutzerpasswort des Heimverzeichnisses eine Sicherungsfunktion gegenüber dem Arbeitgeber hat. Dagegen spricht bereits, dass der Arbeitgeber über seinen Systemadministrator meistens über eine Art „Ober"-Passwort verfügen wird, mit dem er auf die Verzeichnisse und Arbeitsergebnisse aller Abteilungen, Arbeitsgruppen und Mitarbeiter zugreifen kann. Der Arbeitgeber könnte (in Hinblick auf Krankheitsfälle, urlaubsbedingte Abwesenheit, Kündigung etc.) auch jederzeit kraft seines Direktionsrechts die Anweisung erteilen, dass der Arbeitnehmer ihm sein Passwort offenbart. Die Vergabe von Passworten an Mitarbeiter dient nämlich nur dem Schutz von Zugriffen von außen und der Zuordnung einzelner Vorgänge am Computer zum jeweiligen Urheber. Vielleicht trägt man so auch § 9 BDSG Rechnung, indem man sicherstellt, dass der Mitarbeiter nur auf die personenbezogenen Daten zugreifen kann, die er für die Erledigung seiner Aufgaben benötigt.[23] Die Vergabe von Benutzerkennworten bezweckt aber nicht den Geheimnisschutz gegenüber dem Arbeitgeber; dem Mitarbeiter soll keine „private Ecke" auf der arbeitgeberseitigen Computeranlage zur Verfügung gestellt werden.[24] § 202a StGB scheidet deshalb aus.

III. Strafbarkeit nach 206 StGB bei der Kontrolle von E-Mails im Speziellen

Bei der Durchsicht von E-Mails und gegebenenfalls ihrer Weiterleitung könnte allerdings § 206 StGB eine Rolle spielen, wenn dadurch das Fernmeldegeheimnis verletzt würde. Die meisten Autoren sehen hier ein erhebliches Strafbarkeitsrisiko für Unternehmensangehörige und externe Ermittler.[25] Nicht zuletzt, weil eine Entscheidung des OLG Karlsruhe[26] insofern für einiges Aufsehen gesorgt hat, auch wenn die Entscheidung eigentlich eine andere Konstellation, namentlich das Ausfiltern privater E-Mails, insbesondere Spam-Mails,[27] betraf.

1. Arbeitgeber als geschäftsmäßiger Erbringer von Telekommunikationsdiensten

Voraussetzung aller Tatbestandsvarianten von § 206 StGB ist zunächst, dass der Arbeitgeber als Betreiber eines Unternehmens anzusehen ist, das geschäftsmäßig Telekommunikationsdienste erbringt. Der Anwendungsbereich des § 206 StGB ist weiter, als man zunächst annehmen möchte; er ist keinesfalls auf die Nachfolger der Deutschen Bundespost und ihre Konkurrenzunternehmen beschränkt.[28] Das „geschäftsmäßige Erbringen von Telekommunikationsdiensten", wie in § 3 Nr. 10 TKG definiert, umfasst vielmehr das „nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht". Unschädlich ist dabei, wenn der Telekommunikationsdienst nur für eine geschlossene Benutzergruppe, wie Gäste eines Hotels oder Patienten im Krankenhaus, erbracht werden soll.[29] Räumt nun ein Arbeitgeber seinem Mitarbeiter die Möglichkeit ein, vom Arbeitsplatz auf das Internet zuzugreifen und über einen personalisierten E-Mail-Account des Arbeitsgebers nicht nur dienstlich, sondern auch für private Zwecke zu kommunizieren,[30] ist der Arbeit-

[20] *Weißgerber*, NZA 2003, 1005 (1008).
[21] Diese wird vor allem im Rahmen von § 303a StGB eine Rolle spielen, wenn der Arbeitgeber unerlaubt abgespeicherte private Daten löscht.
[22] *Salvenmoser/Schreier* (Fn. 1), Kap. XV Rn. 97.
[23] LAG Hamm, Urt. v. 4.2.2004 – 9 Sa 502/03, Rn. 51.
[24] LAG Köln NZA-RR 2004, 527 (528); *Barton*, CR 2003, 839 (842); *Beckschulze*, DB 2003, 2777 (2783); *Salvenmoser/Schreier* (Fn. 1), Kap. XV Rn. 98; a.A. *Weißgerber*, NZA 2003, 1005 (1008).
[25] *Hoeren*, Skriptum Internetrecht (Stand: März 2009), S. 401.
[26] OLG Karlsruhe MMR 2005, 178 (179 f.).
[27] Vgl. dazu *Heidrich*, CR 2009, 168; *Schmidl*, DuD 2005, 267 (269 ff.); *Kitz*, CR 2005, 450.
[28] *Dann/Gastell*, NJW 2008, 2945 (2946).
[29] Vgl. BT-Drs. 13/8016, S. 29.
[30] *Sieber*, in: Hoeren/ders., Handbuch Multimediarecht, 1. Lfg., Stand: Februar 2000, Kap. 19 Rn. 534; *Beckschulze/Henkel*, DB 2001, 1491 (1496); *Schmidl*, DuD 2005, 267 (269); *Härting*, CR 2007, 311 (312); *Gola*, MMR 1999, 322 (324). Nach OLG Karlsruhe MMR 2005, 178 (179 f.) wurde so selbst eine baden-württembergische Universität zum Tele-

nehmer ebenfalls ein solcher Dritter, soweit er diesen Service privat nutzt. Ist die private Nutzung dagegen verboten, bilden Arbeitgeber und Arbeitnehmer eine Organisationseinheit, § 206 StGB ist von vornherein nicht einschlägig.

Oft ist die Internet- und E-Mail-Nutzung (anders als die des Diensttelefons) allerdings gar nicht geregelt, was daran liegen kann, dass die Unternehmen regelmäßig über eine Flatrate verfügen. Was dann gilt, ist wohl Frage des Einzelfalls: Die Annahme, dass Zweifelsfälle generell zu Lasten des Arbeitgebers gingen, weil es seine Organisationsaufgabe sei, die Nutzung des betrieblichen Computersystems klar zu definieren,[31] ist wohl zu weitgehend. Jedenfalls hat das BAG verhaltensbedingte Kündigungen bei exzessiver Nutzung auch ohne ausdrückliches Verbot der privaten Nutzung schon mehrfach bestätigt.[32] Der Arbeitgeber kann allerdings in der Praxis, anders als man vielleicht zunächst vermuten möchte, durchaus gute Gründe haben, die *gelegentliche* private Nutzung von betrieblichen Kommunikationsmitteln konkludent oder gar ausdrücklich zu erlauben: Gerade bei den Entscheidungsträgern, den höheren Lohngruppen etc. profitieren die Arbeitgeber nämlich davon, dass Arbeit und Privatleben durch stete Ausdehnung des Leistungs- in den Freizeitbereich immer mehr verschmelzen.[33] Dem „Extremjobber", der laut Definition des New Yorker Center for Work-Life Policy (CWLP)[34] deutlich mehr als 60 Stunden pro Woche arbeitet, rund um die Uhr erreichbar ist,[35] hohe Verantwortung trägt, unter enormem Zeitdruck steht und gleichzeitig mit mehreren Projekten befasst ist, wird man nur ungern kleinliche Vorgaben für ein wenig private Kommunikation machen. Die weitere Prüfung wird aber zeigen, ob vielleicht wegen § 206 StGB strengere „Spielregeln" gelten sollten.

2. Taugliche Täter

Zunächst gilt es, § 206 StGB in Hinblick auf den Kreis der tauglichen Täter genauer zu untersuchen. Solche sind in erster Linie der Inhaber oder ein Beschäftigter des Unternehmens. Außenstehende externe Ermittler fallen nicht darunter. Sie stehen zum Unternehmen in keinem *dauerhaften* privatrechtlichen oder öffentlich-rechtlichen Beschäftigungsverhältnis, bloß sporadische Tätigkeiten reichen insofern nicht.[36] Andere unternehmensnahe Personen werden in § 206 Abs. 3 Nrn. 1-3 StGB genannt, sind dort aber abschließend geregelt. Für externe private Ermittler kommen deshalb nur Teilnehmerstrafbarkeiten in Betracht.[37] Da diese aber akzessorisch sind, ist die Strafbarkeit des Inhabers oder eines Beschäftigten für alle Fälle Ausgangspunkt aller weiteren Überlegungen.

3. Weitergabe einzelner belastender E-Mails

Nach § 206 Abs. 1 StGB wird bestraft, wer einer anderen Person Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen. Zunächst gilt es zu prüfen, ob dies *generell* der Weitergabe einzelner belastender E-Mails an Vorgesetzte, die Compliance- oder Personalabteilung, Unternehmensanwälte, Strafverfolgungsbehörden etc. entgegensteht.

a) Andere Person ist auch der eigene Mitarbeiter (z.B. einer forensischen Abteilung), der im gewöhnlichen Geschäftsgang von den E-Mails keine Kenntnis erlangt hätte.[38] Ohne Bedeutung ist ferner, ob der Empfänger eventuell seinerseits schweigepflichtig ist,[39] z.B. gem. § 206 Abs. 1 StGB bei Beschäftigten oder gem. § 203 Abs. 1 Nr. 3, Abs. 3 StGB bei

kommunikationsdienst. Dagegen machen z.B. *Seffer/Schneider*, ITRB 2007, 264 (266); *Haussmann/Krets*, NZA 2005, 259 (260 f.) geltend, dass ein Arbeitgeber nicht i.S.d. § 1 TKG im Wettbewerb auftrete und auch nicht dazu beitrage, eine flächendeckend angemessene und ausreichende Dienstleistung zu gewährleisten. Dies überzeugt so jedoch nicht, da auch zu Zeiten des Postmonopols ein Fernmeldegeheimnis bestand. Auch an der Nachhaltigkeit der Diensterbringung fehlt es nicht, letztere muss nämlich nur auf Dauer angelegt sein, vgl. *Welp*, in: Eser u.a. (Hrsg.), Festschrift für Theodor Lenckner zum 70. Geburtstag, 1998, S. 619 (S. 632).

[31] Vgl. LAG Köln NZA-RR 2004, 527; in diese Richtung auch *Lelley*, GmbHR 2002, R 373; *Fleischmann*, NZA 2008, 1397; § 14 Abs. 1 S. 3 des in Fn. 7 erwähnten BMAS-Entwurfs für ein BeschäftigtendatenschutzG.

[32] BAG NZA 2006, 98; BAG NJW 2007, 2653; vgl. auch *Beckschulze*, DB 2009, 2097; *Schmitz-Scholemann* (RiBAG), in: Focus 31/2007 („Grundsätzlich gilt für privates Internet im Büro: Was nicht erlaubt ist, ist verboten.").

[33] Zu den Gefahren dieser Entwicklung, etwa der Entstehung arbeitsplatzbezogener Subkulturen, vgl. allerdings *Schneider*, NStZ 2007, 555 (559).

[34] Vgl. manager-magazin, Heft 2/2007 („Motivation – Ausweitung der Arbeitszone"); *Hewlett/Luce/Southwell/Bernstein*, Seduction and Risk: The Emergence of Extreme Jobs, 2007.

[35] Oft stellt der Arbeitgeber dem Mitarbeiter ein so genanntes „Smartphone" zur Verfügung, dass auch in der Freizeit ständig mitgeführt werden soll und die Funktionen eines Mobiltelefons, E-Mail-Dienstes, Terminkalenders, Datenspeichers, Diktiergeräts etc. vereint. Das Beisichtragen eines Zweitgerätes für private Zwecke erscheint einem dann kaum zumutbar.

[36] Vgl. *Lenckner*, in: Schönke/Schröder (Fn. 13), § 206 StGB, Rn. 8; vgl. auch *Welp* (Fn. 30), S. 633. Nach *Altenhain*, in: Joecks/Miebach (Fn. 12), § 206 StGB. Rn. 23; *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 2. Aufl. 2005, § 206 Rn. 12, soll auch bei § 206 Abs. 1 StGB bloßes „Mitwirken" bei der Erbringung von Post- oder Telekommunikationsdiensten (vgl. § 39 Abs. 2 S. 1 PostG, § 85 Abs. 2 S. 2 TKG a.F.) ausreichen. Dies erscheint fraglich, da § 206 Abs. 3 StGB dann überflüssig wäre. Aber selbst dieses Kriterium dürfte bei privaten Ermittlern nicht gegeben sein, da ihre Tätigkeit für die Erbringung der Dienste nicht relevant wird.

[37] Der Sache nach fallen sie am ehesten unter § 206 Abs. 4 StGB, sie sind aber keine Amtsträger.

[38] Vgl. *Sieber* (Fn. 30), Kap. 19 Rn. 538; *Lenckner* (Fn. 36), § 206 StGB Rn. 10.

[39] Vgl. zu § 203 StGB: BGHZ 116, 268; BGH[Z] NJW 1993, 1912; *Fischer* (Fn. 14), § 203 StGB Rn. 30b.

Rechtsanwälten, Wirtschaftsprüfern und ihren Gehilfen.[40] Andere Personen sind auch die Strafverfolgungsorgane; ihre Eingriffsbefugnisse spielen erst auf Rechtfertigungsebene (siehe dazu III. 5. b) eine Rolle.

b) Das Fernmeldegeheimnis umfasst gem. § 206 Abs. 5 S. 2 StGB den Inhalt der Telekommunikation und ihre näheren Umstände. Telekommunikation selbst ist gem. § 3 Nr. 22 TKG der technische Vorgang des Aussendens, Übermittelns und Empfangens. Werden private E-Mails zu diesem Zeitpunkt abgefangen und kopiert, um sie nachträglich auszuwerten und weiterzuleiten, ist das Telekommunikationsgeheimnis auf jeden Fall betroffen. Praxisrelevantes Beispiel sind die Sicherungskopien, die von vielen Unternehmen durch Back-up-Systeme standardmäßig in der Übertragungsphase hergestellt werden[41]. Irrelevant für die Strafbarkeit ist dann natürlich, wenn die Mitteilung selbst erst nach Abschluss des Übertragungsvorgangs vorgenommen wird.

Unklar ist dagegen, was gilt, wenn die E-Mails im Zeitpunkt des ersten Zugriffs bereits auf dem Mailserver des Arbeitgebers „ruhen“[42], also ein Telekommunikationsvorgang in einem dynamischen Sinne gar nicht mehr stattfindet. Hoffnung für Arbeitgeber und Ermittler, so Strafbarkeiten vermeiden zu können, gibt eine Entscheidung des Hess. VGH[43], der über die Rechtmäßigkeit eines Auskunfts- und Vorlageersuchens der BaFin zu befinden hatte. Die BaFin hatte auf Ersuchen der amerikanischen Wertpapieraufsicht SEC den Arbeitgeber gem. § 4 Abs. 3 WpHG aufgefordert, sämtliche E-Mails namentlich bezeichneter Mitarbeiter, die bestimmte Namen und Stichworte enthielten, vorzulegen. Gegen diesen Bescheid hatte der Arbeitgeber mit Hinweis auf das Fernmeldegeheimnis Widerspruch eingelegt und schließlich geklagt – ohne Erfolg. Der Hess. VGH sah Art. 10 GG und § 88 TKG als nicht betroffen an.[44] Dabei berief sich das Gericht auf die Rechtsprechung des BVerfG hinsichtlich E-Mails, die der Nutzer auf die Festplatte seines PCs heruntergeladen hatte: Wenn in diesem Fall nur auf den PC selbst zugegriffen wird, so ist das Fernmeldegeheimnis ganz eindeutig nicht betroffen[45] – genauso wenig wie es etwa bei einem ausgedruckten Telefax oder den Aufzeichnungen eines häuslichen Anrufbeantworters der Fall wäre. Das Herunterladen von E-Mails auf dem Arbeits-PC („POP3“) ist in Unternehmen allerdings eher ungewöhnlich.[46] Ein schlichtes Belassen auf dem E-Mail-Server („IMAP“) kann mit diesem jedoch nicht gleichgesetzt werden – so jedenfalls jüngst das BVerfG[47] zum Schutzbereich von Art. 10 GG: Solange die E-Mail auf dem Mailserver eines Providers verbleibt und nicht in den Herrschaftsbereich des Nutzers gelangt, kann der Nutzer die E-Mails zwar für sich auf einem Bildschirm lesbar machen. Er hat aber keine technische Möglichkeit, die Weitergabe der E-Mails durch den Provider zu verhindern. Dieser weiter bestehende, technisch bedingte Mangel an Beherrschbarkeit begründet die besondere Schutzbedürftigkeit durch das Fernmeldegeheimnis. Irrelevant ist demnach auch die Kenntnisnahme durch den Nutzer, solange die E-Mail auf dem Server verbleibt.[48] Dass für nichtstaatliche Eingriffe im Rahmen von § 206 StGB etwas anderes gelten sollte, ist nicht ersichtlich. § 206 Abs. 1 StGB wird deshalb der Weitergabe privater E-Mails bei erlaubter privater Nutzung grundsätzlich entgegenstehen.

c) Für das Unternehmen relevante Inhalte, die auf ein kriminelles Verhalten hindeuten, werden sich allerdings ohnehin eher in einzeln ausgefilterten dienstlichen E-Mails finden. Hinsichtlich dienstlicher E-Mails erbringt der Arbeitgeber gegenüber dem Arbeitnehmer keinen Telekommunikationsdienst. Auch bei erlaubter Mischnutzung ist der Arbeitgeber dann selbst Nutzer (vertreten durch den Arbeitnehmer), das Fernmeldegeheimnis und § 206 StGB sind von vornherein nicht einschlägig.[49]

4. Durchsicht oder Filtern des gesamten E-Mail-Verkehrs

Bei den meisten E-Mail-Programmen werden allerdings alle E-Mails eines Benutzers samt Anhängen in einer einzigen komprimierten Archivdatei gespeichert.[50] Ein Problem besteht nun darin, es ob möglich ist, dienstliche und private E-Mails voneinander zu trennen, ohne dass man sich allein dabei strafbar macht. § 88 Abs. 3 S. 1 TKG verbietet ganz allgemein, sich über das für die Erbringung von Fernmeldediensten erforderliche Maß Kenntnis von Telekommunikati-

[40] Insofern ist der Arbeitnehmer allerdings ohnehin nicht ausreichend geschützt, da das Unternehmen als Auftraggeber die ermittelnden Rechtsanwälte von der Schweigepflicht entbinden kann.

[41] Vgl. *Schöttler*, jurisPR-ITR 4/2009 Anm. 2, D.

[42] *Sieber* (Fn. 30), Kap. 19 Rn. 535; *Barton*, CR 2003, 839 (843).

[43] Hess. VGH NJW 2009, 2470; bestätigt wurde VG Frankfurt am Main CR 2009, 125.

[44] Hess. VGH NJW 2009, 2470 (2471 f.); zustimmend *Beckschulze*, DB 2009, 2097 (2098).

[45] Vgl. BVerfGE 115, 166 (183 ff.); BVerfGE 120, 274 (307 f.). Was greift, ist das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, ggf. auch Art. 13 Abs. 1 GG. Vgl. auch *Nack*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 6. Aufl. 2008, § 100a StPO Rn. 5.

[46] Im Fall des Hess. VGH hatten die Nutzer die Möglichkeit, die E-Mails *aktiv* auf bestimmte, zentrale Speichermedien zu kopieren. Soweit die Nutzer tatsächlich davon Gebrauch gemacht haben, kann man mit VG Frankfurt am Main CR 2009, 125 (126); Hess. VGH NJW 2009, 2470 (2471 f.) argumentieren, dass diese Daten sich nicht mehr von solchen unterscheiden, die der Nutzer selbst angelegt hat.

[47] BVerfG NJW 2009, 2431 (2432 f.); vgl. auch BVerfGE 120, 274 (341).

[48] Vgl. auch *Gaede*, StV 2009, 96 (97 f.); a.A. *Nolte/Becker*, CR 2009, 126 (127); *Krüger*, MMR 2009, 680 (682).

[49] A.A. *Salvenmoser/Schreier* (Fn. 1), Kap. XV Rn. 109.

[50] In diesen Dateien können sich dann hunderte bis tausende Nachrichten nebst Anlagen befinden, vgl. *Kemper*, NStZ 2006, 538 (543).

onsvorgängen zu verschaffen. Die Norm regelt allerdings bekanntermaßen nicht die Strafbarkeit.[51]

a) Für das schlichte Durchsehen oder Filtern von dienstlichen und privaten E-Mails mag, soweit private E-Mails betroffen sind, zunächst eine Strafbarkeit nach § 206 Abs. 2 Nr. 1 StGB nahe liegen. Demnach macht sich strafbar, wer eine verschlossene Sendung öffnet oder sich sonst von ihrem Inhalt Kenntnis verschafft. Problematisch ist jedoch, ob die E-Mail überhaupt unter den Begriff der Sendung fällt. Der Gesetzgeber dürfte hier vornehmlich an Briefe und Pakete gedacht haben. Das OLG Karlsruhe sah allerdings § 206 Abs. 2 Nr. 2 StGB als erfüllt an, wenn private E-Mails ohne Erlaubnis des Empfängers angehalten und unterdrückt werden.[52] § 206 Abs. 2 Nr. 1 StGB verlangt demgegenüber eine *verschlossene* Sendung. Ein Verschlossensein ist dann allerdings nach ganz herrschender Ansicht nur bei körperlichen Sendungen denkbar.[53]

b) Bleibt für das schlichte Durchsehen oder Filtern wiederum nur § 206 Abs. 1 StGB. Das bloße Einsichtnehmen in E-Mails auf einem firmeneigenen Server, aber auch das bloße Mitprotokollieren dienstlicher und privater E-Mail-Kommunikation über unternehmenseigene Filter ist an sich noch keine Mitteilung an eine andere Person.[54] In der Regel wird der Arbeitgeber jedoch eine Kopie des gesamten E-Mail-Bestandes erstellen lassen, welche dann an eine externe Firma zur weiteren Untersuchung (z.B. hinsichtlich bestimmter Mitarbeiter) übermittelt wird. Die auch nur vorübergehende Weitergabe des gesamten E-Mail-Verkehrs, auch das bloße Gewähren von Zugang zu einem Datenbestand, kann dann durchaus als Mitteilung i.S.d. § 206 Abs. 1 StGB verstanden werden. Mitteilen ist nämlich jedes Handeln, das zur Kenntniserlangung durch Dritte führt. Es kann auch dadurch geschehen, dass die Tatsachen verschriftet oder auf einem Datenträger in den Wahrnehmungsbereich des Dritten verbracht werden.[55] Eine Mitteilung ist schließlich selbst durch Unterlassen möglich, wenn Inhaber oder Bediensteter es pflichtwidrig geschehen lässt, dass sich andere – z.B. aufgrund fehlender technischer Schutzmaßnahmen (vgl. § 109 TKG) – Kenntnis von Tatsachen verschaffen, die dem Fernmeldegeheimnis unterfallen.[56] Die Weitergabe ganzer Datenträger dürfte die Rechte der Nutzer sogar ganz besonders beeinträchtigen.

Der Tatbestand könnte allenfalls daran scheitern, dass dem Inhaber oder Beschäftigten die Tatsachen vor der Weitergabe selbst überhaupt nicht „bekanntgeworden" sind.[57] Völlig lebensfremd ist schließlich die Vorstellung, dass der Inhaber oder Beschäftigte den gesamten E-Mail-Bestand vor der Weitergabe selbst in irgendeiner Weise inhaltlich zu Kenntnis nehmen könnte. Aus der Sicht des Nutzers ist dies allerdings auch unerheblich, seine Geheimhaltungsinteressen werden durch den Täter so oder so verletzt. Der Sache nach sollte es deshalb ausreichen, dass der Täter im Rahmen des Dienstverhältnisses in die Lage versetzt wurde, dem Fernmeldegeheimnis unterliegende Tatsachen Dritten wie auch immer (mit oder ohne eigene Kenntnisnahme) zu offenbaren.[58] Nicht anders beurteilt wird dies schließlich auch bei Verletzung von Privatgeheimnissen gem. § 203 StGB (Krankenkassenmitarbeiter verkauft CD mit Patientendaten) und vergleichbaren Tatbeständen.[59] Dem Wortlaut von § 206 Abs. 1 StGB kann man dabei mit der Überlegung gerecht werden, dass dem Täter als Inhaber oder Beschäftigten des Unternehmens doch immerhin „bekanntgeworden" ist, dass

[51] § 44 TKG gewährt allerdings einen Anspruch auf Schadensersatz und Unterlassung. Die §§ 148, 149 TKG betreffen dagegen andere Sachverhalte.

[52] OLG Karlsruhe MMR 2005, 178; ebenso *Fischer* (Fn. 14), § 206 Rn. 15; *Lenckner* (Fn. 36), § 206 Rn. 20; zur Gegenansicht vgl. Fn. 53; zur Spam-Filterung siehe Nachw. in Fn. 27.

[53] Zwar sind E-Mails ebenfalls nicht ohne weiteres einsehbar. Verschlossen ist die E-Mail deshalb aber nicht, allenfalls versteckt. Das ist die Ansichtskarte in der Posttasche des Postboten aber auch. Eine Strafbarkeit wegen § 206 Abs. 2 Nr. 1 StGB scheidet deshalb aus. So auch *Lenckner* (Fn. 36), § 206 Rn. 17; *Fischer* (Fn. 14), § 206 Rn. 13 f. Nach *Altenhain* (Fn. 36), § 206 Rn. 44; *Bosch*, in: Satzger/Schmitt/Widmaier (Fn. 13), § 206 Rn. 8; *Kargl* (Fn. 36), § 206 Rn. 25; *Lackner/Kühl* (Fn. 14), § 206 Rn. 8 sind E-Mails sogar generell nicht von § 206 Abs. 2 Nrn. 1 und 2 StGB erfasst.

[54] *Barton*, CR 2003, 839, 843; *Altenburg/Reinersdorff/Leister*, MMR 2005, 135 (138); *Sieber* (Fn. 30), Kap. 19 Rn. 536. Straflos ist deshalb der neugierige Systemadministrator, der ab und an die E-Mails der Kollegen liest.

[55] Entscheidend ist der Erfolgsunwert der Offenbarung. Vgl. *Welp* (Fn. 30), S. 636; *Altenhain* (Fn. 36), § 206 Rn. 8; *Lackner/Kühl* (Fn. 14), § 206 Rn 7; *Altvater*, in: Laufhütte/Rissing-van Saan/Tiedemann (Fn. 13), Bd. 6, 12. Aufl. 2009, § 206 Rn. 27; *Lenckner* (Fn. 36), § 206 Rn 10.

[56] *Altenhain* (Fn. 36), § 206 Rn. 39; *Altvater* (Fn. 55), § 206 StGB, Rn. 29; *Sieber* (Fn. 30), Kap. 19 Rn. 537; vgl. zur Verletzung von Privatgeheimnissen auch *Fischer* (Fn. 14), § 203 StGB, Rn. 30b; *Lackner/Kühl* (Fn. 14), § 203 Rn 17.

[57] Vgl. *Altenhain* (Fn. 36), § 206 Rn. 38; *Hoyer*, in: Rudolphi u.a. (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, 56. Lfg., Stand: Mai 2003, § 206 Rn. 22; *Kargl* (Fn. 36), § 206 Rn. 21. Beim durchaus als strafwürdig erachteten Postboten, der einem Dritten seine Posttasche zur Einsicht überlässt, wird allerdings pauschal angenommen, er habe den Inhalt vorab gesichtet. Dies überzeugt so wohl nicht (siehe *Lenckner* [Fn. 36], § 206 Rn. 10).

[58] So auch *Welp* (Fn. 30), S. 636; *Lackner/Kühl* (Fn. 14), § 206 Rn. 7; *Altvater* (Fn. 55), § 206 Rn. 19, 28; *Bosch* (Fn. 53), § 206 Rn. 6 f. *Altenhain* (Fn. 36), § 206 Rn. 38 sieht darin einen Verstoß gegen Art. 103 Abs. 2 StGB.

[59] *Cierniak*, in: Joecks/Miebach (Fn. 12), Bd. 3, 2003, § 203 Rn. 44; *Lenckner* (Fn. 36), § 203 Rn. 17; *Otto*, wistra 1999, 201 (202; hier heißt es freilich: „anvertraut worden oder sonst bekanntgeworden ist"). Zu § 17 Abs. 1 UWG (hier heißt es: „anvertraut worden oder zugänglich geworden ist") vgl. *Diemer*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 158. Lfg., Stand: August 2005, § 17 UWG Rn. 22. Entsprechendes gilt bei §§ 353b, 355 StGB; § 85 GmbHG; § 151 GenG; § 333 HGB; § 404 AktG; § 19 PublG; § 315 UmwG; § 138 VAG.

die einem Dritten zur Kenntnisnahme überlassenen Materialien Telekommunikationsvorgänge betreffen.

Zwischenergebnis: Damit muss also davon ausgegangen werden, dass der Arbeitgeber bei Weitergabe des gesamten E-Mail-Bestandes zu Untersuchungszwecken, soweit er neben dienstlicher auch erlaubte private Kommunikation enthält, den Tatbestand des § 206 Abs. 1 StGB verwirklicht. Der Empfänger, meist ein externer Ermittler, leistet dazu zumindest Beihilfe gem. § 27 StGB.[60]

5. Ausschluss von Strafbarkeiten?

a) Möglicherweise lassen sich Strafbarkeiten jedoch durch Einholung eines ausdrücklichen Einverständnisses der Arbeitnehmer[61] vermeiden. Sinnvoll wäre es, dieses gleich mit der Gestattung gelegentlicher privater E-Mail-Nutzung zu verbinden.[62] Mit gewissem organisatorischem Aufwand wäre dies zwar auch im Nachhinein möglich. Besser sollte aber Existenz, Anlass und Art der Untersuchung den Mitarbeitern zunächst verborgen bleiben, um erschöpfend Beweismaterial sammeln zu können und Verdunklungshandlungen zu vermeiden.[63]

Ein wirksamer Verzicht auf Wahrung des Fernmeldegeheimnisses ist aber nur dann möglich, wenn dadurch lediglich schützenswerte Belange der Mitarbeiter betroffen sind,[64] da niemand ohne Ermächtigung über fremde Rechte verfügen kann. Wiederholt man formelartig das, was das BVerfG im Jahre 1992 zu Art. 10 GG und dem Problem der Fangschaltung entschieden hatte[65] – diese bedarf trotz Zustimmung des Anschlussinhabers wegen der fehlenden Zustimmung des Anrufers einer Ermächtigungsgrundlage (namentlich § 101 TKG) – dürfte die Zustimmung des Arbeitnehmers allein hier nicht ausreichen. Gegen das doppelte Zustimmungserfordernis lässt sich allerdings einwenden, dass es im Verhältnis der Telekommunikationspartner untereinander kein Fernmeldegeheimnis gibt.[66] Es ist dem Arbeitnehmer völlig unbenommen, dem Arbeitgeber freiwillig vom Arbeitsplatz aus Einblick in seinen gesamten E-Mail-Verkehr zu gewähren (oder ihm gar eine Kopie desselben auszuhändigen).[67] Wegen der schriftlichen Fixierung des Gedankeninhaltes wird sich der Kommunikationspartner dieser Möglichkeit auch vollauf bewusst sein. Bei einer unternehmensspezifischen E-Mail-Adresse („mustermann@unternehmen.de“) muss er ohnehin damit rechnen, dass auf diesen Account durchaus anderweitige Zugriffsrechte (z.B. des Sekretariats, der Urlaubs- oder Krankheitsvertretung) bestehen können.[68] Er kann sich nicht einmal darauf verlassen, dass der Arbeitgeber überhaupt Telekommunikationsdienste erbringt, also die private E-Mail-Nutzung erlaubt hat. All dies spricht *hier* gegen eine Schutzwürdigkeit des Absenders, sofern der Account-Inhaber mit der Überprüfung einverstanden ist. Dass die Kommentarliteratur insofern überwiegend nicht differenziert und in allen Fällen unter Bezugnahme auf das BVerfG die Zustimmung sämtlicher Kommunikationspartner verlangt,[69] wird man im Rahmen der Beratungspraxis jedoch nicht ignorieren können.

b) Deshalb (und für Fälle, in denen überhaupt kein Einverständnis erteilt wurde) gilt es nun zu prüfen, ob Arbeitgebern und Ermittlern eventuell Rechtfertigungsgründe zur Seite stehen. Die Weiterleitung von Kommunikationsinhalten an Strafverfolgungsbehörden kann natürlich aufgrund eines wirksamen Beschlusses gem. §§ 100a, 100b StPO[70] oder bei ruhenden E-Mails gem. §§ 94 ff., 102 ff. StPO[71] erfolgen. Meistens möchte man allerdings von der Einschaltung der Strafverfolgungsbehörden zunächst absehen. Besondere Rechtfertigungsgründe des TKG helfen dann nicht weiter: § 88 Abs. 3 S. 4 TKG z.B. gilt nur für bevorstehende in § 138 StGB genannte Katalogtaten, die komplette Weitergabe be-

[60] Zur Anwendbarkeit von §§ 28 Abs. 1, 49 Abs. 1 StGB vgl. *Altenhain* (Fn. 36), § 206 Rn. 90. Eine weitere Milderung wegen §§ 27 Abs. 2 S. 2, 49 Abs. 1 StGB soll allerdings ausscheiden, wenn allein wegen des Fehlens des persönlichen Merkmals nur Beihilfe angenommen werden kann, vgl. BGHSt 26, 53 (54).

[61] Eine Zustimmung wirkt hier wohl tatbestandsausschließend, vgl. *Altenhain* (Fn. 36), § 206 Rn. 41.

[62] So der Vorschlag von *Sieber* (Fn. 30), Kap. 19 Rn. 534; *Barton*, CR 2003, 839 (843).

[63] *Klengel/Mückenberger*, CCZ 2009, 81 (83). Wenn ein Mitarbeiter seine E-Mail bereits inkriminierend verwendet hat, würde er die Zustimmung im Nachhinein auch eher widerwillig erteilen. Von einer mutmaßlichen Einwilligung (diese wäre ein Rechtfertigungsgrund) wird man deshalb mangels eindeutigem Interesse keinesfalls ausgehen können. Vgl. *Barton*, CR 2003, 839 (844).

[64] Vgl. *Altvater* (Fn. 55), § 206 Rn. 84

[65] BVerfGE 85, 386 (399).

[66] BayObLG 1974, 393; vgl. auch BVerfGE 120, 274 (341) zur staatlichen Stelle als Kommunikationsbeteiligter. Dieses Argument wurde freilich auch schon (ohne Erfolg) bei der Fangschaltung vorgebracht.

[67] Vgl. BGHSt 39, 335 (343) zum heimlichen Mithören eines Telefonats am Endgerät mit Zustimmung des Anschlussinhabers.

[68] *Seffer/Schneider*, ITRB 2007, 264 (266); *Härting*, CR 2007, 311 (312); vgl. auch *Beckschulze*, DB 2003, 2777 (2780); *Haussmann/Krets*, NZA 2005, 259 (261).

[69] *Kargl* (Fn. 36), § 206 Rn. 45; *Altenhain* (Fn. 36), § 206 Rn. 42; *Lenckner* (Fn. 36), § 206 Rn. 12; *Bock*, in: Geppert/Piepenbrock/Schütz/Schuster (Hrsg.), Beck'scher Kommentar zum TKG, 3. Auflage 2006, § 88 Rn. 19; *Eckhardt*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, Rn. 15; *Zerres*, in: Scheurle/Mayen, Telekommunikationsgesetz, Kommentar, 2. Aufl. 2008, § 88 Rn. 15 f.; ausdrücklich auch für Arbeitsverhältnisse *Ellinghaus*, in: Arndt/Fetzer/Scherer (Hrsg.), Telekommunikationsgesetz, Kommentar, 2008, § 88 TKG, Rn. 12, 40; *Hilber/Frik*, RdA 2002, 89 (94). Wie hier nun jedoch *Altvater* (Fn. 55), § 206 Rn. 85 ff.

[70] Vgl. BGH StV 1997, 398; *Nack* (Fn. 45), § 100a Rn. 21.

[71] Vgl. BVerfG NJW 2009, 2431 (2433 f.); BGH NStZ 2009, 397 („§ 99 StPO“); *Nack* (Fn. 45), § 100a Rn. 22; zur Gegenansicht *Meyer-Goßner*, Strafprozessordnung, Kommentar, 52. Aufl. 2009, § 100a Rn. 6; *Zerres* (Fn. 69), § 88 Rn. 29 m.w.N.

stimmter E-Mail-Bestände wäre so nicht zu rechtfertigen. § 100 TKG dient der Störungssuche und Ermittlung von Leistungserschleichungen,[72] betrifft zudem nur die Bestands- und Verkehrsdaten, nicht die Kommunikationsinhalte. Hinsichtlich allgemeiner Rechtfertigungsgründe stellt sich schon die Frage, ob diese im Fall des § 206 StGB überhaupt anwendbar sind: § 88 Abs. 3 S. 3 TKG erlaubt eine Durchbrechung des Fernmeldegeheimnisses nämlich nur dann, wenn eine gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.[73] § 32 StGB würde aber auch so daran scheitern, dass sich Notwehr nur gegen Rechtsgüter eines Angreifers richten darf. Zum Zeitpunkt der Untersuchung wird aber oft gar kein gegenwärtiger, rechtswidriger Angriff mehr vorliegen; darüber hinaus verletzt die Weitergabe bestimmter E-Mail-Bestände in der Regel auch Interessen von Unschuldigen. Bei § 34 StGB ist zu beachten, dass im Rahmen des Notstands die Einholung staatlicher Hilfe vorrangig ist.[74]

IV. Ergebnis

Die Sichtung von Computerdateien auf firmeneigenen Datenträgern, einschließlich des personalisierten Heimlaufwerks, des E-Mail-Accounts etc. durch den Arbeitgeber oder von ihm beauftragter Ermittler fällt in aller Regel[75] nicht unter die Strafvorschrift des § 202a StGB, unabhängig davon, ob ausschließlich dienstliche oder auch private Dateien betroffen sind. Dies befreit natürlich nicht von der Einhaltung datenschutzrechtlicher und arbeitsrechtlicher Vorgaben.[76] Im Hinblick auf § 206 StGB ist die Kontrolle und Weitergabe relevanter dienstlicher E-Mails an sich unbedenklich. Bei der Untersuchung des E-Mail-Verkehrs als Ganzes, sofern dieser auch erlaubte private Kommunikation enthält, ist jedoch bis zu einer strafgerichtlichen (oder gesetzgeberischen) Klärung Vorsicht geboten, selbst bei vorheriger Einholung eines arbeitnehmerseitigen Einverständnisses (trotz entgegenstehender Ansicht des *Verf.*). Dies gilt auch dann, wenn man sich auf die Untersuchung der Kommunikation einzelner bereits verdächtiger Mitarbeiter beschränkt. Im Zweifelsfall wird man auf entsprechende Ermittlungsmaßnahmen verzichten müssen. Handlungssicherheit in Hinblick auf § 206 StGB besteht zur Zeit jedenfalls nur dann, wenn der Arbeitgeber seine Mitarbeiter schon im Vorfeld darauf verweist, private Korrespondenz ausschließlich über private E-Mail-Dienstleister abzuwickeln. Der Lebenswirklichkeit, in der sich dienstliche und private Kommunikation nie ganz trennen lassen,[77] wird diese Konsequenz freilich nur bedingt gerecht. Auch deshalb erscheint es vorzugswürdig, entgegen der wohl h.M.[78] ein im Vorfeld einzuholendes Einverständnis der Arbeitnehmer (im Gegenzug zur Erlaubnis einer gelegentlichen privaten Nutzung des E-Mail-Accounts) ausreichen zu lassen.

[72] Vgl. *Dann/Gastell*, NJW 2008, 2945 (2946); *Klengel/Mückenberger*, CCZ 2009, 81 (84).

[73] Die Anwendbarkeit verneinen deshalb (zum Teil trotz kriminalpolitischer Zweifel) *Altenhain* (Fn. 36), § 206 Rn. 68; *Fischer* (Fn. 14), § 206 Rn. 9; *Hoyer* (Fn. 57), § 206 Rn. 35; *Kargl* (Fn. 36), § 206 Rn. 47; *Lackner/Kühl* (Fn. 14), § 206 Rn. 15; *Lenckner* (Fn. 36), § 206 Rn. 14. Vgl. auch BT-Drs. 13/3609, S. 53. *Sieber* (Fn. 30), Kap. 1 Rn. 542, 586 betont dagegen, dass die strafrechtliche Rechtfertigung weiter reichen kann als die öffentlich-rechtliche Erlaubnis; i.E. ebenso *Altvater* (Fn. 55), § 206 Rn. 80 ff.; *Schmidl*, DuD 2005, 267 (271).

[74] *Dann/Gastell*, NJW 2008, 2945 (2946).

[75] D.h. abgesehen vom Sonderfall der mit gesondertem Kennwortschutz versehenen Privatdateien oder -verzeichnisse.

[76] Vgl. oben I., Fn. 9, 10.

[77] Siehe oben III. 1., man denke auch an Kommunikation unter Kollegen bei dezentralisierten Arbeitsplätzen etc.

[78] Vgl. Fn. 69.