AUFSÄTZE

ANWALTLICHE KOMMUNIKATION PER E-MAIL – NUR VERSCHLÜSSELT?

RECHTSANWALT DR. HENDRIK SCHÖTTLE*

E-Mails sind aus der anwaltlichen Kommunikation mit Mandanten nicht mehr wegzudenken. Der Autor erörtert, ob eine Verschlüsselungspflicht gegeben ist bzw. ob und unter welchen Bedingungen unverschlüsselt kommuniziert werden darf. Hierzu betrachtet er sowohl berufsrechtliche als auch datenschutz- und strafrechtliche Aspekte.

I. E-MAILS UND VERSCHLÜSSELUNG

Auch wenn es eine Plattitüde sein mag: Die E-Mail ist aus der Anwaltskommunikation nicht mehr wegzudenken. Noch 2006 hieß es, die Behauptung, anwaltliche Online-Rechtsberatung sei vielen Kanzleien nicht mehr fremd, wäre „gewiss eine Übertreibung".[1] Heute mutet diese Einschätzung anachronistisch an. Dennoch tun sich Anwaltschaft und Justiz mit der Technik weiterhin schwer. Bei der Kommunikation mit Gerichten und Behörden sind Telefax und Brief das Mittel der Wahl, während in der Unternehmenswelt längst per E-Mail kommuniziert wird.

Nachdem im Jahr 2014 die Datenschutzbeauftragten des Bundes und der Länder auf der 87. Datenschutzkonferenz die Ende-zu-Ende-Verschlüsselung von E-Mail-Kommunikation verlangten,[2] wurde das Thema gleich von zwei Aufsichtsbehörden aufgriffen: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit äußerte in einer Stellungnahme im Januar 2018, E-Mail-Kommunikation, die nicht Ende-zu-Ende verschlüsselt sei, stelle allgemein – und nicht nur für Berufsgeheimnisträger – aus datenschutzrechtlichen Gründen ein ungeeignetes Kommunikationsmittel dar.[3] Ähnlich äußerte sich der sächsische Datenschutzbeauftragte im März 2017 im 8. Tätigkeitsbericht, er halte dies für „eine absolut ungeeignete Kommunikationsform".[4]

Immer wieder wird eine unverschlüsselte E-Mail im Schrifttum hinsichtlich der Sicherung der Vertraulichkeit mit einer Postkarte[5] verglichen. Dieser Vergleich hinkt jedoch, und zwar deswegen, weil die E-Mail rechtlich, aber auch technisch besser geschützt ist als noch vor zehn Jahren. Vor allem jedoch wird oft unterschlagen, dass der Großteil der E-Mail-Kommunikation heute bereits verschlüsselt abgewickelt wird – nämlich mit der so genannten Transportverschlüsselung.

Bei E-Mail-Verschlüsselung ist grundsätzlich zwischen Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung zu unterscheiden:

Bei der *Transportverschlüsselung* werden die E-Mails auf dem Weg vom Client-Rechner des Absenders zum E-Mail-Server des Absenders, von dort zum E-Mail-Server des Empfängers und zum Client-Rechner des Empfängers verschlüsselt, sie liegen auf den Client-Rechnern und auf den Mailservern allerdings unverschlüsselt vor. Damit sind die E-Mails auf dem Weg durch das Internet vor einer Kenntnisnahme Dritter geschützt, nicht jedoch auf den Client-Rechnern und den E-Mail-Servern.[6] Als Standard hat sich bei Transportverschlüsselung das Transport Layer Security-Protokoll (TLS) etabliert. Es ist eine Erweiterung des Secure Sockets Layer-Protokolls (SSL). SSL/TLS wird inzwischen von allen großen E-Mail-Providern in Deutschland unterstützt.[7]

Bei einer *Ende-zu-Ende-Verschlüsselung* werden die E-Mails auf dem Client-Rechner des Absenders verschlüsselt und erst auf dem Client-Rechner des Empfängers wieder entschlüsselt. Auf den E-Mail-Servern liegen die E-Mails nur in verschlüsselter Form vor, auch auf den Client-Rechnern müssen die Texte nach dem Empfang erst entschlüsselt werden, bevor sie gelesen werden können. Als Standards haben sich S/MIME und PGP bzw. GPG etabliert, die jedoch nicht untereinander kompatibel sind.[8] Beide Standards wurden unlängst angegriffen, derzeit kann nicht ohne weiteres davon ausgegangen werden, dass derart verschlüsselte E-Mails vor fremden Augen sicher sind.[9] Eine Alternative dazu kann eine Container-Lösung sein,

* Der Autor ist Rechtsanwalt, Fachanwalt für IT-Recht und Partner bei Osborne Clarke in München und Mitglied im BRAK-Ausschuss Datenschutz.

[1] *Knöfel*, AnwBl. 2006, 77.

[2] S. Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 27.3.2014, www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/87_DSKMenschenrechteElektrischeKommunikation.html (abger. am 18.4.2018).

[3] Stn. des Hamburgischen Beauftragten für Datenschutz und Internetsicherheit, 4, www.datenschutzbeauftragter-info.de/wp-content/uploads/2018/02/schreiben-der-aufsichtsbehoerde.pdf (abger. am 18.4.2018).

[4] 8. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten, 138, www.saechsdsb.de/images/stories/sdb_inhalt/noeb/taetigkeitsberichte/8-TB-Endfassung-Version-5.pdf (abger. am 18.4.2018).

[5] Wie etwa *Kubach/Gutsche*, DSRITB 2014, 585 (587).

[6] Um Missverständnissen vorzubeugen, sei an dieser Stelle klargestellt, dass die an der Übermittlung beteiligten Knotenrechner im Internet keine Möglichkeit haben, den Inhalt der E-Mail einzusehen, da er für den Transport verschlüsselt wurde.

[7] *Schöttle*, BRAK-Magazin 4/2015, 15 ff.

[8] S. BSI, www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Verschluesselung_email_09032017.html.

[9] S. PGP und S/MIME: E-Mail-Verschlüsselung akut angreifbar, https://www.heise.de/security/meldung/PGP-E-Mail-Verschluesselung-akut-angreifbar-4048489.html

bei welcher die Inhalte mit vom E-Mail-Programm unabhängiger Drittsoftware verschlüsselt werden.[10]

II. VERPFLICHTET DIE VERSCHWIEGENHEIT ZUR VERSCHLÜSSELUNG?

Ist nun ein Rechtsanwalt zu einer Verschlüsselung von E-Mails verpflichtet – und wenn ja, zu welcher? Bei der Beantwortung dieser Frage müssen berufsrechtliche, datenschutzrechtliche und strafrechtliche Aspekte betrachtet werden.

1. BERUFSRECHTLICHE ASPEKTE

a) VERSCHWIEGENHEITSPFLICHT § 43a II BRAO

Nach einer Auffassung lassen sich keine besonderen Sicherungspflichten in Bezug auf die E-Mail-Kommunikation aus dem anwaltlichen Berufsrecht ableiten.[11] Weder Berufsrecht noch Strafrecht verpflichten den Anwalt zu besonderen technischen Vorkehrungen. Eine solche Verpflichtung würde sowohl über das „tradierte Verständnis des Anwaltsgeheimnisses“[12] als auch über den Wortlaut des § 43a II BRAO hinausgehen.

Dagegen lässt sich einwenden, dass selbst die fahrlässige Offenbarung berufsrechtlich mit einer anwaltsgerichtlichen Maßnahme i.S.d. § 114 I BRAO geahndet werden kann.[13] Die Frage ist, an welchem Maßstab eine Verletzung von Sicherungspflichten zu messen ist.

Das Bayerische Landesamt für Datenschutzaufsicht hat im Jahr 2014 Mailserver bayerischer Unternehmen automatisiert auf das Vorhandensein von Transportverschlüsselung geprüft und im Fall des Fehlens die betroffenen Unternehmen angeschrieben und Abhilfe verlangt. Es geht davon aus, dass ein fehlendes Angebot von Transportverschlüsselung nicht mehr dem Stand der Technik entspricht.[14] In der Tat bieten nahezu alle großen E-Mail-Provider inzwischen Transportverschlüsselung an, einige von ihnen verlangen den Einsatz inzwischen sogar zwingend von ihren Kunden.[15]

Aus den vorgenannten Gründen ist eine Pflicht des Anwalts zur Verwendung einer *Transportverschlüsselung* wohl zu bejahen. Diese kann allerdings nur so weit greifen, wie auch die Gegenseite eine solche Verschlüsselung unterstützt. Unterstützt der E-Mail-Provider des Mandanten keine solche Verschlüsselung, hat der Anwalt zumindest alles getan, um eine Transportverschlüsselung anzubieten. Letztlich obliegt die Auswahl eines zuverlässigen E-Mail-Providers, welcher Verschlüsselungsmaßnahmen anbietet, dem Mandanten selbst.

Wie sieht es nun bei *Ende-zu-Ende-Verschlüsselung* aus? Besteht auch eine Pflicht, eine solche Technologie einzusetzen? Anders als bei einer Transportverschlüsselung ist sowohl die Einrichtung als auch die Benutzung eines solchen Systems wesentlich aufwändiger.

Zum einen gibt es keinen einheitlichen Standard – es muss mit dem Kommunikationspartner zunächst geklärt werden, welche Technik eingesetzt werden soll. Auch werden, anders als bei Transportverschlüsselung, in der Regel keine Einwegschlüssel eingesetzt, die automatisch generiert werden. Die Schlüssel der Beteiligten müssen – soweit sie nicht über einen Key-Server bezogen werden – vielmehr manuell eingerichtet und ausgetauscht werden. Anders als bei Transportverschlüsselung, die vom E-Mail-Provider des Mandanten in der Regel schon ohne Zutun des Mandanten angeboten wird und eingesetzt werden kann, muss der Mandant beim Einsatz von Ende-Zu-Ende-Verschlüsselung also selbst tätig werden.

Zum anderen wirft eine solche Verschlüsselung erhebliche technische Fragen auf – vor allem in Bezug auf eine ordnungsgemäße Handaktenführung und in Bezug auf die Durchsuchbarkeit eingehender E-Mails. Der Anwalt, der nicht ausschließlich papierbasiert arbeitet, wird E-Mails, die ihn Ende-zu-Ende verschlüsselt erreicht haben, in seinem IT-System auch entschlüsselt aufbewahren müssen, um sie wiederfinden und durchsuchen zu können. Zudem muss er dafür Sorge tragen, dass derartige E-Mails auch in einer Handakte zu finden sind. Werden Handakten elektronisch geführt, müssen die E-Mails also entschlüsselt und zur jeweiligen Handakte hinzugefügt werden.

Dann aber schrumpft der Sicherheitsgewinn gegenüber der Transportverschlüsselung erheblich: Denn auf den Systemen des Anwalts liegen die E-Mails dann auch in entschlüsselter Form vor. Allein in Bezug auf den E-Mail-Provider ist dann noch gegenüber der Transportverschlüsselung ein Vorteil gegeben. Denn dort lägen die E-Mails bei einer Transportverschlüsselung unverschlüsselt vor, bei der Ende-zu-Ende-Verschlüsselung hingegen verschlüsselt. Der E-Mail-Provider ist jedoch ohnehin vom Telekommunikationsgeheimnis nach § 88 TKG erfasst und dürfte in bei ihm unverschlüsselt abgelegte E-Mails nur einsehen, soweit dies zur Leistungserbringung erforderlich ist. Und schließlich setzen realistische Szenarien eines Hackings oftmals beim Empfänger der Nachricht selbst an und nicht beim meist besser geschützten E-Mail-Provider – also bei dem Rechtsanwalt, auf dessen Servern die Nachrichten aus Archivierungsgründen auch entschlüsselt abgelegt sind, oder beim Mandanten.

Schließlich darf nicht vergessen werden, dass auch Ende-zu-Ende-Verschlüsselung anfällig ist für Sicherheitslücken. Erst vor kurzem wurden mehrere Sicherheitslücken in den Protokollen S/MIME und PGP entdeckt, die unter dem Schlagwort „Efail“ bekannt wurden; die beteiligten Forscher gingen so weit, den insbesondere im Firmenumfeld eingesetzten Standard S/MIME für „unrettbar kaputt“ zu erklären.[16] Damit bliebe allen-

[10] Näher *Schöttle*, BRAK-Magazin 4/2015, 15 ff.
[11] *Härting*, NJW 2005, 1248 ff.
[12] *Härting*, NJW 2005, 1248 (1249).
[13] *Henssler*, in Henssler/Prütting, BRAO, 3. Aufl. 2010, § 43a Rn. 119.
[14] BayLDA, Pressemitt. v. 9.9.2014, www.lda.bayern.de/media/pm2014_12.pdf.
[15] S. Golem v. 31.3.2014: E-Mail nur noch mit TLS, www.golem.de/news/verschluesselung-ab-heute-e-mail-nur-noch-mit-tls-1403-105487.html.
[16] S. PGP und S/MIME: E-Mail-Verschlüsselung akut angreifbar, https://www.heise.de/security/meldung/PGP-E-Mail-Verschluesselung-akut-angreifbar-4048489.html

falls noch die Verwendung der bereits erwähnten Container-Lösung, um eine sichere Ende-zu-Ende-Verschlüsselung zu gewährleisten.

Die Herleitung einer Pflicht zum Einsatz von Ende-zu-Ende-Verschlüsselung scheitert nach einer Auffassung an der Berufsfreiheit des Rechtsanwalts, Art. 12 I GG,[17] denn ohne die einfache, unverschlüsselte E-Mail-Kommunikation ist der Berufsalltag nicht mehr vorstellbar. Es sprechen angesichts der vorstehenden Ausführungen gute Argumente dafür, dass eine Pflicht zur Verwendung von Ende-zu-Ende-Verschlüsselung nicht aus § 43a II BRAO hergeleitet werden kann.

b) AUSNAHMETATBESTAND SOZIALADÄQUANZ

Die Benutzung der nicht Ende-zu-Ende verschlüsselten E-Mail-Kommunikation wohl sozialadäquat i.S.v. § 2 III lit. c BORA. Diese Norm ist als Satzungsrecht nicht in der Lage, die in § 43a II BRAO normierte Verschwiegenheitspflicht aufzuweichen oder zu erweitern. Allerdings wird man die Norm zur Konkretisierung des Umfangs der Verschwiegenheitspflicht heranziehen können.[18] Zumindest wäre es sehr überraschend, wenn das, was die BORA als zulässige negative Konkretisierung der Verschwiegenheitspflicht ansieht, nicht für eine Auslegung der BRAO statthaft wäre.[19]

Das Merkmal der Sozialadäquanz setzt beim Verhalten des Anwalts im Rahmen der Arbeitsabläufe in der Kanzlei an. Dieses Verhalten muss objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entsprechen. Mit der Regelung sollte die Rechtsgrundlage für die Zulässigkeit von Outsourcing (nicht nur für IT-Leistungen) geschaffen werden, dies vor dem Hintergrund, dass der Anwalt sich den modernen Kommunikationsmöglichkeiten nicht entziehen kann.[20] Was einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise entspricht, ist ausschließlich objektiv zu bestimmen.[21] Man kann nicht ernsthaft bestreiten, dass der Versand von E-Mails üblich und von der Allgemeinheit akzeptiert ist. Damit sprechen gute Argumente dafür, dass die Kommunikation per E-Mail, dem „Versandmittel Nr. 1“,[22] sozialadäquat im Sinne der Vorschrift ist.

2. DATENSCHUTZRECHTLICHE ASPEKTE

Die Aufsichtsbehörden folgen der Ansicht, die Anwendung des BDSG (und künftig dann auch der DS-GVO) durch das anwaltliche Berufsrecht werde nicht verdrängt, sondern lediglich ergänzt.[23] Ohne die Diskussion um das Verhältnis zwischen anwaltlichem Berufsrecht und Datenschutzrecht zu vertiefen,[24] soll an dieser Stelle von einer Anwendbarkeit der datenschutzrechtlichen Regelungen auf die Anwaltschaft ausgegangen werden.

Der Hamburgische und der Sächsische Datenschutzbeauftragte halten die Versendung von unverschlüsselten E-Mails im Hinblick auf den technisch-organisatorische Datenschutz für ein ungeeignetes Kommunikationsmittel.[25] Die datenschutzrechtlichen Bedenken betreffen, wenn sie auch auf Rechtsanwälte angewendet werden, insoweit nicht nur diese als Berufsgeheimnisträger, sondern sämtliche Adressaten des Datenschutzrechts. Der seit dem 1.1.2018 geltende neue § 2 VII BORA ist insoweit deklaratorisch[26] und ändert an der bestehenden Rechtslage nichts. Nach der wohl herrschenden Meinung fand sowohl der bis zum 25. Mai 2018 gegolten habende § 9 BDSG-alt als auch die nunmehr geltenden Art. 25 und 32 DS-GVO auf Rechtsanwälte Anwendung.[27]

a) ENDE-ZU-ENDE-VERSCHLÜSSELUNG ALS STAND DER TECHNIK?

Regelungen zu technisch-organisatorischem Datenschutz wurden bis zum 25.5.2018 von § 9 BDSG-alt, seitdem dann von Art. 5 I f und Art. 25, 32 DS-GVO aufgestellt. In diesen Normen wird Verschlüsselung als eine Maßnahme genannt, die nach dem Stand der Technik erfolgen soll. Auf eine konkrete Festlegung verzichten die Normen aus nachvollziehbaren Gründen.

Der Hamburgische Beauftragte für Datenschutz und Internetsicherheit geht wohl zumindest von der Notwendigkeit einer Transportverschlüsselung[28] aus, auch wenn seiner Auffassung nach eine Ende-zu-Ende-Verschlüsselung zu bevorzugen sei. Der Sächsische Datenschutzbeauftragte spricht allgemein von Verschlüsselung, nennt dann aber PGP als eine Verschlüsselungsart, die er anbietet.[29]

Für die Beurteilung der Frage, welche Maßnahmen nun verpflichtend angenommen werden können, ist einerseits zu prüfen, was bei dem jeweiligen Verfahren als Stand der Technik angesehen wird, und andererseits, ob diese Maßnahme hinsichtlich des Aufwands auch angemessen ist.[30] Weder BDSG noch DS-GVO definieren den Stand der Technik. Nach wohl herrschender Ansicht sind mit dem Stand der Technik diejenigen Technologien gemeint, die auf gesicherten Erkenntnissen beruhen und in der Praxis jeweils bereits in ausreichendem Maß zur Verfügung stehen, um angemessen

[17] *Degen/Emmert*, in: dies., Elektronischer Rechtsverkehr, 1. Aufl. 2016, Rn. 440.
[18] BeckOK-BORA/*Römermann/Praß*, 19. Ed. 1.3.2018, § 2 Rn. 7.
[19] Vgl. dazu BeckOK-BORA/*Römermann/Praß*, § 2 Rn. 2b.
[20] BeckOK-BORA/*Römermann/Praß*, § 2, Rn. 35a ff.
[21] BeckOK-BORA/*Römermann/Praß*, § 2, Rn. 35c.
[22] *Degen/Emmert*, in: dies., Rn. 438.
[23] So z.B. 25. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, 97 f., www.datenschutz-hamburg.de/uploads/media/25._Taetigkeitsbericht_Datenschutz_2014-2015_HmbBfDI_01.pdf (abger. am 18.4.2018).
[24] S. dazu auch *Schöttle*, AnwBl. 2005, 740 ff.
[25] Stn. des Hamburgischen Beauftragten für Datenschutz und Internetsicherheit, 3 sowie 8. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten, 138.
[26] BeckOK-BORA/*Römermann/Praß*, Rn. 43a.
[27] Vgl. *Kazemi*, NJW 2018, 443.
[28] Stn. des Hamburgischen Beauftragten für Datenschutz und Internetsicherheit, 3 (abger. am 18.4.2018).
[29] 8. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten, 138 (abger. am 18.4.2018).
[30] BayLDA, Sicherheit der Verarbeitung – Art. 32 DS-GVO, S. 2, www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf (abger. am 18.4.2018).

umgesetzt zu werden.[31] Nach Art. 25 I, Art. 32 I DS-GVO fließen in die anschließende Abwägung noch die Kosten der Implementierung, Art, Umfang, Umstände und Zwecke der Verarbeitung ein, sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken.

Transportverschlüsselung (TLS oder SSL) hat sich mittlerweile wohl als Standard etabliert,[32] kann also als Stand der Technik bezeichnet werden und lässt sich ohne weiteres in die vorhandene Infrastruktur implementieren. Eine Ende-zu-Ende-Verschlüsselung hingegen geht mit einem erheblich höheren Implementierungsaufwand einher.[33]

Dies liegt, wie ausgeführt, daran, dass sowohl der Versender als auch der Empfänger die gleiche Technik benutzen müssen, da die unterschiedlichen existierenden Verschlüsselungsmethoden in der Regel nicht miteinander kompatibel sind. Darüber hinaus ist die Verwendung von Ende-zu-Ende-Verschlüsselung, etwa über PGP oder S/MIME nicht ganz trivial und verlangt vertiefte Kennnisse von den an der Kommunikation Beteiligten.[34] Dies erkennt auch die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme vom 11.4.2018 an.[35] Sie geht davon aus, dass die Ende-zu-Ende-Verschlüsselung zu bevorzugen sei und dass ein öffentliches Interesse daran bestehe; gleichwohl verlangt sie nicht, dass sämtliche Kommunikation derart verschlüsselt werden müsse. Die Verschlüsselung müsse standardisiert, stark und effizient sein. Die Artikel-29-Datenschutzgruppe regt in ihrer Stellungnahme die Entwicklung und Förderung einer solchen Ende-zu-Ende-Verschlüsselung an – was gleichzeitig zeigt, dass diesbezüglich offensichtlich noch Handlungsbedarf besteht.

Nur der Vollständigkeit halber sei an dieser Stelle darauf hingewiesen, dass auch mit einseitig implementierten Maßnahmen eine Ende-zu-Ende-Verschlüsselung erreicht werden kann, wie etwa mit der Verwendung von Container-Dateien von Verschlüsselungstools oder dem Angebot einer browserbasierten Web-Client-Lösung.

b) KEINE SPEZIELLEN PFLICHTEN FÜR BERUFSGEHEIMNISTRÄGER NACH DS-GVO

Des Weiteren stellt sich die Frage, ob die Pflicht zur Verwendung von Ende-zu-Ende-Verschlüsselung – soweit man sie überhaupt aus der DS-GVO herleiten kann – nur für Rechtsanwälte und gegebenenfalls andere Berufsgeheimnisträger gelten soll oder auch für andere Personen. Der Hamburgische Datenschutzbeauftragte[36] leitet die Pflicht zur Ende-zu-Ende-Verschlüsselung für Rechtsanwälte ausschließlich aus dem Datenschutzrecht ab.[37] Das allgemeine Datenschutzrecht legt allerdings keine besonderen berufsrechtlichen Anforderungen eines Anwalts fest. Auch zählen Mandatsinformationen nicht zu den sensiblen Daten, die in Art. 9 DS-GVO geregelt sind.

Allein aus der DS-GVO selbst ergeben sich damit keine spezifischen Pflichten für Rechtsanwälte, sie können allenfalls implizit aus den Normen hergeleitet werden. Leitet man eine Pflicht zur Verwendung von Ende-zu-Ende-Verschlüsselung aus dem Datenschutzrecht ab, so dürfte diese kaum auf Rechtsanwälte beschränkt sein, sondern müsste dann auch für andere Adressaten des Datenschutzrechts gelten, wie etwa die Datenschutzaufsichtsbehörden selbst.

3. STRAFRECHTLICHE BEWERTUNG

Zum Teil wird eine Pflicht zur Verwendung von Ende-zu-Ende-Verschlüsselung der E-Mail-Kommunikation aus § 203 StGB hergeleitet.[38] Der Versand einer nicht Ende-zu-Ende verschlüsselten E-Mail erfüllt jedoch nicht dessen Tatbestand.

Zwar kann § 203 StGB als unechtes Unterlassungsdelikt i.S.d. § 13 StGB verwirklicht werden. So kann das offene Liegenlassen einer Akte und die Nichthinderung einer Einsichtnahme darin den Tatbestand des § 203 StGB erfüllen.[39] Allerdings genügt das bloße Gewähren der Möglichkeit einer Kenntnisnahme für § 203 StGB nicht, weil es auf die Kenntnisnahme selbst ankommt. In der Literatur wird vertreten, dass eine Offenbarung dann ausscheidet, wenn die Kenntnisnahme strafbewehrt und das Geheimnis dadurch rechtlich geschützt ist.[40] Ob dies wirklich in einer solchen Allgemeinheit gelten kann, mag dahinstehen.[41]

An dieser Stelle mag jedoch wieder das Kriterium der Sozialadäquanz herangezogen werden: So, wie sich der Rechtsanwalt darauf verlassen kann, dass ein Postbeförderungsdienst die ihm anvertrauten Briefe nicht öffnet, so wird man sich sicherlich auch darauf verlassen dürfen, dass ein E-Mail-Provider ebenso handelt. Denn selbst unverschlüsselte E-Mails sind seit inzwischen mehr als zehn Jahren vor einer unbefugten Kenntnisnahme strafrechtlich nach § 202b StGB geschützt. Daneben greift außerdem das Post- und Fernmeldegeheimnis des § 206 StGB sowie das Telekommunikationsgeheimnis nach § 88 TKG für die E-Mail-Provider. Damit ist die E-Mail auf dem Weg vom Absender zum Empfänger aus strafrechtlicher Sicht grundsätzlich lückenlos geschützt.

Darüber hinaus fordert § 13 StGB für die Gleichstellung des Unterlassens mit dem aktiven Tun, dass „das Unterlassen der Verwirklichung des gesetzlichen Tat-

[31] *Hartung*, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 25 DS-GVO Rn. 21 m.w.N.
[32] S. oben I 1 a sowie *Schöttle*, BRAK-Magazin 4/2015, 15 ff.
[33] *Kubach/Gutsche*, DSRITB 2014, 585 (590).
[34] *Kubach/Gutsche*, DSRITB 2014, 585 (590).
[35] Artikel-29-Datenschutzgruppe, Statement on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU, ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51026.
[36] Stn. des Hamburgischen Beauftragten für Datenschutz und Internetsicherheit, 1 (abger. am 18.4.2018).
[37] Für eine rein berufsrechtliche Herleitung dürfte er auch nicht zuständig sein.
[38] 8. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten, 138.
[39] *Fischer*, StGB, 65. Aufl. 2018, § 203 Rn. 35.
[40] *Lewinski*, BRAK-Mitt. 2004, 12.
[41] So wird es in der Regel sicherlich nicht ausreichen, sich auf den Tatbestand des Hausfriedensbruchs zurückzuziehen, anstatt die Kanzleiräume abzuschließen.

bestandes durch ein Tun entspricht".[42] Dementsprechend, legt man als Maßstab die „Vergleichbarkeit im Unwert" zugrunde, wird zumindest zu verlangen sein, dass der Schweigepflichtige damit gerechnet habe, der Dritte werde vom Inhalt des Geheimnisses tatsächlich Kenntnis nehmen. Käme es darauf nicht an, würde also für eine Erfüllung des Straftatbestands die tatsächliche Kenntnisnahme genügen, wäre damit auch die Briefpost und die Kommunikation per Telefax für den Anwalt zu riskant und im Ergebnis nicht mehr einsetzbar: denn käme es etwa zu einer unbefugten Kenntnisnahme eines Telefax (was bei den oft von mehreren Personen genutzten Faxanschlüssen und den offen wie eine Postkarte im Faxgerät liegenden empfangenen Ausdrucken durchaus wahrscheinlicher ist als bei einem einer einzigen Personen zugordneten E-Mail-Postfach), dann wäre in einem solchen Fall bereits der Straftatbestand erfüllt.

Die Vollendung liegt jedenfalls nur dann vor, wenn ein Dritter vom Inhalt des Geheimnisses tatsächlich Kenntnis genommen hat.[43] Es kann auch keine Analogie mit dem bloßen Herumliegenlassen von Akten gezogen werden. Der Server des E-Mail-Anbieters dürfte eher mit dem Aktenschrank im Büro zu vergleichen sein. Man wird nicht per se damit rechnen müssen, dass beliebige Dritte auf die Informationen auf dem Server zugreifen.

Im Ergebnis sprechen gute Argumente dafür, dass das Fehlen von Ende-zu-Ende-Verschlüsselung bei der E-Mail-Kommunikation durch Berufsgeheimnisträger bereits den objektiven Tatbestand des § 203 I StGB nicht erfüllt.

III. EINWILLIGUNG IN DIE UNVERSCHLÜSSELTE E-MAIL-KOMMUNIKATION

1. ERFORDERLICHKEIT DER EINWILLIGUNG

Obgleich wohl eine objektive Pflicht, E-Mail-Kommunikation Ende-zu-Ende zu verschlüsseln nicht angenommen werden kann, bestimmt dennoch der Mandant als „Herr des Geheimnisses" sowohl das „Ob" als auch das „Wie" des Geheimnisses.[44] Denn nur der Mandant kann das subjektive Schutzbedürfnis der von ihm übermittelten Informationen festlegen. Nach einer Auffassung reicht die Transportverschlüsselung nicht aus, um sämtliche Risiken der Kenntnisnahme auszuräumen,[45] daher brauche man eine Einwilligung des Mandanten unter Aufklärung über die Risiken der unverschlüsselten E-Mail-Kommunikation. Wie vorstehend ausgeführt, sprechen gute Argumente dafür, dass eine Transportverschlüsselung durchaus geeignet ist, ein ausreichendes Sicherheitsniveau zu bewirken. Dennoch soll nachfolgend betrachtet werden, wann eine solche Einwilligung angenommen werden kann.

a) KONKLUDENTE EINWILLIGUNG

Grundsätzlich ist eine konkludente Einwilligung in die unverschlüsselte E-Mail-Kommunikation dadurch möglich, dass der Mandant mit seinem Rechtsanwalt selbst unverschlüsselt per E-Mail solche Informationen übermittelt, die ein Mandatsgeheimnis darstellen.[46] Zum Teil wird vertreten, dass die vom Mandanten für den Versand genutzte E-Mail-Adresse oder Faxnummer ohne weiteren Abklärung nicht als „Mandanten"-Anschrift benutzt werden darf, weil dann nicht gewährleistet sei, dass keine Dritten von der Kommunikation Kenntnis erhalten.[47] Dies mag wohl in Bezug auf eine Telefaxnummer zutreffend sein. Bezüglich eines E-Mail-Postfachs dürfte aber grundsätzlich davon ausgegangen werden, dass nur eine einzelne Person darauf Zugriff hat, sofern sich nicht klar aus der E-Mail-Adresse ergibt, dass es sich um eine Funktionsadresse handelt (etwa info@unternehmen.de).

Im Ergebnis wird man annehmen können, dass der Mandant, welcher den Anwalt per E-Mail kontaktiert, gleichzeitig darin einwilligt, auf diesem Wege auch eine Antwort vom Anwalt zu bekommen. Nur dann, wenn sich aus dem Kontext eindeutig etwas anderes ergibt, mag man annehmen, dass der Mandant mit einer Kommunikation nicht einverstanden ist.

b) WANN BESTEHT EINE AUFKLÄRUNGSPFLICHT?

Es ist allgemein für jede Ausnahme und Befreiung von der Verschwiegenheitspflicht zwingend erforderlich, dass der Mandant die dafür erforderliche Einsichts- und Prüfungsfähigkeit besitzt.[48] Zwar handelt es sich bei einer Einwilligung nicht um die Entbindung von der Verschwiegenheitspflicht, sondern um die Konkretisierung ihrer subjektiven Reichweite. Allerdings kann nichts anderes in Bezug auf die E-Mail-Kommunikation gelten. Der Mandant muss sich also der Risiken der E-Mail-Kommunikation bewusst sein.

Nach einer Auffassung genügt der Anwalt nur dann seinen Sorgfaltspflichten, wenn er im Rahmen einer Einwilligungserklärung auf die bestehenden Risiken im Rahmen der E-Mail-Kommunikation hingewiesen hat.[49] Es stellt sich allerdings die Frage, ob eine solche Hinweispflicht angesichts der Verbreitung der E-Mail-Kommunikation noch zeitgemäß ist. Heutzutage scheint es geradezu das Mittel der Wahl zu sein, eine schützenswerte Person aufgrund von legaldefinierten oder gesetzlich abgeleiteten Informationspflichten mit Hinweisen zu beglücken, so dass man zunächst auch hier geneigt sein mag, bei Wahl des sichersten Weges ebenfalls eine solche Information zu verlangen.

[42] *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, 5. Aufl. 2017, § 203 Rn. 19a.
[43] *Dannecker*, in: Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2017, § 203 Rn. 51 m.w.N.
[44] Vgl. z.B. *Henssler*, in: Henssler/Prütting, § 43a Rn. 62 ff.
[45] *Sorge*, NJW-Beil. 2016, 100 ff.; *Kubach/Gutsche*, DSRITB 2014, 585 ff.
[46] *Träger*, in: Feuerich/Weyland, BRAO, 9. Aufl. 2016, § 43a Rn. 25b; *Henssler*, in: Henssler/Prütting, § 43a Rn. 68 f.; dagegen aber *Kubach/Gutsche*, DSRITB 2014, 585 (592).
[47] *Träger*, in: Feuerich/Weyland, § 43a, Rn. 25b.
[48] *Groß*, in: Schnitzer, Anwaltshdb. Familienrecht, 4. Aufl. 2014, § 2 Rn. 18.
[49] *Degen/Emmert*, in: dies., Rn. 447.

Realistisch betrachtet, dürfte dies jedoch nicht (mehr) notwendig sein. Laut einer aktuellen Statistik wurden im Jahr 2017 in Deutschland 771 Milliarden E-Mails verschickt – im Schnitt mehr als 9.300 pro Einwohner; der Studie zufolge sind mehr als 90 % der Deutschen ab 14 Jahren online.[50] Ganz anders sieht es beim Telefax aus: Nach einer Studie aus dem Jahr 2015 nutzte nur jeder fünfte Erwerbstätige ein Telefax im beruflichen Umfeld[51] – die Tendenz dürfte fallend und im privaten Umfeld noch dramatisch niedriger sein. Gerade die jüngere Generation wird das Fax nur noch als merkwürdig schlecht aufgelösten, teuren und umständlichen Web-Service zum Versand von PDF-Dateien an Telefonnummern kennen. Ihr wird kaum bewusst sein, dass bei der Mehrzahl der Gegenstellen in Behörden und Gerichten tatsächlich Hardware steht, die bedrucktes Papier produziert, welches dann über diverse Schreibtische wandert und von vielen Augen gelesen wird.

Nüchtern betrachtet wird man also davon ausgehen können, dass die überwiegende Mehrheit mit E-Mail als Kommunikationsdienst vertraut ist und dass dementsprechend auch keine Aufklärung über damit verbundene Risiken erforderlich ist. Eher wird man verlangen können, über mangelnde Vertraulichkeit beim der Allgemeinheit kaum noch bekannten Telefax zu informieren als über die Risiken eines allgemein etablierten Kommunikationsdienstes wie der E-Mail. Teilt also ein Mandant im Rahmen eines Mandatsverhältnisses seinem Anwalt eine E-Mail-Adresse mit, sprechen gute Argumente dafür, dass der Anwalt mit seinem Mandanten per E-Mail kommunizieren kann. Dies gilt wie ausgeführt, erst recht, wenn der Mandant seinen Anwalt per E-Mail kontaktiert.

Eine Informationspflicht seitens des Rechtsanwalts mag allenfalls dann noch begründet sein, wenn der Rechtsanwalt situationsbedingt Anhaltspunkte dafür hat, dass der Mandant im Einzelfall nicht in der Lage ist, Sicherheitsrisiken der E-Mail-Kommunikation richtig einzuschätzen, die sich aus einer konkreten Gefährdungslage oder aufgrund besonderer Sensibilität der übermittelten Informationen ergeben. Dies wird allerdings nur in seltenen Fällen angenommen werden können, etwa wenn konkret mit einer Überwachung der Kommunikation des Mandanten durch Ermittlungsbehörden zu rechnen ist.

2. UNMÖGLICHKEIT DER EINWILLIGUNG?

Der Hamburgische Datenschutzbeauftragte geht davon aus, dass bei den sensiblen Daten auch die Einwilligung in die elektronische Übertragung ohne Verschlüsselung nicht möglich sei, da die technisch-organisatorischen Maßnahmen nach § 9 BDSG oder Art. 32 I DS-GVO nicht verzichtbar seien.[52] Diese Auffassung dürfte allerdings den Schutz der Betroffenen zu stark strapazieren und einen unzulässigen Eingriff in die Handlungsfreiheit der Betroffenen darstellen – vor allem vor dem Hintergrund, dass die Abwicklung von Mandantenkommunikation per unverschlüsselter E-Mail alltäglich ist. Eine generelle Ablehnung der Einwilligungsfähigkeit dürfte allenfalls in krassen Ausnahmefällen gegeben sein, etwa wenn dem Mandanten nicht klar ist, was er tut.

Das Mandatsgeheimnis ist kein abstraktes Schutzgut, welches der Disposition durch den Mandanten entzogen ist. Es dient allein seinen Interessen und endet dort, wo der Mandant dies wünscht. Schließlich ist es dem Mandanten ja auch unbenommen, sich mit der von seinem Rechtsanwalt vertretenen Sache an die Öffentlichkeit zu wenden. Wenn schon dies nicht aufgrund des Mandatsgeheimnisses verboten ist, dann muss dies erst recht bei weitaus geringeren Beeinträchtigungen wie einer möglichen, unbefugten Kenntnisnahme gelten. Dies gilt auch in datenschutzrechtlicher Sicht: Dem Betroffenen steht es selbstverständlich auch frei, ihn betreffende personenbezogene Daten zu veröffentlichen, damit kann dort nichts anderes gelten.

3. EINWILLIGUNG BETROFFENER DRITTER

Nach wohl herrschender Meinung reicht das Datenschutzrecht weiter als die berufsrechtliche Verschwiegenheitspflicht, weil es auch den Schutz von Gegnern des Mandanten und der sonstigen Dritten gewährleistet.[53] Daher stellt sich die Frage, ob hinsichtlich der Kommunikation per E-Mal eine datenschutzrechtliche Einwilligung etwa eines Prozessgegners oder von anderen Dritten erforderlich ist, deren Daten per E-Mail übermittelt werden.

Zumindest dann, wenn der Anwalt einen Kommunikationsweg anbietet, der nach dem Stand der Technik geschützt ist und der letztlich dem Merkmal der Sozialadäquanz genügt, dürfte eine Einwilligung entbehrlich sein. Wie ausgeführt, kann es durchaus auch bei Kommunikation auf anderen Wegen, etwa per Post oder Telefax, zu einer Kenntnisnahme durch Dritte kommen, gerade das Telefax ist durch seine technische Gestaltung prädestiniert für eine Kenntnisnahme durch Dritte, zumindest dann, wenn es Ausdrucke in physischer Form erstellt. Dennoch wird nicht ernsthaft verlangt, sämtliche Kommunikation per Telefax aus datenschutzrechtlichen Gründen einzustellen. Für die Kommunikation per E-Mail kann zumindest dann nichts anderes gelten, wenn sie nach dem Stand der Technik geschützt ist. Dazu dürfte, wie ausgeführt, eine Transportverschlüsselung gehören, zumindest ist diese anzubieten. Im Ergebnis ist eine Einwilligung Dritter also dann entbehrlich, wenn die E-Mail per Transportverschlüsselung geschützt ist.

[50] S. www.heise.de/newsticker/meldung/771-Milliarden-Nachrichten-E-Mail-Volumen-in-Deutschland-2017-auf-Rekordwert-3961288.html.

[51] http://www.faz.net/aktuell/wirtschaft/faxgeraet-ist-in-deutschlands-bueros-immer-noch-beliebt-13806252.html.

[52] Stn. des Hamburgischen Beauftragten für Datenschutz und Internetsicherheit, 2.

[53] So auch der Hamburgische Datenschutzbeauftragte in seiner Stellungnahme, 98 m.w.N.

IV. FAZIT

Eine Transportverschlüsselung stellt derzeit wohl den Stand der Technik dar. Sie ist im Hinblick auf die datenschutzrechtlichen Anforderungen wohl das Mittel der Wahl für sämtliche Adressaten des Datenschutzrechts und somit auch für die Anwaltschaft.

Anders sieht es bei der Ende-zu-Ende-Verschlüsselung aus. Bei dem derzeitigen Stand der Technik und angesichts der aktuellen Rechtslage sprechen gute Argumente gegen das Bestehen einer Pflicht zur Verwendung einer Ende-zu-Ende-Verschlüsselung für Rechtsanwälte als Berufsgeheimnisträger. Ohne die Mitwirkung des Mandanten ist eine Ende-zu-Ende-Verschlüsselung momentan nicht möglich, einen einheitlichen Standard gibt es nicht. Darüber hinaus ist der Sicherheitsgewinn bei der Anwendung von Ende-zu-Ende-Verschlüsselung gering. Denn der Client-Rechner, auf welchem die E-Mail unverschlüsselt vorliegt, ist im Fall eines Angriffs das lohnendste und damit das wahrscheinlichste Angriffsziel. Damit ist die Ende-zu-Ende-Verschlüsselung nur so sicher wie die Client-Rechner von Anwalt und Mandant – letztere sind das schwächste Glied in der Kette.

In der Nutzung oder der Angabe der E-Mail-Adresse zur Kontaktaufnahme durch den Mandanten ist eine konkludente Einwilligung in die Nutzung dieses Kommunikationswegs durch den Mandanten zu sehen, zumindest dann, wenn der Anwalt eine Transportverschlüsselung anbietet. Eine Aufklärung über die Risiken der E-Mail-Kommunikation ist angesichts der weiten Verbreitung der E-Mail nur dann erforderlich, wenn der Anwalt konkrete Anhaltspunkte dafür hat, dass der Mandant im konkreten Fall die Sicherheitsrisiken der E-Mail-Kommunikation nicht richtig einzuschätzen vermag.

Was bedeutet das für den Rechtsanwalt in der Praxis? Er sollte sicherstellen, dass der von ihm gewählte E-Mail-Provider Transportverschlüsselung anbietet.

Bei dem Anwalt, der keine Ende-zu-Ende verschlüsselte Kommunikation anbietet, ist ein Hinweis auf die fehlende Möglichkeit einer Ende-zu-Ende-Verschlüsselung vor der Mandatsaufnahme sinnvoll, aber nicht zwingend erforderlich. Sollte der Mandant damit nicht einverstanden sein, kann er mit dem Anwalt auf anderen Kanälen kommunizieren oder von der Aufnahme einer Mandatsbeziehung absehen.

Will der Anwalt zusätzliche Sicherungsmaßnahmen anbieten, kann er dies in Form einer Ende-zu-Ende-Verschlüsselung tun, entweder integriert in vorhandene E-Mail-Clients oder als eigenständige Lösung, etwa in Form von Containerdateien.

Will der Anwalt auf Nummer sicher gehen, kann er in Zweifelsfällen eine ausdrückliche Einwilligung einholen, auch wenn dies aus rechtlicher Sicht in der Regel nicht erforderlich sein dürfte.