Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

9
K&R

Der Betrieb einer Facebook-Seite ist ein „schwerer datenschutzrechtlicher Verstoß“
Prof. Dr. Alexander Roßnagel

565 Die Guidelines des EDSA zur Bußgeldzumessung nach der DSGVO
Dr. Timo Handel

571 Das Phänomen der politischen Online-Werbung im Zeitalter der Digitalisierung
Florian Flamme und **Amelie Mehlan**

577 Vom Irrglauben an die Geheimhaltung durch TLS bei E-Mails
Dr. Florian Deusch und **Prof. Dr. Tobias Eggendorfer**

581 Update Informationsfreiheits- und Transparenzrecht 2021/2022
Prof. Dr. Jens M. Schmittmann

587 Anpassung der Leitlinien des GEREK an Rechtsprechung des EuGH zu Nulltarifangeboten
Dr. Marc Salevic und **Rebecca Trampe-Berger**

589 Länderreport Schweiz
Lukas Bühlmann

593 **BVerfG:** Grundrechtsverstoß durch fehlerhafte Auslegung eines urheberrechtlichen Unterlassungstitels

596 **BGH:** YouTube II: Video-Sharing-Plattform muss angemessene Maßnahmen gegen Urheberrechtsverletzung ergreifen

605 **BGH:** uploaded II: Sharehoster mit einschlägigem Geschäftsmodell haftet für Urheberrechtsverletzungen Dritter

609 **BGH:** cusanus.de: Kennzeichenmäßige Verwendung einer Domain

623 **BGH:** Grundpreisangabe im Internet muss in unmittelbarer Nähe des Preises stehen

636 **VG Osnabrück:** Rechtswidrige Pressemitteilung der Staatsanwaltschaft zu Ermittlungsverfahren
mit Kommentar von **Martin W. Huff**

25. Jahrgang **September 2022** Seiten 565 – 644

dfv Mediengruppe · Frankfurt am Main

wie etwa dem der verschiedenen Akteur:innen, weiter eingeschränkt, allerdings ist nicht ausgeschlossen, dass die vage Definition der politischen Werbung unvorhersehbare Folgen in der Rechtspraxis haben könnte.

Bei einer derart weiten Definition ist es naheliegend, dass Werbeinhalte, die aktuell als Wirtschaftswerbung einzustufen wären, zukünftig auch als politische Werbung aufzufassen sind.[77] Ebenso ist denkbar, dass durch die Verordnung in ihrer jetzigen Entwurfsfassung ein wesentlicher Teil der Vorgänge, die bisher als politische Werbung zu bewerten sind, nicht mehr erfasst werden würde. Die Medienanstalten warnen insofern vor einer weitgehenden Aushöhlung des Verbotes politischer Werbung im Rundfunk und einem Wegfallen von Kennzeichnungspflichten in Telemedien.[78] Der Bundesrat hat aus selbigen Gründen ebenfalls eine Eingrenzung des Begriffs der politischen Werbung gefordert.[79] Zudem hat der weite Anwendungsbereich auch in kompetenzrechtlicher Sicht Kritik nach sich gezogen. Transparenz sei nur ein Mittel von vielen, um die freie Meinungsbildung in der Union zu gewährleisten. Es brauche auch insbesondere Maßnahmen zur Sicherung der Staatsferne, die Verhinderung einseitiger Einflussnahme ebenso wie die Absicherung des Ausdrucks größtmöglicher Breite und Vollständigkeit bestehender Meinungen in den Medien.[80] In diesem Zusammenhang müsse jedoch sichergestellt bleiben, dass die Regelungskompetenz zur Sicherung des Medienpluralismus nach den europäischen Verträgen den nationalen Mitgliedstaaten zugeschrieben ist.[81]

Insgesamt ist der Regulierungsentwurf in Hinblick auf die einheitliche Regulierung grenzüberschreitender politischer Werbebotschaften sinnvoll. Zukünftig können sich Einblicke in die „Blackbox" politischer Werbung im Internet erhofft werden. Die in dem Verordnungsentwurf statuierten Vorschriften zur Transparenz setzen hier wirksam an. Damit reiht sich der Gesetzesvorschlag in eine Transparenzoffensive seitens der Europäischen Kommission ein, die bereits aus den Vorschriften zur Regulierung sehr großer Online-Plattformen aus dem DSA-E bekannt ist.[82] Neben den geschilderten Bedenken hinsichtlich der Begriffsbestimmung sowie der Kompetenzen stellt der Entwurf einen weiteren wichtigen Schritt dar, um aus regulatorischer Sicht auf die durch die Digitalisierung geschaffenen Veränderungen im digitalen Raum und neuen Herausforderungen für die Demokratien angemessen reagieren zu können.

77 Die Medienanstalten sprechen in einem Positionspapier vom 11. 4. 2022 vom Risiko einer sog. Übererfassung, abrufbar unter: https://www.die-medienanstalten.de/fileadmin/user_upload/20220411_Positionspapier_TransparenzPolitischeWerbung.pdf.

78 Positionspapier der Medienanstalten vom 11. 4. 2022, S. 2 abrufbar unter: https://www.die-medienanstalten.de/fileadmin/user_upload/20220411_Positionspapier_TransparenzPolitischeWerbung.pdf.

79 BT-Drs. 826/21 (B), S. 5.

80 Vgl. BT-Drs. 826/21 (B), S. 3.

81 Vgl. BT-Drs. 826/21 (B), S. 3.

82 Vgl. Art. 13, 23, 24, 29, 30 DSA-E.

Florian Flamme
ist wiss. Mitarbeiter am Institut für Informations-. Telekommunikations- und Medienrecht (öffentlich-rechtliche Abteilung) in Münster und Lehrbeauftragter an der Hochschule des Bundes in Münster.

Amelie Mehlan
ist wiss. Mitarbeiterin am Institut für Informations-, Telekommunikations- und Medienrecht (öffentlich-rechtliche Abteilung) in Münster und Lehrbeauftragte an der FOM Hochschule für Oekonomie und Management in Münster.

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

Vom Irrglauben an die Geheimhaltung durch TLS bei E-Mails

Zugleich Kommentar zu OLG Schleswig-Holstein, Urteil vom 28. 4. 2022 – 6 U 39/21, K&R 2022, 628 ff. (in diesem Heft)

Kurz und Knapp

§ 2 Nr. 1b GeschGehG lässt den Geheimnisschutz nur gelten, wenn der Geheimnisinhaber angemessene Schutzmaßnahmen getroffen hat. Für Informationen in digitaler Form legt der Beitrag dar, inwieweit Verschlüsselung gesetzlichen Geheimnisschutz bewirken kann. Insbesondere geht es um eine Entscheidung des OLG Schleswig-Holstein zu den Unterschieden zwischen TLS- und Ende-zu-Ende-Verschlüsselung. Die Autoren beziehen kritisch Stellung.

I. Relevanz der IT-Sicherheit für das Geschäftsgeheimnisgesetz, insbesondere Verschlüsselung

Geheimnisschutz greift gemäß § 2 Nr. 1b GeschGehG nur für solche Informationen, die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber sind. Welche Maßnahmen obliegen dem Inhaber konkret? Dazu haben die zugrundeliegende Know-how-RL (EU) 2016/943 (ErwG14 und Art. 2 Nr. 1c) und der nationale Gesetz-

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 29. 7. 2022.

geber[1] nur abstrakte Kriterien vorgegeben, wie z. B. den Wert und die Bedeutung des Geheimnisses für das Unternehmen, dessen Entwicklungskosten, die Größe des Unternehmens und die dort üblichen Geheimhaltungsmaßnahmen. Rechtsprechung und Literatur haben deshalb die Aufgabe, Einzelfälle zu beurteilen und nähere Richtlinien für die Subsumtion dieser Anforderungen herauszuarbeiten. Da die Geheimhaltung/Vertraulichkeit einer Information ein klassisches Schutzziel der IT-Sicherheit adressiert, wird dabei auf „technische und organisatorische Maßnahmen" (TOM) abgestellt, die aus dem IT-Sicherheits- und Datenschutzrecht bekannt sind (z. B. Art. 24, 25, 32 DSGVO). Bisherige Gerichtsentscheidungen legen dazu folgende Prüfungsschritte zugrunde:[2]

(1) Identifikation der geheimzuhaltenden Information und Beurteilung der Schutzbedürftigkeit,

(2) Identifikation und Bewertung der Schutzmaßnahmen:
   (a) Auswahl des Personenkreises – need to know,
   (b) organisatorische Maßnahmen: Kennzeichnung und Behandlung der Information im Unternehmen und Geheimhaltungsvereinbarungen,
   (c) technische/physische Maßnahmen.

Die technischen Maßnahmen sind relevant, wenn geheimzuhaltende Informationen – wie meist – in digitaler Form vorliegen, etwa im IT-System des Unternehmens oder mittels elektronischer Kommunikation übertragen werden, z. B. per E-Mail. In diesen Fällen ist die Herausarbeitung und Bewertung technischer Sachverhalte gefragt. Das OLG Schleswig-Holstein hatte sich dazu jüngst mit der Frage zu befassen, ob die „Transportverschlüsselung" einer E-Mail mit dem Verschlüsselungsprotokoll TLS (Transport Layer Security) eine Geheimhaltungsmaßnahme i. S. d. § 2 GeschGehG sein kann. Es ging um eine Teil-Kostenrechnung bzw. Preiskalkulation (Excel-Tabelle), die die Klägerin über ihre Leistungen zur Bewertung von Grundstücken erstellt hatte. Die Klägerin begehrte Geheimnisschutz dieser Preiskalkulation gegenüber der Beklagten, einer Wettbewerberin (zugleich jedoch Mitgesellschafterin eines Joint-Ventures). Sie begründete den Geheimnisschutz u .a. damit, dass die Personen, denen die Preiskalkulation im klägerischen Unternehmen bekannt war, die Excel-Tabelle nicht per unverschlüsselter E-Mail transportierten, sondern ihre E-Mails verschlüsselten, und zwar durch die Transportverschlüsselung TLS. Der Senat hielt dies für eine angemessene Geheimhaltungsmaßnahme.[3] Auf der Grundlage des technischen Sachverhalts (Abschnitt II.) stellen die Autoren diese Bewertung des Senats auf den Prüfstand (Abschnitt III.).

II. Verschlüsselung aus Sicht der Informatik

1. Ziele der IT-Sicherheitsmaßnahmen

Beim Übertragen und Speichern von Daten ist aus Sicht der IT-Sicherheit bedeutsam, dass Daten:

- unverändert (Integrität),
- ihrem Autor zuzurechnen (Authentizität),
- für einen unberechtigten Dritten uneinsehbar (Vertraulichkeit),
- und vor Verlust geschützt sind (Verfügbarkeit).

Die drei erstgenannten Schutzziele lassen sich mittels Verfahren der Kryptographie realisieren: Vertraulichkeit lässt sich durch Verschlüsselung erreichen, Authentizität und Integrität durch Signaturen. Verschlüsselung stellt dabei sicher, dass nur, wer im Besitz des geeigneten Schlüssels ist, Zugriff auf die Daten erhält.

Dazu gibt es abhängig vom Anwendungszweck zwei grundsätzliche Verschlüsselungsverfahren: Symmetrische und asymmetrische. Während bei ersterem zum Ver- und Entschlüsseln derselbe Schlüssel dient, der somit zwischen Absender und Empfänger sicher ausgetauscht werden muss, nutzt das zweitere ein mathematisch voneinander abhängiges Schlüsselpaar des Adressaten. An dessen öffentlichen Schlüssel verschlüsselt, kann er die Nachricht nur noch mit seinem privaten Schlüssel entschlüsseln. Der Vorteil dieses Verfahrens ist, dass der öffentliche Schlüssel, der zum Verschlüsseln genutzt wird, nicht geheimgehalten werden muss. Der aufwendige sichere Schlüsseltausch des symmetrischen Verschlüsselns entfällt. Allerdings ist die asymmetrische Verschlüsselung um einiges rechenintensiver und dadurch langsamer. In der Praxis findet sich daher vielfach hybride Verschlüsselung, bei der ein pro Vorgang zufälliger symmetrischer Schlüssel asymmetrisch verschlüsselt ausgetauscht wird. Die Nachrichten selbst werden dann mit jenem Schlüssel symmetrisch verschlüsselt ausgetauscht. Dieses Vorgehen löst das Problem des sicheren Schlüsseltausches bei der symmetrischen Verschlüsselung und kompensiert den Performancenachteil der asymmetrischen.[4]

Praktisch findet dabei hybride Verschlüsselung in der Regel bei der Datenübertragung ihren Einsatz und symmetrische bei der Verschlüsselung einzelner Dateien und ganzer Datenträger lokal. Die lokale Verschlüsselung ist v. a. relevant, um bei Verlust der Datenträger einen Datenabfluss zu verhindern, wie es z. B. bei der britischen Royal Air Force mit Mitarbeiterdaten geschah.[5] Ebenso verhindert diese Verschlüsselung den unberechtigten Zugriff neugieriger Administratoren und weiterer Wartungskräfte.

2. End-zu-End-Verschlüsselung und „Transportverschlüsselung"

a) Bei der Datenübertragung unterscheiden Anwender häufig zwischen „End-zu-End"-Verschlüsselung, bei der von Nutzer zu Nutzer die Daten durchgehend mit demselben Schlüssel verschlüsselt sind, und „Transportverschlüsselung", bei der zwischen zwei an der Kommunikation beteiligten Systemen die Übertragung verschlüsselt ist. Für diese Unterscheidung ist relevant, dass je nach Art der Datenübertragung mehr als zwei Systeme daran beteiligt sein können. D. h., die Transportverschlüsselung ist auf den Zwischenstationen unterbrochen. Denn verschlüsselt ist lediglich der Transport, an den Zwischenstationen wird

1 BT-Drs. 19/4724, S. 24 f.

2 Eine gute Zusammenfassung der Rechtsprechung liefern *Apel/Nickl*, K&R 2022, 385, 387; zu den IT-Sicherheitselementen im GeschGehG: *Barudi*, in: Kipker, Cybersecurity, 2022, Kap. 9 Rn. 93; *Voigt*, in: Voigt, IT-Sicherheitsrecht, 2. Aufl. 2021, Kap. C Rn. 152 und *Deusch/Eggendorfer*, in: Taeger/Pohle, Computerrechts-Handbuch, 37. EL 2022, Kap. 50.1 Rn. 423 (36. EL: Rn. 421), zu den Prüfungsschritten z. B. OLG Schleswig-Holstein, 28. 4. 2022 – 6 U 39/21, K&R 2022, 628 ff., (in diesem Heft) = juris Rn. 79 - 116; ähnlich: OLG Düsseldorf, 11. 3. 2021 – I-15 U 6/20, WRP 2021, 1080, 1087, Rn. 25, 39 - 53, *Alexander*, in: Köhler/Bornkamm/Feddersen, UWG, 40. Aufl. 2022, § 2 GeschGehG Rn. 48 - 72.

3 OLG Schleswig-Holstein, 28. 4. 2022 – 6 U 39/21, K&R 2022, 628 ff., (in diesem Heft) = juris Rn. 109, 111 - 115.

4 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 2), Kap. 50.1 Rn. 16 - 30, 171 - 198; *Singh*, Geheime Botschaften, 1999, Kap. 6 S. 324 ff., Kap. 7 S. 353 ff.; *Schwenk*, Sicherheit und Kryptographie im Internet, 2002, Kap. 1.4 f. S. 6 ff.; *Bauer*, Kryptologie, 1993, Kap. 11; *Ertel/Löhmann* (Hrsg.), Angewandte Kryptographie, 6. Aufl. 2021, Kap. 2 S. 21 ff., Kap. 5 S. 77 ff.

5 https://www.spiegel.de/politik/ausland/peinliche-panne-royal-air-force-fuerchtet-erpressungen-nach-datendiebstahl-a-626663.html.

die betreffende Nachricht entschlüsselt und sodann gegebenenfalls wieder neu verschlüsselt. Des Öfteren wird dieser Vorgang beschönigend als „Umverschlüsselung" bezeichnet. Dabei erhält jede Zwischenstation vollständige Kenntnis der übertragenen Daten.[6]

Bei der Transportverschlüsselung lagern zudem die Daten auf dem Zielsystem unverschlüsselt, bei einer End-zu-End-Verschlüsselung erfolgt die Entschlüsselung erst zur Nutzung.

In der Implementierung findet sich zudem bei einer Transportverschlüsselung je nach Anwendung die „opportunistische" Verschlüsselung, so z. B. bei der Übertragung von E-Mails. Hier entscheidet der Absenderserver abhängig von den Möglichkeiten des Empfängersystems, ob eine Verschlüsselung der Übertragung möglich ist. Das Verfahren handeln die Systeme aus, dabei nutzen sie die bestmögliche von beiden Systemen unterstützte Verschlüsselung – im Worst Case könnte das auch eine nicht mehr als sicher geltende Verschlüsselung sein (FREAK-Angriff).[7]

Dagegen ist bei einer End-zu-End-Verschlüsselung in der Regel das Verfahren und der Algorithmus von den beteiligten Parteien ausgewählt und festgelegt.

b) Welches Verfahren geeignet ist, bestimmt der Anwendungszweck: Logt sich ein Nutzer auf einer Webseite ein, überträgt man das Passwort zwischen Client (Browser) und Webserver transportverschlüsselt mit TLS. Das ist ausreichend, weil in dem Fall der Client und Webserver auch die jeweiligen Kommunikationsendpunkte sind, und das Passwort unmittelbar weiterverarbeitet und aus dem Speicher des Servers verworfen wird. Beim Versand von E-Mails dagegen erfüllt erst eine End-zu-End-Verschlüsselung die Anforderung „Vertraulichkeit", da mehrere Mailserver beteiligt sind, die jeweils Endpunkte einer Transportverschlüsselung sind, wo die E-Mail jeweils unverschlüsselt lagert.[8]

III. Schlussfolgerungen für die Verwendung des TLS-Protokolls für den Transport von Informationen, für die das GeschGehG gelten soll

1. Prüfungsreihenfolge des OLG Schleswig-Holstein

In dem Fall gemäß Abschnitt I. folgt das OLG Schleswig-Holstein zunächst konsequent der dort genannten Prüfungsreihenfolge:

(1) Es identifiziert die Preiskalkulation als geheimzuhaltenden Information und ordnet deren Schutzbedürftigkeit dem „unteren mittleren Bereich" zu. Die Preiskalkulation ist damit schützenswert und die Klägerin muss Schutzmaßnahmen ergreifen, allerdings müssen diese Maßnahmen keine hohen Anforderungen erfüllen.[9]

(2) Im Anschluss identifiziert und bewertet der Senat die Schutzmaßnahmen der Klägerin. Mit der Auswahl des begrenzten Personenkreises, der im klägerischen Unternehmen Zugang zur Preiskalkulation hatte, sei das Need-to-Know-Prinzip erfüllt. Alle beteiligten Personen seien hinreichend zur Verschwiegenheit verpflichtet.[10]

2. Irrglaube des Gerichts an TLS-Verschlüsselung von E-Mails als technische Schutzmaßnahme

Genauere Betrachtung verdienen die Ausführungen des Senats zu den technischen Schutzmaßnahmen i. S. d. § 2 Nr. 1b GeschGehG:

a) Die Klägerin trug vor, sie habe übliche Schutzmaßnahmen getroffen wie Passwörter und Firewall. Im IT-System sei die Preiskalkulation durch die Einstellungen der Benutzerrechte nur für die definierten Personen abrufbar. Zudem hätten die Beteiligten die Preiskalkulation ausschließlich per E-Mail unter Nutzung von TLS kommuniziert. Die Beklagte habe zugestanden, dass es sich bei der TLS-Verschlüsselung um ein „Standardprotokoll" handle. Eine Ende-zu-Ende-Verschlüsselung sei nicht notwendig gewesen, weil mit Angriffen auf die Information an den „Knotenpunkten der Versendung" nicht zu rechnen sei; es habe kein Anlass zur Annahme bestanden, dass dort Dritte nach den Geheimnissen suchen. Dies sei aber der besondere Schutz, den die Ende-zu-Ende-Verschlüsselung gegenüber der TLS-Verschlüsselung biete. Mit der TLS-Verschlüsselung habe die Klägerin ein „gängiges Verschlüsselungsprogramm" ausgewählt, das vorliegend ausreichend sei, zumal selbst das „besondere elektronische Anwaltspostfach" (beA) keine Ende-zu-Ende-Verschlüsselung beinhalte.[11]

b) Diese Ausführungen lassen sich aus folgenden Gründen nicht mit den technischen Gegebenheiten vereinbaren, wie sie in Abschnitt II. dargestellt sind:

- Sinn und Zweck einer Verschlüsselung ist es aus technischer Sicht, den Zugriff Unberechtigter auf die verschlüsselte Information zu unterbinden. In der E-Mail-Kommunikation ist dafür die Ende-zu-Ende-Verschlüsselung das Verfahren, das dem Stand der Technik entspricht. Bereits die Zugriffsmöglichkeit Unbefugter an den Knotenpunkten spricht aus technischer Sicht dagegen, eine per TLS-Protokoll versendete E-Mail als „verschlüsselt" zu bezeichnen.
- Falsch ist zudem die Annahme des Senats, bei der TLS-Verschlüsselung handle es sich um ein „Verschlüsselungsprogramm". TLS ist vielmehr ein Protokoll (mithin eine Art Sprache), das vorgibt, wie zwei Rechner, die an einer Kommunikation von Daten beteiligt sind, diese Daten miteinander auszutauschen haben. Das Protokoll[12] besteht dabei aus einer fest vorgegebenen Art und Abfolge von Nachrichten. Teilweise können dabei die beteiligten Systeme nach strengen Vorschriften und Abläufen Optionen aushandeln. TLS dient zur Vereinbarung von Verschlüsselungsparametern auf dem Transport der Information.[13]
- Das ist in der Praxis sicher, wenn beide beteiligten Rechner feststehen, wie z. B. beim Hochladen von

6 Das Verhalten folgt aus dem Konzept der Transportverschlüsselung, siehe u. a. *Ertel/Löhmann* (Fn. 4), Kap. 8.5, Kap. 2.3, *Schwenk* (Fn. 4), Kap. 1.6 sowie S. 77 ff.

7 Zum FREAK-Angriff https://freakattack.com/, https://www.smacktls.com/, https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa/, zur Verwendung von TLS im Mail-Versende-Protokoll SMTP https://datatracker.ietf.org/doc/html/rfc2487.

8 *Ertel/Löhmann* (Fn. 4); *Schwenk* (Fn. 4).

9 OLG Schleswig-Holstein, 28. 4. 2022 – 6 U 39/21, K&R 2022, 628 ff., (in diesem Heft) = juris Rn. 79 - 82.

10 OLG Schleswig-Holstein, 28. 4. 2022 – 6 U 39/21, K&R 2022, 628 ff., (in diesem Heft) = juris Rn. 84 - 106.

11 OLG Schleswig-Holstein, 28. 4. 2022 – 6 U 39/21, K&R 2022, 628 ff., (in diesem Heft) = juris Rn. 107 - 116, kritisch zum beA *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 2), Kap. 50.1 Rn. 387 f.; *Deusch/Eggendorfer*, K&R 2021, 689, 694 f.

12 Protokoll ist hier im Sinne eines Ablaufs zu verstehen, analog dem Protokoll zum Empfang eines Staatsoberhauptes, nicht jedoch als Mitschrift oder Aufzeichnung.

13 *Schwenk* (Fn. 4), Kap. 4; *Ertel/Löhmann* (Fn. 4), Kap. 2.3, Kap. 8.5; https://datatracker.ietf.org/wg/tls/about/, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html.

Daten auf eine Webseite über HTTPS[14] und wenn die Daten vom Zielsystem unmittelbar weiterverarbeitet werden, wie zum Beispiel beim Online-Einkauf. Sollen die Daten dagegen auf der Webseite „gelagert" werden, z. B. bei Cloud-Speicher-Anbietern wie OneDrive oder Dropbox, war zwar die Übertragung geschützt, die Lagerung jedoch ist unsicher: Der Anbieter und jeder (erfolgreiche) Angreifer des Systems können die Daten einsehen. E-Mail-Absender haben es dagegen nicht unter Kontrolle, ob alle beteiligten Rechner das TLS-Protokoll anwenden. Es ist daher zweifelhaft, ob die Verwendung des TLS-Protokolls überhaupt als Schutzmaßnahme „des Geheimnisinhabers" i. S. d. § 2 Nr. 1b GeschGehG bezeichnet werden kann.

- Zweifelhaft sind auch die Ausführungen des Senats, die TLS-Verschlüsselung sei ausreichend, weil nicht mit einem unberechtigten Zugriff auf die Preiskalkulation an den Knotenpunkten zu rechnen sei, obwohl die E-Mail dort unverschlüsselt liege und es gebe keinen Anlass dafür, das Dritte dort nach diesen Informationen suchten. Diese Argumentation zäumt das Pferd am Schwanz auf: Wenn nicht davon auszugehen ist, dass Dritte die Preiskalkulation suchen, weshalb ist dann überhaupt die Verschlüsselung notwendig? Der Senat unterstellt mit seiner Argumentation, es sei wahrscheinlicher, dass Dritte die Preiskalkulation auf dem Transportweg stehlen (wo sie verschlüsselt ist) als an dem Knotenpunkt, wo sie unverschlüsselt ist. Den Beweis für diese Hypothese lässt der Senat aber offen. Im Dunkeln bleibt auch, wieso das Gericht ausgerechnet bei der relativ langen Lagerzeit im Vergleich zur kurzen Übertragungszeit ein geringeres Risiko sieht.[15]
- Auffallend ist: Aus keiner Stelle des OLG-Urteils geht hervor, ob die befassten Gerichte Beweis erhoben haben zur Schutzwirkung der TLS-Verschlüsselung oder der sonstigen Schutzmaßnahmen, die die Klägerin vorgetragen hat. Die Ausführungen des Senats legen nahe, dass verfahrensrechtlich keine Beweiserhebung notwendig war: Die Beklagte hatte zugestanden, dass das TLS-Protokoll eine „allgemein übliche Schutzmaßnahme"[16] und „Standard"[17] sei. Somit bleibt leider offen, auf welcher Sachverhaltsgrundlage die (aus Sicht der Autoren fragwürdigen) Aussagen des Gerichts zum TLS-Protokoll und seinem angeblichen Vertraulichkeitsschutz bei der E-Mail-Kommunikation beruhen.
- Der Hinweis des Gerichts auf das beA ist ebenfalls fragwürdig. Denn zum Sicherheitsniveau der „Verschlüsselung" des beA bestehen grundsätzlich dieselben technischen Einwände: Auch beim beA wird die Verschlüsselung im Web-Postfach der Nutzer durch den Diensteanbieter aufgebrochen.[18] Einzig lässt sich dem beA zugutehalten, dass die beteiligten Server in der Theorie der Kontrolle eines einzigen Anbieters unterliegen. Das wäre nach der Lesart einiger immerhin eine organisatorische Vertraulichkeitsmaßnahme, wenn auch eine schwache. Bei E-Mails außerhalb des beA dagegen können Server mehrerer Anbieter in verschiedenen Jurisdiktionen beteiligt sein.
- Zusammenfassend ist festzuhalten: Der Inhalt der streitigen Preiskalkulation mag möglicherweise nicht so schützenswert sein, dass er eine verschlüsselte Kommunikation verlangt. In diesem Fall wäre das Urteil des OLG Schleswig-Holstein nachvollziehbar gewesen, wenn es auf die Notwendigkeit der Verschlüsselung verzichtet hätte. Nicht nachvollziehbar ist jedoch die Behauptung des schleswig-holsteinischen Senats, die Versendung einer E-Mail mit dem TLS-Protokoll sei eine Maßnahme zur Geheimhaltung i. S. d. § 2 Nr. 1b GeschGehG. Das TLS-Protokoll verschafft einer E-Mail keine Vertraulichkeit, die aus technischer Sicht als erheblich einzustufen wäre.

Anders dagegen bei einer Kommunikation, die ausschließlich auf zwei Webserver begrenzt ist, z. B. bei der Nutzung von Internetplattformen wie etwa Online-Shops oder auch Entwicklungsplattformen: Hier kann für den Transport einer Information vom Client des Nutzers zum Web-Server des Plattformanbieters (und vice versa) das TLS-Protokoll einen wirksamen Schutz bieten. Entscheidend sind neben dem Verwendungszweck auf den Systemen (z. B. Lagerung vs. Nutzung) die weiteren Sicherheitsmaßnahmen zu den beteiligten Rechnern.

Anzumerken ist zudem, dass auch die weiteren IT-Sicherheitsziele neben der Vertraulichkeit nicht gewährleistet sind: TLS prüft standardmäßig nur, ob das empfangende System tatsächlich das gewünschte Empfängersystem ist, nicht jedoch, ob der Sender auch der berechtigte Sender ist. Es kann also trotz TLS problemlos eine E-Mail mit der Absenderkennung eines Dritten versandt werden, die den Anschein erweckt, sie stamme vom Geheimnisinhaber. Das IT-Sicherheitsziel der Authentizität ist damit nicht gegeben. Auch ist die in TLS vorgesehene Integritätsprüfung der übertragenen Daten nur auf dem Übertragungsweg möglich, ein späterer Nachweis, ob die Daten unverändert sind, ermöglicht TLS nicht. Ende-zu-Ende-Verschlüsselung kann jedoch beides. In der anwaltlichen Praxis entspricht TLS unter den Gesichtspunkten Authentizität und Integrität dem einfachen Brief: es ist weder klar, wer der wirkliche Absender ist, noch ob tatsächlich das gewünschte Schreiben einlag. Ende-zu-Ende-Verschlüsselung lässt sich in der Hinsicht am ehesten mit der Postzustellungsurkunde vergleichen. Insoweit bietet Ende-zu-Ende-Verschlüsselung einen über die Geheimhaltung hinausgehenden Nutzen.

IV. Fazit

Aus technischer Sicht bietet TLS in der E-Mail-Kommunikation keinen sinnvollen Vertraulichkeitsschutz, ebenso wenig bei der Speicherung von Dateien auf Servern oder Ähnlichem. Dennoch sind oftmals anderslautende Beurteilungen zu lesen, wie etwa im hier diskutierten Urteil des OLG Schleswig-Holstein. TLS ist allerdings nicht zur Verschlüsselung von E-Mails entwickelt worden, sondern zu einem anderen Zweck: TLS erzeugt eine Art digitalen Briefumschlag, der auf Zwischenstationen entfernt werden kann („Umverschlüsselung"). Das kann ausreichend sein, soweit es keine Zwischenstationen gibt (wie z. B. beim Hochladen von Kreditkartendaten in eine Webanwendung); es ist aber beim E-Mail-Versand, der typisch in mindestens drei Etappen stattfindet (vom Mailprogramm zum Absender-Mailserver, von dort zum Empfänger-Mail-

14 HTTPS steht für HTTP Secure, also sicheres HTTP. HTTP ist ebenfalls ein Protokoll und überträgt Webseiten. Die Sicherheit erreicht HTTPS durch den Einsatz von TLS.

15 In technischer Hinsicht sind auf beide Anteile der Kommunikation, Lagerung und Übertragung, verschiedene Angriffe möglich, die jeweils zu einer Offenlegung der Daten führen können. Damit ist eine Privilegierung eines Anteils nicht logisch nachvollziehbar.

16 OLG Schleswig-Holstein, 28. 4. 2022 – 6 U 39/21, K&R 2022, 628 ff., (in diesem Heft) = juris Rn. 109.

17 OLG Schleswig-Holstein, 28. 4. 2022 – 6 U 39/21, K&R 2022, 628 ff., (in diesem Heft) = juris Rn. 113.

18 Zur beA-Kritik der Autoren siehe oben Fn. 11.

server, dort dann weiter zum Empfänger-Mailprogramm), höchst problematisch. TLS schafft zudem keinen Schutz bei der Lagerung von Daten. E-Mails aber liegen typisch für einen längeren Zeitraum auf dem Empfängermailserver.

Prozessbeteiligten eines Geheimnisrechtsstreits sollten daher den technischen Sachverhalt genau klären, gegebenenfalls unter sachverständiger Hilfe, und ihren Sachvortrag daran ausrichten. Auch in der Vertragsgestaltung und Compliance-Beratung zum Geheimnisschutz empfehlen sich Regelungen, die einen korrekt ermittelten Sachverhalt zugrunde legen. In der Praxis empfiehlt sich zur Kommunikation vertraulicher Inhalte per E-Mail die Ende-zu-Ende-Verschlüsselung.

Florian Deusch
ist als Rechtsanwalt und Fachanwalt für Informationstechnologierecht in der Anwaltskanzlei Dr. Gretter tätig und Lehrbeauftragter an der Hochschule Ravensburg-Weingarten. Er ist zudem als Datenschutzbeauftragter tätig.

Tobias Eggendorfer
ist Professor für IT-Sicherheit an der Hochschule Ravensburg-Weingarten und freiberuflicher IT-Berater. Er ist zudem als Datenschutzbeauftragter tätig.

Prof. Dr. Jens M. Schmittmann*

Update Informationsfreiheits- und Transparenzrecht 2021/2022

Kurz und Knapp

Das Informationsfreiheits- und Transparenzrecht hat in den letzten Jahren zunehmend an Bedeutung gewonnen. Dieser Beitrag zeichnet die Entwicklung in Gesetzgebung, Rechtsprechung und Literatur nach. Er knüpft an den Beitrag von Schmittmann, Update Informationsfreiheits- und Transparenzrecht 2020/2021, K&R 2021, 568 ff. an.

I. Einleitung

Nachdem im Zuge der Einführung der DSGVO[1] das Informationsfreiheits- und Transparenzrecht sowohl auf Bundes- als auch auf Landesebene angepasst worden ist,[2] waren im Berichtszeitraum lediglich geringfügige Änderungen auf der Ebene der Bundesländer zu verzeichnen.

In Nordrhein-Westfalen gilt das Gesetz über die Freiheit des Zugangs zu Informationen für das Land Nordrhein-Westfalen (Informationsfreiheitsgesetz) vom 27. 11. 2001,[3] das zuletzt durch Art. 46 des Gesetzes vom 1. 2. 2022,[4] in Kraft getreten am 19. 2. 2022, geändert worden ist.

Im Freistaat Sachsen, der bislang weder Informationsfreiheits- noch ein Transparenzgesetz kannte, hat der Landtag am 13. 7. 2022 den vom Sächsischen Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung (SMJusDEG) erarbeiteten Entwurf des Sächsischen Transparenzgesetzes beschlossen.[5] Am 1. 1. 2023 tritt das Gesetz in Kraft. Dazu hat der Freistaat Sachsen mitgeteilt: „Mit dem ‚Gesetz über die Transparenz von Informationen im Freistaat Sachsen' sollen alle Bürgerinnen und Bürger einen Zugang zu Informationen der Regierung und Verwaltung des Freistaates erhalten, wie zum Beispiel Regierungsbeschlüsse, Gesetzentwürfen, Gutachten, Studien, Berichte, Informationen über Zuwendungen sowie Beteiligungen des Freistaates. Diesen Zugang erhalten sie zum einen auf Antrag, zum anderen perspektivisch auch über sich im Aufbau befindliche Transparenzplattform, auf der die Verwaltung die Informationen selbst zur Verfügung stellen wird."[6]

In Schleswig-Holstein gilt das Informationszugangsgesetz für das Land Schleswig-Holstein (IZG-SH) vom 19. 1. 2012,[7] das zuletzt durch Art. 5 Gesetz vom 16. 3. 2022[8] geändert worden ist.[9]

In den übrigen Bundesländern haben sich Änderungen nicht ergeben.

II. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

Dem Bundesbeauftragten für den Datenschutz wurde mit Inkrafttreten des IFG Bund am 1. 1. 2006 zusätzlich die Ombuds-, Beratungs- und Kontrollfunktion eines Bundesbeauftragten für die Informationsfreiheit übertragen. Auf Peter Schaar folgte zunächst am 19. 12. 2013 Andrea Voßhoff, bevor der SPD-Politiker Ulrich Kelber das Amt am 7. 1. 2019 übernahm.[10]

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat in seinem am 5. 4. 2022 erschienenen 30. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit 2021[11] neben den datenschutzrechtlichen Themen

* Mehr über den Autor erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 2. 8. 2022.

1 VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG, ABl. 2016, L 119/1.

2 Vgl. *Schmittmann*, K&R 2019, 542 ff.; *Schmittmann*, K&R 2020, 584 ff.; *Schmittmann*, K&R 2021, 568 ff.

3 GV NW 2001, S. 806.

4 GV NW 2022, S. 122.

5 Die Verkündung im GVBl. Sachsen ist bislang nicht erfolgt (Stand: 15. 8. 2022).

6 Vgl. https://www.medienservice.sachsen.de/medien/news/1049647.

7 GVOBl. 2012, S. 89.

8 GVOBl. SH 2022, S. 285.

9 GVOBl. 2019, S. 310.

10 S. BfDI, https://www.bfdi.bund.de/DE/BfDI/DerBfDI/bfdi-node.html.

11 S. BfDI, https://www.bfdi.bund.de/DE/Service/Publikationen/Taetigkeitsberichte/taetigkeitsberichte_node.html.