Rechtsgutachten

zur

Strafrechtlichen Bewertung des Einsatzes von LIMIT1

von Prof. Dr. Alexander Roßnagel

Kassel, den 3. November 2017

Inhalt

1. Gutachtenauftrag

Der Beauftragte für Datenschutz und Informationsfreiheit der freien Hansestadt Hamburg beauftragte den Gutachter mit einer strafrechtlichen Bewertung des Einsatzes des Untersuchungswerkzeugs LIMIT. In diesem Gutachten soll als zentrale Rechtsfrage geklärt werden, ob Mitarbeiter der Aufsichtsbehörde das Prüfwerkzeug, das in der Behörde für behördliche Sachverhaltsaufklärungen von Datenschutzverstößen[1] entwickelt worden ist, in strafrechtlich unbedenklicher Weise einsetzen können. Dabei gilt es zu klären, in welcher Weise ein Einsatz des Geräts insbesondere mit §§ 202a und § 202b StGB vereinbar ist.

„LiMiT" ist eine Abkürzung für „Licht in der Mitte des Tunnels". Der Begriff „Tunnel" steht dabei für die Verbindung eines Geräts mit dem Internet und die dabei übertragenen Daten, die normalerweise nicht (jedenfalls nicht einfach und nicht vollständig) zugänglich sind. Als sog. Man-In-The-Middle-Device kann LiMiT dabei helfen, Licht in diese dunklen Datenflüsse zu bringen.

Das Gerät vermittelt den Internet-Zugang eines zu prüfenden Geräts im Verfügungsbereich sowie unter Kontrolle der Behörde. Es verarbeitet möglicherweise personenbezogene Daten, die zwischen diesem und dem Internet übertragen werden und zeichnet die hierbei übermittelten Daten dauerhaft so auf, dass sie einer anschließenden Inspektion zum Zwecke der datenschutzrechtlichen Kontrolle zur Verfügung stehen. Dabei ist unter bestimmten Bedingungen auch der Einblick in solche Daten möglich, bei denen das zu prüfende Gerät so eingerichtet ist, dass die Daten SSL-verschlüsselt mit dem entsprechenden Internet-Server ausgetauscht werden.

Bei LiMiT handelt sich um ein System, das dabei hilft, den Internet-Datenverkehr eines WLAN-fähigen Geräts (Smartphone, Tablet, Laptop, Smart-TV, …) aufzuzeichnen und zu analysieren. In den meisten Fällen ist dabei auch der Einblick in SSL-transportverschlüsselte Inhalte möglich.

Folgende Eigenschaften zeichnet LiMiT aus:[2]

- Es sind keine oder nur geringfügige Anpassungen der Geräte erforderlich, deren Daten aufgezeichnet werden sollen.
- Insbesondere muss keine Software aufgespielt werden.
- Daher kann LiMiT zur Überprüfung der Datenflüsse nahezu jedes (WLAN-fähigen) Geräts eingesetzt werden.

---

1 S. zu diesen z.B. *Bodden/Rasthofer/Richter/Roßnagel*, DuD 2013, 720 (723f.).

2 LIMIT1: Anleitung, Version 0.2 vom Januar 2017, S. 1.

LiMiT funktioniert wie jeder gewöhnliche Internet-WLAN-Router, indem er den über das aufgespannte WLAN angeschlossenen Geräten den Zugang ins Internet vermittelt. Zusätzlich zu dieser reinen Vermittlung finden zwei weitere Prozesse statt:

- Die Daten, die zwischen dem angeschlossenen Gerät und dem Internet ausgetauscht werden, werden in einer Datenbank gespeichert.

- Soweit möglich werden SSL-verschlüsselte Verbindungen durch LiMiT1 umgeschlüsselt, so dass der Inhalt im Klartext vorliegt und für die spätere Auswertung gespeichert wird.

Zusätzlich zu dieser Routing-Funktion bietet LiMiT ein vielfältiges Set von Auswertungswerkzeugen, mit denen aufgezeichnete Daten betrachtet, durchsucht und analysiert werden können.[3]

Beim Einsatz von LiMIT überprüft die Aufsichtsbehörde nur erworbene Apps auf eigenen Geräten hinsichtlich der Einhaltung datenschutzrechtlicher Vorgaben für die Übermittlung personenbezogener Daten. Diese Prüfung führt sie durch, wenn sie einen Anfangsverdacht hat, dass die untersuchte App gegen datenschutzrechtliche Vorgaben verstößt. Der Hersteller oder Verkäufer der App wird über die Untersuchung des Kommunikationsverhaltens der App nicht vorher unterrichtet.

2. Mögliche Tatbestandshandlungen

Die Nutzung von LiMIT könnte zwei Straftatbestände erfüllen. In Betracht kommen zum einen das Ausspähen von Daten nach § 202a Abs. 1 StGB und zum anderen das Abfangen von Daten nach § 202b Abs. 1 StGB. Zu prüfen ist daher, welcher Straftatbestand bezogen auf die objektive Handlung in Frage kommt.

2.1 Der Tatbestand des Ausspähens von Daten

Nach dem Tatbestand des § 202a Abs. 1 StGB wird bestraft, wer sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft. Zugang verschaffen bedeutet das Herstellen der eigenen Herrschaft über die Daten in der Weise, dass der Täter oder ein anderer sie zur Kenntnis nehmen kann .[4] Nach § 202a Abs. 2 StGB werden Daten geschützt, die entweder elektronisch gespeichert sind oder übermittelt werden.

Der Anwender von LiMIT erfasst zwar nicht die in einem fremden Gerät gespeicherten Daten, wohl aber Daten, die elektronisch übermittelt werden, um sich diese Daten zu verschaffen. Soweit die Daten aber nicht gegen unberechtigten Zugang besonders gesichert sind und nicht

---

[3] LIMIT1: Anleitung, Version 0.2 vom Januar 2017, S. 2f.

[4] *Heger*, in: Lackner/Kühl, StGB, 2014, § 202a Rn. 5.

durch Überwindung der besonderen Zugangssicherung verschafft werden, kommt eine Verwirklichung des Tatbestands des § 202a Abs. 1 StGB nicht in Betracht. Dieser Straftatbestand ist daher nur für die Fälle zu prüfen, in denen die Überwindung einer besonderen Zugangssicherung erforderlich ist.

2.2 Der Tatbestand des Abfangens von Daten

Dagegen wird nach § 202b Abs. 1 StGB bestraft, wer sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung einer Datenverarbeitungsanlage verschafft. Der Straftatbestand hat große Ähnlichkeit mit dem des Ausspähens von Daten nach § 202a StGB. Er setzt jedoch nicht die besondere Sicherung der Daten und deren Überwindung durch den Täter voraus. Insofern ist der Straftatbestand des § 202b weiter als der des § 202a StGB. Tatobjekt können im Rahmen des § 202b StGB jedoch nur solche Daten sein, die sich zur Zeit der Tat in einem Übertragungsvorgang befinden.[5] Insofern ist der Straftatbestand des § 202b StGB spezieller als der des § 202a StGB.

Die Tathandlung beim Einsatz von LiMIT besteht im Wesentlichen darin, entweder selbst eine Datenübermittlung zu initiieren und dabei die Datenströme und Dateninhalte zu überwachen oder eine von einer App initiierte Datenübermittlung zu erfassen und die Daten zu speichern.[6] Da es sich immer um die Erfassung und Speicherung von Daten während eines Datenübermittlungsvorgangs handelt und nicht um Daten, die mit Schutzmaßnahmen gesichert auf einem Rechner oder Datenträger gespeichert sind und unter Überwindung der Schutzmaßnahmen ausgespäht werden, geht die folgende Prüfung vorrangig vom Tatbestand des § 202b Abs. 1 StGB aus.

Allerdings ist der Straftatbestand des § 202b Abs. 1 StGB aufgrund des letzten Satzteils der Vorschrift subsidiär.[7] Diese Strafvorschrift greift nur, „wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist“. Da eine Tat nach § 202b Abs. 1 StGB „mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft“ wird und für eine Tat nach § 202a Abs. 1 StGB ein Strafrahmen von „bis zu drei Jahren“ Freiheitsstrafe „oder Geldstrafe“ besteht, tritt die Strafbarkeit nach 202b Abs. 1 StGB zurück, wenn die Tat nach § 202a Abs. 1 strafbar ist.[8] Ob dies der Fall ist, wird nach der Prüfung des Straftatbestands des § 202b Abs. 1 StGB untersucht.

---

5 BT-Drs. 16/3565, 11; *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202b Rn. 3.

6 So für WLAN-Catcher auch *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 66.

7 *Heger*, in: Lackner/Kühl, StGB, 2014, § 202a Rn. 6; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202b Rn. 11.

8 *Heger*, in: Lackner/Kühl, StGB, 2014, § 202a Rn. 6; *Fischer*, Kommentar zum StGB, 2016, § 202b, Rn. 10; *Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202b, Rn. 12; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202b Rn. 11.

3. Objektiver Tatbestand des Abfangens von Daten

Zu prüfen ist also, ob der Mitarbeiter der Aufsichtsbehörde, der mit LiMIT Metadaten oder Inhaltsdaten erfasst, sich gemäß § 202b Abs. 1 StGB „unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung einer Datenverarbeitungsanlage verschafft".

Für den Einsatz von LiMIT macht es einen Unterschied, ob die Datenübermittlung von dem Mitarbeiter der Aufsichtsbehörde veranlasst wurde oder ob sie von einer App auf dem Endgerät der Aufsichtsbehörde selbsttätig initiiert wurde.

3.1 Von einem Mitarbeiter veranlasste Datenübermittlung

Im ersten Fall initiiert der Mitarbeiter die Datenübermittlung, weil er in das Endgerät einen entsprechenden Befehl zu Datenübertragung eingibt oder weil er eine App so nutzt, dass diese zur Erbringung des jeweiligen Dienstes eine Datenübertragung mit seinem Wissen und seinem Einverständnis an einen bekannten Empfänger anstößt. Die Übermittlung wird durch die Sendefunktion des Endgeräts umgesetzt.

3.1.1 Verschaffte Daten

LiMIT speichert die Daten, die zwischen dem angeschlossenen Gerät und dem Internet ausgetauscht werden, in einer Datenbank. Dies betrifft sowohl die Metadaten, die für das Routing der IP-Pakete relevant sind und aus denen der Empfänger der Daten erkannt werden kann, als auch die Inhaltsdaten, aus denen den Zweck der Datenübertragung und damit die datenschutzrechtliche Zulässigkeit der Datenübertragung erkannt werden kann. Beides sind Daten im Sinn von § 202a Abs. 2 StGB, weil sie „elektronisch … übermittelt werden". Der Unterschied zwischen Metadaten und Inhaltsdaten ist für das Tatbestandsmerkmal „sich Daten verschaffen" nicht relevant. Auf den Inhalt der Daten kommt es nicht an.[9] Ebenso wenig spielt es eine Rolle, ob die Daten personenbezogen oder nicht personenbezogen sind.[10]

3.1.2 Verschaffen

Daten sind „verschafft", wenn sie so in den Herrschaftsbereich des Speichernden gelangen, dass er in der Lage ist, sie zur Kenntnis zu nehmen.[11] Bei verschlüsselten Daten ist ein „Verschaffen" erst dann erfüllt, wenn die Daten entschlüsselt werden und damit ihr Inhalt zur Kenntnis genommen werden kann.[12]

---

9 *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 4.

10 *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 3; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 2.

11 *Heger*, in: Lackner/Kühl, StGB, 2014, § 202b Rn. 3; *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202b Rn. 9.

12 *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 53 und § 202b Rn. 16; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 7 und § 202b Rn. 7.

3.1.3 Anwendung technischer Mittel

Die Daten müssen „unter Anwendung von technischen Mitteln“ verschafft worden sein. Unter technischen Mitteln versteht die Vorschrift Software, Codes oder Passwörter.[13] Da LiMIT ein Software-Programm ist, das den Zugriff und die Speicherung der Daten ermöglicht, wird beim Einsatz von LiMIT auch das Tatbestandsmerkmal „unter Anwendung von technischen Mitteln“ erfüllt.

3.1.4 Nichtöffentliche Datenübermittlung

Die Daten müssen „aus einer nichtöffentlichen Datenübermittlung einer Datenverarbeitungsanlage“ stammen. Die Daten werden durch das Endgerät der Aufsichtsbehörde übertragen. Ob die Datenübermittlung öffentlich oder nichtöffentlich ist, entscheidet sich nicht nach der Art oder dem Inhalt der Daten, sondern nach der Art des Übertragungsvorgangs.[14] Die Übermittlung ist nichtöffentlich, wenn der Absender die zu übermittelnden Daten für einen erkennbar eingeschränkten Empfängerkreis bestimmt hat.[15] Es kommt nicht darauf an, dass die Datenübermittlung in besonderer Weise, etwa durch Verschlüsselung, geschützt ist.[16]

Dies ist beim Einsatz von LiMIT der Fall. Die Daten stammen aus der Datenübermittlung, die ausgehend vom Endgerät der Behörde an irgendeinen Empfänger im Internet erfolgt. Dies ist eine Punkt-zu-Punkt-Übermittlung und keine öffentliche Übermittlung an alle, die sie empfangen können und wollen. Die Übermittlung erfolgt somit an einen erkennbar eingeschränkten Empfängerkreis. Insofern ist auch das Tatbestandsmerkmal der „nichtöffentlichen“ Übermittlung erfüllt.

Fraglich ist jedoch, ob die „nichtöffentliche Datenübermittlung einer Datenverarbeitungsanlage“ auch anzunehmen ist, wenn es die eigene Datenverarbeitungsanlage ist, deren Datenübermittlung durch den Handelnden selbst initiiert worden ist. Die Zielsetzung der Strafvorschrift ist es, fremde Kommunikation vor Ausforschung zu schützen, nicht zu verhindern, dass die eigene Kommunikation daraufhin überprüft wird, ob sie so funktioniert, wie der Berechtigte, der die Datenübertragung von seinem Endgerät aus initiiert hat, dies mit ihr bezweckt. Daher ist beim beschriebene Einsatz von LiMIT im Regelfall davon auszugehen, dass keine gegenüber dem Täter, dem Prüfer der Aufsichtsbehörde, schützenswerte Kommunikation stattfindet. Durch den Einsatz von LiMIT erfolgt keine konkrete Rechtsgutsgefährdung.

---

13 BT-Drs. 16/3656, 11; *Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202b, Rn. 8; *Hilgendorf*, in: Leipziger Kommentar zum StGB, 2009, § 202b, Rn. 17.

14 BT-Drs. 16/3656, 11.

15 *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202b Rn. 6; *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202b Rn. 10; *Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202b, Rn. 4a; *Hilgendorf*, in: Leipziger Kommentar zum StGB, 2009, § 202b, Rn. 9.

16 S. z.B. *Fischer*, Kommentar zum StGB, 2016, § 202b, Rn. 4; *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202b Rn. 6; *Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202b, Rn. 4a.

3.1.5 Nicht für den Täter bestimmt

Schließlich ist zu prüfen, ob die Daten, die der Handelnde sich verschafft, „nicht für ihn bestimmt" sind. Für diese Frage kommt es nicht darauf an, wer Eigentümer des Sendegeräts[17] ist und ob die Übermittlung der Daten von ihm initiiert wurde.[18] Die Daten sind auch nicht allein deswegen für den Handelnden bestimmt, weil die Daten auf ihn bezogen sind.[19] Nicht jede betroffene Person darf daher die Daten abfangen.

Vielmehr ist für die Bestimmung entscheidend, ob derjenige, der über die Daten verfügen darf, sie zur Kenntnisnahme durch den Handelnden bestimmt hat.[20] Entscheidend ist also, wer bezogen auf die Daten verfügungsberechtigt ist und für wen er die Daten bestimmt hat. Verfügungsbefugt ist im Regelfall derjenige, der die Daten erstellt oder erzeugt hat oder der ihre Erzeugung oder Speicherung veranlasst.[21]

Soweit der Mitarbeiter der Aufsichtsbehörde die Inhaltsdaten – wie etwa bei einer Mail – selbst erstellt hat, ist er auch verfügungsbefugt. Soweit sein Endgerät und die auf ihm befindlichen Programme die Daten – wie etwa die Metadaten der Kommunikation – auf seine Initiative hin erzeugt haben, ist er ebenfalls verfügungsbefugt. In diesen Fällen sind die Daten zwar nicht für ihn bestimmt, sondern für einen Empfänger.[22] Insofern ist festzustellen, dass das Tatbestandsmerkmal „nicht für ihn bestimmt" formal erfüllt ist.

Es könnte aber materiell an einem Verstoß gegen den Schutzgehalt der Strafvorschrift fehlen. Die Vorschrift des § 202b StGB schützt das formale Geheimhaltungsinteresse des Verfügungsbefugten.[23] Da der Mitarbeiter der Aufsichtsbehörde aber selbst der Verfügungsbefugte ist, richtet sich seine Handlung nur gegen sich selbst und sein eigenes formales Geheimhaltungsinteresse, so dass sie nicht den Tatbestand des § 202b StGB erfüllt.

Ob die Daten verschlüsselt sind oder nicht, spielt für diese Bewertung keine Rolle.[24] Die Daten

---

17 *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 7a; *Lenckner/Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202a, Rn. 9f.; *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 19; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 4; *Krischker*, ZD 2015, 464 (466)

18 *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202a Rn. 8; *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 19; *Heger*, in: Lackner/Kühl, StGB, 2014, § 202a Rn. 3.

19 *Heger*, in: Lackner/Kühl, StGB, 2014, § 202a Rn. 3; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 4.

20 *Eisele*, in: Schönke/Schröder, Kommentar zum StGB, § 202b, Rn. 7; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, 2014, § 202a Rn. 4; *Hilgendorf*, in: Leipziger Kommentar zum StGB, 2009, § 202b, Rn. 20; *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 19; *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202a Rn. 7.

21 *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 19 und § 202b Rn. 8; *Lenckner/Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202a, Rn. 9; *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 7a; *Hilgendorf*, in: Leipziger Kommentar zum StGB, 2009, § 202b, Rn. 26; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 4; *Krischker*, ZD 2015, 464 (466).

22 *Heger*, in: Lackner/Kühl, StGB, 2014, § 202a Rn. 3.

23 S. z.B. *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202b Rn. 2; *Heger*, in: Lackner/Kühl, StGB, 2014, § 202b Rn. 1.

24 *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202b Rn. 6.

sind teilweise nach dem SSL-Verfahren für den Datentransport verschlüsselt. Diese Verschlüsselung erfolgt durch die Übermittlungsfunktion des Endgeräts der Aufsichtsbehörde automatisch, wenn diese Funktion mit dem Empfänger in einem Handshake-Verfahren den Übertragungsschlüssel bestimmt hat.[25] Diese Verschlüsselung enthält daher keinen Hinweis, dass die Daten nicht für die Aufsichtsbehörde bestimmt sind oder ihre Speicherung gegen ihr formelles Geheimhaltungsinteresse verstößt.

3.1.6 Keine Erfüllung des Tatbestands des Abfangens von Daten

Als Zwischenergebnis kann also festgehalten werden, dass der Einsatz von LiMIT zur Erfassung und Speicherung von Metadaten und Inhaltsdaten nicht den Tatbestand des § 202b Abs. 1 StGB erfüllt, wenn die Datenübermittlung durch einen Mitarbeiter der Aufsichtsbehörde selbst initiiert worden ist und von der eigenen Datenverarbeitungsanlage der Behörde ausgeht. Zwar sind die Tatbestandsmerkmale „sich oder einem anderen unter Anwendung von technischen Mitteln … Daten (§ 202a Abs. 2) aus einer … Datenübermittlung … verschafft“ erfüllt. Es fehlt jedoch an den Tatbestandsmerkmalen „nicht für ihn bestimmte Daten … aus einer nichtöffentlichen Datenübermittlung“. Denn die Datenübermittlung ist nicht gegenüber demjenigen geheim zu halten, der sie selbst veranlasst hat. Das gleiche Ergebnis ist festzuhalten, wenn der Mitarbeiter die Daten selbst erstellt oder ihre Erzeugung selbst initiiert hat und daher über die Daten verfügungsbefugt ist.

3.2 Von einer App veranlasste Datenübermittlung

Etwas Anderes könnte aber dann gelten, wenn der Mitarbeiter der Aufsichtsbehörde sich Daten verschafft, die ohne sein Zutun durch die Software einer App erzeugt oder kopiert und verschickt worden sind.

In diesem zweiten zu untersuchenden Fall geht die Initiative zur Datenübermittlung von einer App im Endgerät des Nutzers aus. Sie geht gerade nicht auf die Initiative des Mitarbeiters der Aufsichtsbehörde zurück, sondern wird von diesem weder bemerkt noch gewollt oder geduldet. Vielmehr entsteht die Initiative zur Übermittlung in Folge einer vorherigen Programmierung der App durch den Hersteller aufgrund eines bestimmten Ereignisses. Dieses kann ein Datum, ein bestimmter Zeitablauf oder ein besonderes Ereignis im Rahmen der Nutzung der App oder des Endgeräts sein. Ein solches Ereignis kann auch eine vom Nutzer initiierte Datenübermittlung sein, die von der App genutzt wird, um weitere zusätzliche Daten (z.B. den Inhalt des Terminkalenders oder der Kontaktliste) an den gleichen Empfänger, dem auch der Nutzer Daten übermitteln will, zu senden oder Daten an einen anderen Empfänger zu übermitteln. In allen Fällen nutzt die App die Sendefunktion des Endgeräts, um die Daten über ein WLAN zu übermitteln.

Dieser zweite Fall wäre möglich, wenn durch den Erwerb der App zwar deren Nutzung, nicht aber der Zugriff auf die der Ausführung der App zugrundeliegenden Daten und Programme

[25] S. näher Kap. 4.1.

eröffnet worden ist.[26] In diesem Fall könnte es sich um die „nichtöffentlichen Übermittlung“ von Daten handeln, die „nicht für ihn bestimmt“ sind, weil die Verfügungsbefugnis nicht bei dem Mitarbeiter, sondern bei dem Hersteller der App liegt und dieser die Daten nur für den Empfänger bestimmt hat.

3.2.1 Nicht für den Täter bestimmte Daten

Auch in diesem Fällen würde es keine Rolle spielen, dass die Daten vom Endgerät der Aufsichtsbehörde aus übermittelt werden. Für das Entstehen der Verfügungsmacht, die über die Bestimmung der Daten entscheidet, ist weder das Eigentum am Datenträger noch die Tatsache, dass die Daten den Handelnden selbst betreffen, von Bedeutung.[27] Auch in diesen Fällen liegt die Verfügungsbefugnis bei dem Hersteller der App, wenn dem Erwerber der Zugriff auf die App-Software nicht eröffnet ist und die App selbsttätig (also nur auf Veranlassung der Herstellers) Daten erzeugt oder kopiert und deren Übermittlung anstößt.[28] In diesem Fall sind die Daten, die übermittelt werden, nicht für den Mitarbeiter der Aufsichtsbehörde bestimmt, sondern nur für den vorgesehenen Empfänger.[29] Dies dürfte zumindest für die Inhaltsdaten gelten.

Dagegen könnten die Metadaten der Übermittlung dann anders zu beurteilen sein, wenn diese auch für die Übermittlungsfunktion des Endgeräts notwendig sind und ihr zur Verfügung gestellt werden sollen, damit diese die Inhaltsdaten an die richtige Empfängeradresse versenden kann. In diesem Fall wären die Metadaten zumindest auch für die Sendefunktion des Endgeräts der Aufsichtsbehörde und damit auch für den Mitarbeiter der Aufsichtsbehörde bestimmt. In diesem Fall könnte er daher die Metadaten ohne Verstoß gegen § 202b Abs. 1 StGB mit LiMIT auslesen und speichern. Dass er mit den für ihn bestimmten Daten in einer anderen Weise umgeht, als der Verfügungsbefugte dies vorgesehen hat, spielt für die Bestimmung der Daten für ihn keine Rolle.[30]

---

26 *Heger*, in: Lackner/Kühl, StGB, 2014, § 202a Rn. 3.

27 S. Nachweise in Fn. 17 und 19.

28 S. z.B. *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 7a; *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202a Rn. 10; vielfach reklamieren die Hersteller den Quellcode als Betriebsgeheimnis – *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 28.

29 S. auch das Beispiel der Scheck- und Kreditkarten – s. z.B. *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202a Rn. 10.1; *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 7a; *Lenckner/Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202a, Rn. 11; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 4; das Beispiel von Programmdaten von Spielautomaten nennen *Lenckner/Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202a, Rn. 11 und *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 4. Dieser führt auch das Mobiltelefon und die SIM-Lock-Software an.

30 *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 21; *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202a Rn. 9; *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 7; *Lenckner/Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202a, Rn. 11; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 5; *Krischker*, ZD 2015, 464 (466).

3.2.2 Nichtöffentliche Datenübermittlung

Eine Übermittlung, die nicht der Mitarbeiter der Aufsichtsbehörde, sondern die App veranlasst und die an einen anderen Empfänger gerichtet ist, könnte eine nichtöffentliche Datenübermittlung darstellen. Die Datenübermittlung wurde durch den Hersteller der App programmiert. Dieser hat durch diese Programmierung vorgesehen, dass die Daten nach ihrer Übermittlung nur durch den in den Metadaten genannten Empfänger zur Kenntnis genommen werden. Dadurch hat er sein formelles Geheimhaltungsinteresse zum Ausdruck gebracht. Dass die Übermittlung datenschutzrechtlich unzulässig ist, spielt für dieses Tatbestandsmerkmal keine Rolle. Die Datenübermittlung der Daten ist auch nichtöffentlich, wenn sie durch das Endgerät der Aufsichtsbehörde erfolgt.

3.2.3 Erfüllung des Tatbestands des Abfangens von Daten

Damit erfüllt der Mitarbeiter der Aufsichtsbehörde, der LiMIT nutzt, um von einer App selbsttätig initiierte Datenübermittlungen zu erfassen und zu speichern, hinsichtlich der Inhaltdaten, nicht jedoch in Bezug auf die Metadaten, den objektiven Tatbestand der Strafvorschrift des Abfangens von Daten nach § 202b Abs. 1 StGB.

4. Objektiver Tatbestand des Ausspähens von Daten

Die Strafvorschrift des § 202a Abs. 1 StGB greift – auch beim Abfangen von Daten aus einem Übermittlungsvorgang – dann ein, wenn der Täter dabei sich oder einem Dritten „Zugang“ zu Daten verschafft, die zusätzlich „gegen unberechtigten Zugang besonders gesichert sind“, und dabei die „Zugangssicherung“ überwindet. Dies könnte bei der Entschlüsselung verschlüsselt übermittelter Daten der Fall sein. Dies ist vor allem für den Fall zu bedenken, dass die Sendefunktion des Endgeräts die zu übermittelnden Datenpakete für den Transport nach dem Standard SSL/TLS mit dem öffentlichen Schlüssel des Empfängers verschlüsselt[31] und diese verschlüsselten Pakete von LiMIT so „umgeschlüsselt“ werden, „dass der Inhalt im Klartext vorliegt und für die spätere Auswertung gespeichert“ werden kann.[32]

4.1 Besondere Sicherung

Die Transportverschlüsselung nach dem Standard „Transport Layer Security“ (TLS) (vormals Secure Sockets Layer – SSL) verschlüsselt die einzelnen Datenpakete für den Transport durch das Internet nach einem hybriden Verschlüsselungsprotokoll. Nach einem durch Zertifikate gesicherten asymmetrisch verschlüsselten Handshake-Verfahren verwenden beide Seiten

---

[31] Dies war im Februar 2017 bei etwa 2,7% der Webseiten in Deutschland der Fall – s. Deutsch Internet Statistiken, reflecte.de. In einer Untersuchung von rund 40.000 Webseiten klein- und mittelständischer Unternehmen in Baden-Württemberg durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg haben 7% der Internetseiten https und TLS genutzt – s. *Petrlic/Manny*, DuD 2017, 88 ff.

[32] LIMIT1: Anleitung, Version 0.2 vom Januar 2017, S. 2f.

zum Nachrichtenaustausch ein symmetrisches Verschlüsselungsverfahren. Unter der Verwendung von LiMIT erfolgt das Handshake-Verfahren und die Vereinbarung des symmetrischen Schlüssels mit LiMIT statt dem von der App gewünschten Empfänger der Nachricht. LiMIT führt nach der Analyse der Nachrichten mit diesem Empfänger das Handshake-Verfahren und die Verschlüsselung der Nachrichten durch und sendet ihm die von LiMIT verschlüsselten Nachrichten zu.[33]

Daten sind im Sinn des § 202a StGB dann „gegen unberechtigten Zugang besonders gesichert", wenn der Verfügungsberechtigte Vorkehrungen getroffen hat, die objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sind, den unberechtigten Zugriff auf Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren.[34] Als eine solche Vorkehrung ist auch eine Verschlüsselung der Daten anzusehen[35] – sowohl bei einer Ende-zu-Ende-Verschlüsselung als auch bei einer Transportverschlüsslung,[36] die nur Schutz vor unberechtigtem Ausspähen der übertragenen Daten auf der Transportstrecke bieten soll. Entscheidend ist, dass der Verfügungsberechtigte die Sicherungsvorrichtung trifft und damit sein spezielles Interesse an der Geheimhaltung der Daten erkennbar zum Ausdruck bringt.[37]

Die Transportverschlüsselung wird in dem hier zu beurteilenden Fall aber nicht durch den Verfügungsbefugten, also den Anbieter der App vorgenommen, sondern durch die Sendefunktion des Endgeräts der Aufsichtsbehörde. Verfügungsberechtigter über die Daten und Durchführender der besonderen Schutzmaßnahmen fallen somit auseinander. Dies wäre unbedenklich, wenn derjenige, die die Schutzvorkehrungen anbringt, dies im Auftrag des Verfügungsbefugten täte. Dies ist jedoch hier nicht der Fall, da der App-Anbieter die Übermittlung gegen oder ohne den Willen des Inhabers des Endgeräts initiiert, dessen Endgerät die Transportverschlüsselung automatisch durchführt. Im zu beurteilenden Fall ist vielmehr derjenige, der die Transportverschlüsselung durchführt, zugleich auch derjenige, der sie wieder aufhebt. Eine vom Täter und nicht vom Verfügungsbefugten angebrachte Sicherheitsvorkehrung kann nicht erkennbarer Ausdruck des Interesses des Verfügungsbefugten an der Geheimhaltung der von ihm übermittelten Daten sein. Für die Tatbestandsverwirklichung fehlt es daher an besonderen Sicherheitsvorkehrungen des Verfügungsbefugten gegen einen unberechtigten Zugang

---

33 *IETF*, RFC 7525; *BSI*, Technische Richtlinie TR-02102-2 (Version 2017-01).

34 S. z.B. *BGH*, NJW 2015, 3463; *BGH*, MMR 2010, 711; BT-Drs. 16/3656, 10; *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 35; *Lenckner/Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202a, Rn. 14; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 6; *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 8f.; *Hilgendorf*, in: Leipziger Kommentar zum StGB, 2009, § 202b, Rn. 30; *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202a Rn. 13.

35 S. z.B. *Hilgendorf*, in: Leipziger Kommentar zum StGB, 2009, § 202b, Rn. 35; *Lenckner/Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202a, Rn. 16; *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 41 und 84; *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202a Rn. 13; *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 9a; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 6.

36 S. *Luch/Hofmann*, K&R 2014, 161 (164).

37 BT-Drs. 16/3565, 10; *BGH*, MMR 2010, 711; *Heger*, in: Lackner/Kühl, StGB, 2014, § 202a Rn. 4; *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 9; *Lenckner/Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202a, Rn. 14; *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 35.

des Täters zu den Daten.[38]

4.2 Überwindung der Zugangssicherung

Selbst wenn entgegen dieser Feststellung dennoch eine nach § 202a Abs. 1 StGB geeignete Sicherheitsvorkehrung angenommen würde, stellte sich die Frage, ob der Mitarbeiter der Aufsichtsbehörde, der LiMIT anwendet, diese Zugangssicherung überwindet. Eine „Überwindung" der Zugangssicherung liegt vor, wenn der Täter die Zugangssicherung außer Kraft setzt oder umgeht.[39] Ob dies mit einem nicht unerheblichen Aufwand erfolgen muss, ist strittig.[40] Die herrschende Meinung fordert dies nicht.[41]

Findet eine Überwindung statt, wenn derjenige, der die Zugangssicherung selbst angebracht hat und die Möglichkeiten hat, sie wieder aufzuheben, sie ihrer Schutzfunktion beraubt? Dies könnte der Fall sein, wenn die App und damit der Verfügungsbefugte die Sicherung angebracht hätte. Von der Schutzrichtung des § 202a Abs. 1 StGB setzt die Vorschrift eine für den Täter fremde Sicherung voraus. Ein Täter, der die Sicherung selbst angebracht hat, sich selbst die Möglichkeiten vorbehalten hat, sie auch wieder zu Kontrollzwecken aufzuheben und sie mit von ihm hierfür eigens vorgesehenen Hilfsmitteln aufhebt, „überwindet" nicht eine Sicherung, sondern entfernt eine eigene Sicherung wie es sie danach auch wieder hinzufügt. Er ist daher kein tauglicher Täter für den Tatbestand des § 202a Abs. 1 StGB.[42] Im Ergebnis ist daher festzustellen, dass der Mitarbeiter der Aufsichtsbehörde keine besondere Schutzvorkehrung, die gegen ihn gerichtet ist, überwindet. Auch aus diesem Grund begeht er keine Straftat nach § 202a Abs. 1 StGB.

5. Befugnis der Kenntnisnahme

Soweit die Software einer App selbsttätig Inhaltsdaten erzeugt und deren Übermittlung an einen bestimmten Empfänger veranlasst und der Mitarbeiter der Aufsichtsbehörde mit Hilfe von LiMIT diese Daten speichert und entschlüsselt, könnte bezogen auf die Inhaltsdaten der objektive Tatbestand von § 202b Abs. 1 StGB erfüllt sein. Dann müsste aber das Verschaffen der Daten auch „unbefugt" sein. Das Merkmal „unbefugt" schließt den Tatbestand aus, wenn

---

38 Dagegen richtet sich bei dem von *Luch/Hofmann*, K&R 2014, 161 (164) untersuchten Fall des E-Postbriefs die Transportverschlüsselung, auf die sich der Berufsgeheimnisträger verlässt, ausschließlich gegen Dritte.

39 BT-Drs. 16/3656, 10; *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 11b; *Hilgendorf*, in: Leipziger Kommentar zum StGB, 2009, § 202b, Rn. 18; *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202a Rn. 17.

40 So BT-Drs. 16/3656, 10.

41 S. z.B. *Fischer*, Kommentar zum StGB, 2016, § 202a, Rn. 11b.

42 Ebenso sehen *Luch/Hofmann*, K&R 2014, 161 (164) die Mitarbeiter der Post bei der Transportverschlüsselung des E-Postbriefs nicht als taugliche Täter des § 202a StGB. Sie halten zwar eine Straftat nach § 202b StGB für möglich. Diese scheidet hier aber aus den oben genannten Gründen aus.

die Befugnis sich daraus ergibt, dass die Daten für den Täter bestimmt sind.[43] Es betrifft die allgemeine Rechtswidrigkeit der Tat, wenn sich die Befugnis aus einer anderen Rechtsnorm ergibt.[44]

Die Befugnis zum Abfangen und zur Kenntnisnahme der Daten könnte sich aus den Aufsichtsbefugnissen der Datenschutzaufsichtsbehörde ergeben.[45]

5.1 Aufsichtsbefugnisse nach dem geltenden Bundesdatenschutzgesetz

Die Aufsichtsbehörde hat nach § 38 Abs. 1 Satz 1 BDSG die Aufgabe, die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten regeln, zu kontrollieren. Diese Aufsichtsaufgabe ist eher weit und umfasst sowohl anlassbezogene als auch anlassunabhängige Kontrollen.[46] Sie umfasst auch die Telemedienangebote, die durch eine App im Endgerät des Nutzers vermittelt werden. Die Aufsichtsaufgabe gilt nach § 1 Abs. 5 Satz 1 und 3 BDSG auch für App-Services, die von außerhalb Deutschlands, der Europäischen Union und des Europäischen Wirtschaftsraums angeboten werden, wenn die Datenverarbeitung im Endgerät des Nutzers in Deutschland erfolgt.[47] Dann kann die Aufsichtsbehörde ihrer Aufgabe nur nachkommen, wenn sie die Datenverarbeitung im Endgerät untersucht.

Die Aufgabe allein begründet jedoch noch nicht eine bestimmte Aufsichtsbefugnis.[48] Die Befugnis, Daten zu erheben und zu verarbeiten, könnte sich aus § 38 Abs. 1 Satz 3 BDSG ergeben. Danach darf die Aufsichtsbehörde „die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen“. Diese Regelung enthält eine Zweckbindung für gespeicherte Daten, wird aber von einem Teil der Kommentarliteratur auch als Legitimationsgrundlage für

---

43 S. z.B. *Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202b, Rn. 10; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 5 und 10.

44 Dies gilt insbesondere für Befugnisse von Behörden – s. z.B. *Weidemann*, in: von Heintschel-Heinegg, BeckOK StGB, 2017, § 202a Rn. 21 ff.; *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 58 und 62 sowie § 202b Rn. 19; *Lenckner/Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202a, Rn. 24; *Eisele*, in: Schönke/Schröder, Kommentar zum StGB, 2014, § 202b, Rn. 10; *Altenhain*, in: Matt/Renzikowski, Kommentar zum StGB, 2013, § 202a Rn. 10; *Heger*, in: Lackner/Kühl, StGB, 2014, § 202b Rn. 5; *Krischker*, ZD 2015, 464 (467).

45 Zur Rechtfertigung durch gesetzliche Ermächtigungen s. z.B. *Graf*, in: Münchener Kommentar zum StGB, Band 4, 2012, § 202a Rn. 65 ff.; *Krischker*, ZD 2015, 464 (467).

46 *Petri*, in: Simitis, BDSG-Kommentar, 2014, § 38 Rn. 32 und 61; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG-Kommentar, 2014, § 38 Rn. 17; *Grittmann*, in: Taeger/Gabel, Kommentar zum BDSG, TMG und TKG, 2013, § 38 BDSG, Rn. 10; *Gola/Schomerus*, BDSG-Kommentar, 2015, § 38 Rn. 2; *Hillenbrand-Beck*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 5.4 Rn. 45 und 64.

47 *Bodden/Rasthofer/Richter/Roßnagel*, DuD 2013, 720 (725).

48 So jedoch *Petrlic/Manny*, DuD 2017, 88 (89).

die zweckgebundene Datenverarbeitung und -nutzung durch die Aufsichtsbehörde angesehen.[49] Andere beschränken die Vorschrift – entsprechend ihrem Wortlaut – auf die Zweckbindung, gespeicherte Daten nur für Aufsichtszwecke zu verwenden.[50] Nach dieser Ansicht gelten auch für die Datenschutzaufsichtsbehörden die allgemeinen Regelung für die Datenverarbeitung durch öffentliche Stellen,[51] im Bund § 13 Abs. 1 BDSG und in der freien Hansestadt Hamburg § 12 Abs. 1 LDSG Hamburg. Danach ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.[52] Soweit das Verschaffen der Daten für die in § 38 Abs. 1 Satz 1 BDSG genannte Aufgabe, die Ausführung von datenschutzrechtlichen Vorgaben zu kontrollieren, erforderlich ist, ist die Aufsichtsbehörde hierzu auch befugt. Die Wahl zwischen zulässigen Aufsichtsmitteln liegt in ihrem pflichtgemäßen Ermessen.[53] Gegenstand, Umfang und Tiefe der Prüfung bestimmt die Aufsichtsbehörde.[54] Auch bestimmt sie, auf welche Weise, in welchen Zeitabständen und in welcher Intensität sie welche Datenverarbeitungsvorgänge welcher verantwortlichen Stelle überprüft.[55]

Eine spezielle Befugnis zur Verarbeitung personenbezogener Daten zu Aufsichtszwecken könnte sich außerdem indirekt aus § 38 Abs. 3 Satz 1 BDSG und direkt aus § 38 Abs. 4 BDSG ergeben.

Nach § 38 Abs. 3 Satz 1 BDSG haben die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Diese Auskünfte können auch Passworte für zugriffsgeschützte Programme[56] oder die Schlüssel für verschlüsselte Daten betreffen, wenn die Aufsichtsbehörde den Zugang benötigt oder Daten entschlüsseln muss, um ihre Aufsichtsaufgabe erfüllen zu können. Ihre Erkenntnisse aus den Auskünften der Kontrollierten darf die Aufsichtsbehörde für Aufsichtszwecke (nach § 13 Abs. 1 BDSG und § 12 Abs. 1 LDSG Hamburg) auch automatisiert verarbeiten.

Nach § 38 Abs. 4 Satz 1 BDSG sind die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben

---

49 *Grittmann*, in: Taeger/Gabel, Kommentar zum BDSG, TMG und TKG, 2013, § 38 BDSG, Rn. 15; *Gola/Schomerus*, BDSG-Kommentar, 2015, § 38 Rn. 9.

50 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG-Kommentar, 2014, § 38 Rn. 7; *Petri*, in: Simitis, BDSG-Kommentar, 2014, § 38 Rn. 38

51 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG-Kommentar, 2014, § 38 Rn. 7.

52 Außerdem ermöglicht § 38 Abs. 1 Satz 3 i.V.m. § 14 Abs. 2 Nr. 1 bis 3, 6 und 7 BDSG Übermittlungen und Zweckänderungen in der Kooperation mit anderen Behörden – s. *Petri*, in: Simitis, BDSG-Kommentar, 2014, § 38 Rn. 38.

53 *Grittmann*, in: Taeger/Gabel, Kommentar zum BDSG, TMG und TKG, 2013, § 38 BDSG, Rn. 10; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG-Kommentar, 2014, § 38 Rn. 16; *Gola/Schomerus*, BDSG-Kommentar, 2015, § 38 Rn. 14; *Krischker*, ZD 2015, 464 (467).

54 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG-Kommentar, 2014, § 38 Rn. 18.

55 *Grittmann*, in: Taeger/Gabel, Kommentar zum BDSG, TMG und TKG, 2013, § 38 BDSG, Rn. 10.

56 S. *Petri*, in: Simitis, BDSG-Kommentar, 2014, § 38 Rn. 65; *Hillenbrand-Beck*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 5.4 Rn. 77.

erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Die Ergebnisse dieser Prüfungen und Besichtigungen darf die Aufsichtsbehörde auch in ihren Computern verarbeiten. Die Mitarbeiter der Aufsichtsbehörde können nach § 38 Abs. 4 Satz 2 BDSG geschäftliche Unterlagen sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. Dabei können sie ihre Erkenntnisse ebenfalls automatisiert verarbeiten.[57] Der Auskunftspflichtige hat diese Maßnahmen nach § 38 Abs. 4 Satz 4 BDSG zu dulden.

Eine spezifische Regelung, Datenverarbeitungsvorgänge, die in Endgeräten von Betroffenen stattfinden, zu untersuchen und auszuwerten, besteht nicht. Die Frage wird auch in der Kommentarliteratur zum Bundesdatenschutzgesetz nicht explizit aufgegriffen. Die Vorschrift des § 38 Abs. 4 Satz 1 BDSG regelt wegen des Eingriffs in das Grundrecht aus Art. 13 GG den besonderen Fall, dass die Datenverarbeitungsvorgänge in Datenverarbeitungsanlagen auf den Grundstücken der verantwortlichen Stellen erfolgen und nur dort kontrolliert werden können.[58] Eine Pflicht zur vorherigen Ankündigung der Kontrolle sieht § 38 Abs. 4 Satz 1 BDSG nicht vor.[59] Die allgemeine Kontrollbefugnis ergibt sich jedoch aus § 38 Abs. 4 Satz 2 BDSG, wonach die Mitarbeiter der Aufsichtsbehörde geschäftliche Unterlagen sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme einsehen können. Diese Untersuchungsobjekte sind nicht abschließend, sondern nur beispielhaft genannt.[60] Diese Befugnis ist nicht auf die Grundstücke der Kontrollierten beschränkt, sondern besteht für alle gespeicherten personenbezogenen Daten und Datenverarbeitungsprogramme, wo immer die Aufsichtsbehörde Zugang zu diesen hat.[61] Dies muss erst recht gelten, wenn die Untersuchung der Wirkungsweise einer App im Endgerät die einzige Möglichkeit ist, die Aufsichtsaufgabe wahrzunehmen. Ein weiteres Beispiel für eine anerkannte Untersuchungsmethode der Aufsichtsbehörde außerhalb der Grundstücke des Verantwortlichen sind Online-Überprüfungen von Webseiten durch automatische Prüftools.[62] Die Aufsichtsbehörde darf solche Untersuchungen auch präventiv durchführen.[63]

Zu dem gleichen Ergebnis gelangt eine Anwendung des Verhältnismäßigkeitsprinzips. Dieses

---

57 *Gola/Schomerus*, BDSG-Kommentar, 2015, § 38 Rn. 23; *Petri*, in: Simitis, BDSG-Kommentar, 2014, § 38 Rn. 63; *Hillenbrand-Beck*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 5.4 Rn. 75.

58 *Gola/Schomerus*, BDSG-Kommentar, 2015, § 38 Rn. 22.

59 *Grittmann*, in: Taeger/Gabel, Kommentar zum BDSG, TMG und TKG, 2013, § 38 BDSG, Rn. 30; *Gola/Schomerus*, BDSG-Kommentar, 2015, § 38 Rn. 22; *Hillenbrand-Beck*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 5.4 Rn. 72; *Petri*, in: Simitis, BDSG-Kommentar, 2014, § 38 Rn. 61; *Nguyen*, ZD 2015, 269.

60 *Petri*, in: Simitis, BDSG-Kommentar, 2014, § 38 Rn. 63; *Grittmann*, in: Taeger/Gabel, Kommentar zum BDSG, TMG und TKG, 2013, § 38 BDSG, Rn. 33.

61 Umfassende Untersuchungsbefugnisse: *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG-Kommentar, 2014, § 38 Rn. 9.

62 S. z.B. *Krischker*, ZD 2015, 464 ff.; *Petrlic/Manny*, DuD 2017, 88 ff.; *Petri*, in: Simitis, BDSG-Kommentar, 2014, § 38 Rn. 36.

63 *Grittmann*, in: Taeger/Gabel, Kommentar zum BDSG, TMG und TKG, 2013, § 38 BDSG, Rn. 10; *Hillenbrand-Beck*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 5.4 Rn. 45 und 64; *Krischker*, ZD 2015, 464 (467f.).

fordert hinsichtlich der Kontrollen, das jeweils mildeste effektive Kontrollmittel einzusetzen.[64] Daher kann von der Befugnis der Vorort-Kontrollen in einem Erst-Recht-Schluss auf die Befugnis zur Kontrolle von Apps in den Diensträumen der Aufsichtsbehörde geschlossen werden.[65] Diese Befugnis erfasst daher auch Datenverarbeitungsvorgänge, die ein App-Anbieter als verantwortliche Stelle im Endgerät des Betroffenen ausführt. Deren Untersuchung in den Diensträumen der Aufsichtsbehörde ist ein erheblich milderes Mittel der Aufsicht als Vor-Ort-Kontrollen – wenn sie denn möglich wären.

Aus § 38 Abs. 4 Satz 3 BDSG, der auf § 24 Abs. 6 BDSG verweist, der wiederum auf § 24 Abs. 2 BDSG verweist, wird deutlich, dass als Geheimnisse geschützte Daten der Aufsichtsbehörde nicht vorenthalten werden dürfen.[66] Vielmehr darf diese die geheimen Daten zur Kenntnis nehmen, ist aber zur Geheimhaltung[67] und nach § 38 Abs. 1 Satz 3 BDSG zu einer strengen Zweckbindung verpflichtet, die Daten nur zu Aufsichtszwecken zu verarbeiten.

Die Kontrollen unter Einsatz von LiMIT dienen vorrangig nur der Sachverhaltsaufklärung. Wenn diese zu einem begründeten Verdacht eines Verstoßes gegen datenschutzrechtliche Vorgaben führen, sollte der App-Verantwortliche vor weiteren behördlichen Schritten informiert werden und ihm Gelegenheit zur Stellungnahme gegeben werden. Dies ist jedoch ein Gebot rechtsstaatlichen Verfahrens und hat keinen Einfluss auf die strafrechtliche Bewertung der App-Untersuchungen als „befugt“.

5.2 Aufsichtsbefugnisse nach der Datenschutz-Grundverordnung

An diesem Ergebnis wird sich mit Geltungsbeginn der Datenschutz-Grundverordnung zum 25. Mai 2018 – bis auf einige Aufgabenerweiterungen – nichts Wesentliches ändern. Die umfassende Aufsichtsaufgabe ergibt sich dann aus Art. 57 Abs. 1 lit. a und h DSGVO. Nach Art. 57 Abs. 1 lit. a) DSGVO „muss“ die Aufsichtsbehörde „die Anwendung dieser Verordnung überwachen“.[68] Hierzu soll sie nach Art. 57 Abs. 1 lit. h) DSGVO „Untersuchungen über die Anwendung dieser Verordnung durchführen“. Diese Aufgabe betrifft alle notwendigen Ermittlungen von Datenschutzverstößen.[69]

Konkrete Rechtsänderungen, die die Datenschutz-Grundverordnung bewirkt, werden allerdings neue und zusätzliche Tätigkeitsfelder und Tätigkeitsziele der Aufsichtsbehörden erzwingen. Zum einen erweitert sich das Tätigkeitsfeld der Datenschutzaufsicht durch die Ausweitung der materiellen Anwendbarkeit des Datenschutzrechts auf die Marktortfälle des Art. 3 Abs. 2 DSGVO. Nach Art. 3 Abs. 2 DSGVO ist sie künftig aber auch für all die Fälle zuständig, in denen „die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der

---

64 *Petri*, in: Simitis, BDSG-Kommentar, 2014, § 38 Rn. 61.

65 So *Krischker*, ZD 2015, 464 (468) für Online-Überprüfungen von Webservices.

66 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG-Kommentar, 2014, § 38 Rn. 11.

67 S. *Petri*, in: Simitis, BDSG-Kommentar, 2014, § 38 Rn. 69.

68 S. hierzu *Roßnagel*, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017, 95 ff.

69 *Nguyen*, in: Gola, Kommentar zur DSGVO, 2017, Art. 57 Rn. 4.

Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter“ erfolgt. Voraussetzung ist lediglich, dass die Datenverarbeitung „im Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist,“ oder „das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt“. Die Datenschutzaufsicht wird danach für viele Fälle der Datenverarbeitung im Internet zuständig sein, für die sie bisher nicht zuständig war.[70] Dies betrifft auch viele Apps, die aus Drittländern außerhalb der Europäischen Union und dem Europäischen Wirtschaftsraum angeboten werden. Gerade wenn die Aufsichtsbehörden bei diesen Verantwortlichen oder Auftragsverarbeitern keine Untersuchungen vor Ort vornehmen können, werden sie viele Prüfungen durchführen müssen, bei denen sie versuchen müssen, die notwendigen Informationen durch Webrecherchen oder Untersuchungen der Apps zu gewinnen und diese zu bewerten.

Eine weitere Aufgabenerweiterung ergibt sich durch das neue Konzept eines Datenschutzes durch Systemgestaltung. Art. 25 Abs. 1 DSGVO fordert vom Verantwortlichen, „geeignete technische und organisatorische Maßnahmen“ zu treffen, „die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen“. Diese Maßnahmen der Technikgestaltung hat der Verantwortliche „sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung“ auszuwählen und anzuwenden. Er soll die technischen und organisatorischen Maßnahmen „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen“ auswählen. Die Vorschrift des Art. 25 DSGVO ist viel zu abstrakt und viel zu unbestimmt, um dem Verantwortlichen klare Vorgaben für eine datenschutzfreundliche Systemgestaltung zu geben.[71] Um diese Vorschrift umzusetzen müssen die Aufsichtsbehörden die Datenverarbeitungsvorgänge der Verantwortlichen intensiv untersuchen und ihnen auf der Grundlage ihrer Untersuchungen Vorschläge, Anreize und Unterstützung bieten.[72]

Die Aufsichtsaufgaben sind sehr weit gefasst[73] und umfassen sowohl anlassbezogene als auch

---

70 S. z.B. *Roßnagel*, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017, 96.

71 S. z.B. *Husemann*, Datenschutz durch Systemgestaltung, in: Roßnagel, Das neue Datenschutzrecht, 2018, Kap. 5 Rn. 44 ff.

72 S. *Roßnagel*, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017, 124f.

73 S. z.B. *Braun*, Durchsetzung des Datenschutzrechts, in: Roßnagel, das neue Datenschutzrecht, 2018, § 6 Rn. 50; *Körffer*, in: Paal/Pauly, Kommentar zur DSGVO, 2016, Art. 57 Rn. 10.

anlassunabhängige Kontrollen.[74] Umfang und Intensität bei Erfüllung der Aufgaben liegen dabei allein im pflichtgemäßen Ermessen der Aufsichtsbehörde.[75] Um die Aufgaben zu erfüllen, sind die notwendigen Befugnisse in Art. 58 DSGVO einzusetzen. Diese sind so zu interpretieren, dass die Aufsichtsbehörden ihre Aufgaben nach Art. 57 DSGVO effektiv wahrnehmen können. Dies ergibt sich aus dem unionsrechtlichen Auslegungsgrundsatz des „effet utile". Dieser fordert, insbesondere Befugnisnormen so auszulegen, dass das Unionsrecht die höchstmögliche praktische Wirksamkeit entfalten kann.[76]

Die Aufsichtsbehörde kann sich zur Erfüllung dieser Aufgaben aller Aufsichtsbefugnisse des Art. 58 DSGVO bedienen. Insbesondere kann sie sich auf Art. 58 Abs. 1 lit. b und e DSGVO berufen. Nach Art. 58 Abs. 1 lit. b DSGVO hat die Aufsichtsbehörde die Befugnis, Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen. Datenschutzüberprüfungen ermöglichen alle Verfahrensschritte, die zur Ermittlung von Verfahrensverstößen erforderlich sind.[77] Datenschutzüberprüfungen umfassen somit nicht nur (unangeküdigte)[78] Vor-Ort-Prüfungen – die Befugnis zur Vor-Ort-Kontrolle ist in Art. 58 Abs. 1 lit. f DSGVO eigens geregelt –, sondern als milderes Mittel auch Prüfungen, die ohne die Räume des Verantwortlichen zu betreten, durchgeführt werden können. Genannt werden zum Beispiel „Testkäufe", um zu prüfen, ob die erforderlichen Informationen mitgeteilt werden.[79] Insofern gilt hier auch die Argumentation zu § 38 Abs. 4 BDSG.[80] Die Aufsichtsbehörde kann die Datenverarbeitungsvorgänge der Verantwortlichen in dem Umfang und an dem Ort überprüfen, der ihr sinnvoll erscheint.[81] Dies gilt auch für die Diensträume der Aufsichtsbehörde.[82] Sie kann Datenverarbeitungsprogramme einsehen, ohne dass diese für die Datenschutzüberprüfung vorbereitet wurden.[83] Ihre Prüfungen muss die Aufsichtsbehörde nicht bei dem Verantwortlichen vorher anmelden.[84] Bei Verantwortlichen, die der Datenschutz-Grundverordnung unterliegen, aber mit ihren Datenverarbeitungsanlagen nicht in der Europäischen Union oder im Europäischen Wirtschaftsraum belegen sind, ist die Untersuchung ihrer Apps in der Aufsichtsbehörde das einzige Mittel, um die von Art. 57 Abs. 1 lit. a) DSGVO aufgegebene Kontrollaufgabe zu erfüllen. Sie Maßnahme ist daher nach Art. 57 Abs. 1 lit. a DSGVO geboten und nach Art. 58 Abs. 1 lit. b DSGVO zulässig.

---

74 S. z.B. *Selmayr*, in: Ehmann/Selmayr, Kommentar zur DSGVO, Art. 58 Rn. 11; *Körffer*, in: Paal/Pauly, Kommentar zur DSGVO, 2017, Art. 58 Rn. 10; *Ziebarth*, in: Sydow, DSGVO-Kommentar, 2017, Art. 58 Rn. 8; *Nguyen*, in: Gola, Kommentar zur DSGVO, 2017, Art. 58 Rn. 2, 3 und 8.

75 *Braun*, Durchsetzung des Datenschutzrechts, in: Roßnagel, das neue Datenschutzrecht, 2018, § 6 Rn. 58. *Körffer*, in: Paal/Pauly, Kommentar zur DSGVO, 2017, Art. 58 Rn. 10; *Ziebarth*, in: Sydow, DSGVO-Kommentar, 2017, Art. 57 Rn. 2.

76 *Nguyen*, in: Gola, Kommentar zur DSGVO, 2017, Art. 57 Rn. 3 und Art. 58 Rn. 2.

77 *Nguyen*, in: Gola, Kommentar zur DSGVO, 2017, Art. 58 Rn. 6.

78 *Nguyen*, ZD 2015, 269.

79 *Ziebarth*, in: Sydow, DSGVO-Kommentar, 2017, Art. 58 Rn. 22.

80 S. Kap. 5.1.

81 *Nguyen*, in: Gola, Kommentar zur DSGVO, 2017, Art. 58 Rn. 7

82 *Nguyen*, in: Gola, Kommentar zur DSGVO, 2017, Art. 57 Rn. 7.

83 *Nguyen*, in: Gola, Kommentar zur DSGVO, 2017, Art. 58 Rn. 6.

84 *Nguyen*, in: Gola, Kommentar zur DSGVO, 2017, Art. 58 Rn. 8.

Soweit dies notwendig ist, gibt Art. 58 Abs. 1 lit. e DSGVO der Aufsichtsbehörde zusätzlich die Befugnis, von dem Verantwortlichen Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten. Aber auch diese Befugnis kann sie gegenüber Anbietern aus einem Drittstaat nur sehr beschränkt nutzen und ist auf die eigene Informationsgewinnung durch Kontrollen in der Aufsichtsbehörde selbst angewiesen. Dies kann auf Art. 58 Abs. 1 lit. e DSGVO gestützt werden, weil diese Vorschrift den „Zugriff … innerhalb des verarbeitenden Systems“ meint.[85] Wenn das verarbeitende System nicht an der Niederlassung des Verantwortlichen ist, sondern in der Hand der betroffenen Person, so darf dieses untersucht werden. Außerdem ist anerkannt, dass das Betreten der Niederlassung nicht zwingend ist. Vielmehr kann der Zugang auch durch ein mobiles Gerät und daher auch aus der Aufsichtsbehörde heraus erfolgen.[86]

Die Speicherung der zu überprüfenden Daten ist nach § 13 LDSG Hamburg oder einem künftigen Landesdatenschutzgesetz zulässig.

5.3 Aufsichtsbefugnisse nach dem neuen Bundesdatenschutzgesetz

Nach dem neuen Bundesdatenschutzgesetz vom 30. Juni 2017, das am 25. Mai 2018 – zusammen mit der Datenschutz-Grundverordnung – wirksam wird und das bisherige Bundesdatenschutzgesetz ersetzt, werden die Aufsichtsaufgaben und die Aufsichtsbefugnisse im Wesentlichen gleich bleiben. Aufsichtsaufgaben und Aufsichtsbefugnisse bestimmt vorrangig die Datenschutz-Grundverordnung. Das neue Bundesdatenschutzgesetz enthält jedoch in § 40 BDSG-neu ergänzende und konkretisierende Regelungen.[87]

Nach § 40 Abs. 1 BDSG-neu behalten die Aufsichtsbehörden der Länder die Aufsicht über die Anwendung der Vorschriften über den Datenschutz bei nichtöffentlichen Stellen.

§ 40 Abs. 4 Satz 1 BDSG-neu gibt der Aufsichtsbehörde – wie bisher auch – die Befugnis, von den Verantwortlichen zu verlangen, dass sie ihnen die zur Erfüllung ihrer Aufsichtsaufgabe notwendigen Auskünfte erteilen. Nach § 40 Abs. 5 Satz 1 BDSG-neu ist die Aufsichtsbehörde befugt, Grundstücke und Geschäftsräume zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten. Weitere Befugnisse sind in § 40 BDSG-neu nicht geregelt, weil vorrangig die Aufsichtsbefugnisse nach Art. 58 DSGVO gelten.[88] Insofern ändert sich durch § 40 BDSG-neu nichts gegenüber den Feststellungen zur Datenschutz-Grundverordnung.

5.4 Befugnis der Aufsichtsbehörden

Zu den Aufsichtsbefugnissen der Aufsichtsbehörden kann zusammenfassend festgehalten

---

85 So *Ziebarth*, in: Sydow, DSGVO-Kommentar, 2017, Art. 58 Rn. 30.

86 *Ziebarth*, in: Sydow, DSGVO-Kommentar, 2017, Art. 58 Rn. 32.

87 *Braun*, Durchsetzung des Datenschutzrechts, in: Roßnagel, das neue Datenschutzrecht, 2018, § 6 Rn. 76.

88 *Braun*, Durchsetzung des Datenschutzrechts, in: Roßnagel, das neue Datenschutzrecht, 2018, § 6 Rn. 64.

werden, dass sie sowohl nach dem bis zum 24. Mai 2018 geltenden Datenschutzrecht als auch nach dem ab dem 25. Mai 2018 geltenden neuen Datenschutzrecht nach der Datenschutz-Grundverordnung und dem neuen Bundesdatenschutzgesetz befugt sind, Datenschutzkontrollen an Apps im eigenen Endgerät durchzuführen und dabei auch das Übermittlungsverhalten der Apps zu überprüfen. Wenn sie dabei LiMIT einsetzen, erfolgen nur Datenverarbeitungen, zu denen sie befugt sind. Das Verschaffen der Daten ist somit durch die Befugnis zur Datenschutzkontrolle gerechtfertigt.

6. Ergebnis

Die Datenschutzaufsichtskontrollen von Apps mit Hilfe des Untersuchungswerkzeugs LiMIT verstoßen nicht gegen §§ 202a oder 202b StGB.

Zwar verschafft sich der kontrollierende Mitarbeiter unter Anwendung von technischen Mitteln Daten aus einer nichtöffentlichen Datenübermittlung einer Datenverarbeitungsanlage. Doch sind dies im Regelfall seine eigenen Daten in einer von ihm initiierten Übermittlung, so dass ein Verstoß gegen die Strafvorschrift des § 202b Abs. 1 StGB ausscheidet. Außerdem ist er derjenige, der die Verfügungsbefugnis über die Daten hat, so dass das Tatbestandsmerkmal „nicht für ihn bestimmte Daten“ für ihn nicht greift.

Dagegen liegt die Verfügungsbefugnis bei dem App-Verantwortlichen, wenn die App selbsttätig Daten erzeugt oder auf Daten des Endgeräts zugreift und deren Übermittlung an einen bestimmten Empfänger veranlasst. Daher sind zumindest die Inhaltsdaten nicht für den kontrollierenden Mitarbeiter bestimmt. Nutzt die App die Übermittlungsfunktion des Endgeräts, dann sind die Metadaten jedoch für das Endgerät und damit auch seinen Eigentümer bestimmt.

Eine Ausspähung von Daten gemäß § 202a StGB findet nicht statt, weil durch die TLS-Verschlüsselung durch das Endgerät der Aufsichtsbehörde keine besondere Sicherung gegen ihren Mitarbeiter erfolgt und dieser durch die „Umschlüsselung“ der Daten auch keine besondere Sicherung überwindet.

Sofern dennoch der Tatbestand der Straftatbestände des §§ 202a oder 202b StGB erfüllt sein sollte, fehlt es an der Rechtswidrigkeit der Tat, da die Datenschutzkontrollen mit LIMIT „befugt“ erfolgen, wenn sie allein dazu dienen, die Aufsichtsaufgabe der Aufsichtsbehörde zu erfüllen.

7. Literatur

Bodden, E./Rasthofer, S./Richter, P./Roßnagel, A.: Schutzmaßnahmen gegen datenschutzunfreundliche Smartphone-Apps – Technische Möglichkeiten und rechtliche Zulässigkeit des Selbstdatenschutzes bei Apps, DuD 2013, 720.

Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-02102-2: Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS) (Version 2017-01).

Däubler, W./Klebe, T./Wedde, P./Weichert, T. (Hrsg.), Bundesdatenschutzgesetz – Kompakt-Kommentar zum BDSG, 4. Auf., Frankfurt a. M. 2014.

Fischer, T.: Kommentar zum Strafgesetzbuch, 63. Aufl., München 2016.

Gola, P. (Hrsg.), Datenschutz-Grundverordnung – VO (EU) 2016/679, München 2017.

Gola, P./Schomerus, R.: Bundesdatenschutzgesetz, Kommentar, 12. Aufl., München 2015.

Ehmann, E./Selmayr, M.: Datenschutz-Grundverordnung, München 2017.

Heintschel-Heinegg, von B. (Hrsg.): Beck'scher Online-Kommentar StGB, 35. Edition, München 2017.

Internet Engineering Task Force (IETF): Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) (RFC 7525), 2015.

Joecks, W./Miebach, K. (Hrsg.): Münchener Kommentar zum StGB, Bd. 4, 2. Aufl., München 2012.

Krischker, S.: Datenschutzkontrollen und Hacking, ZD 2015, 464.

Kühling, J./Buchner, B. (Hrsg.): Datenschutz-Grundverordnung, Kommentar, München 2017.

Lackner, K./Kühl, K. (Hrsg.): Strafgesetzbuch, Kommentar, 28. Aufl., München 2014.

Leipziger Kommentar zum Strafgesetzbuch, Band 6, 12. Aufl., Berlin 2009.

Luch, A. D./Hofmann, C.: § 203 StGB als Hemmschuh der elektronischen Kommunikation?, K&R 2014, 161.

Matt, H./Renzikowski, J. (Hrsg.): Strafgesetzbuch, Kommentar, München 2013.

Nguyen, A. M.: Die zukünftige Datenschutzaufsicht in Europa, ZD 2015, 265.

Paal, B. P./Pauly, D. A. (Hrsg.): Datenschutz-Grundverordnung, München 2017.

Petrlic, R./Manny, K.: Wie sicher ist der Zugriff auf Websites im Internet?, DuD 2017, 88.

Roßnagel, A. (Hrsg.): Handbuch Datenschutzrecht, München 2003.

Roßnagel, A.: Datenschutzaufsicht nach der Datenschutz-Grundverordnung – Neue Aufgaben und Befugnisse der Aufsichtsbehörden, Wiesbaden 2017.

Roßnagel, A. (Hrsg.): Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, Baden-Baden 2018.

Schönke, A./Schröder, H. (Hrsg.): Strafgesetzbuch, Kommentar, 29. Aufl., München 2014.

Simitis, S. (Hrsg.): Bundesdatenschutzgesetz, Kommentar, 8. Aufl., Baden-Baden 2014.

Sydow, G. (Hrsg.), Europäische Datenschutzgrundverordnung, Kommentar, Baden-Baden 2017.

Taeger, J./Gabel, D. (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Aufl., Frankfurt a. M. 2013.