Die Datenkrake als Nutztier der Strafverfolgung

Zum strafprozessualen Zugriff auf Facebook-Profile

Dr. Markus Englerth / Yoan Hermstrüwer*

A. Einleitung

Im Oktober 2012 meldete der Social-Network-Gigant Facebook einen spektakulären Erfolg: Eine Milliarde aktive Nutzer. Damit besitzt nach Angaben des Unternehmens mittlerweile jeder siebte Mensch auf unserem Planeten ein Profil in dem sozialen Netzwerk.[1] Doch Facebook macht die Welt durch globale Vernetzung nicht nur kleiner. Es macht digitale Kommunikation auch riskanter.[2] Einen Datenbestand, wie das Unternehmen ihn hegt und pflegt, würden sich selbst technologisch fortgeschrittene Überwachungsstaaten nicht träumen lassen.[3] Der deutschen Staatsgewalt sind Aufbau und Verwaltung einer vergleichbaren zentralen Datenbank nach den vom BVerfG entwickelten Grundsätzen verwehrt.[4] Doch was ist dieses Verbot in unserer Informationsgesellschaft noch wert, wenn man das Risiko, dass informationshungrige Ermittlungsbehörden sich stattdessen den freigiebigen Umgang mit personen-

* Dr. Markus Englerth ist Rechtsanwalt in der Berliner Sozietät „Danckert Spiller Richter Bärlein". Yoan Hermstrüwer, Licencié en droit, ist Research Fellow und Doktorand am Max-Planck-Institut zur Erforschung von Gemeinschaftsgütern in Bonn.

1 Vgl. *Süddeutsche Zeitung* v. 4.10.2012 (abrufbar unter: >http://www.sueddeutsche.de/digital/sozialenetzwerke-facebook-hat-eine-milliarde-nutzer-1.1487102<). Als aktive Nutzer definiert Facebook diejenigen, die sich mindestens einmal im Monat mit ihrem Account anmelden. Die Zahl der täglich aktiven Nutzer wird auf etwa die Hälfte geschätzt (vgl. >http://www.golem.de/news/soziales-netzwerk-facebook-hat-1-milliarde-aktive-nutzer-1210-94910.html<). Die Zahl wird allerdings auch dadurch künstlich in die Höhe getrieben, dass viele Nutzer inzwischen – unter Verstoß gegen die Nutzungsbedingungen von Facebook – mehrere Profile angelegt haben.

2 Ähnlich der Präsident des BVerfG *A. Voßkuhle* in einem Interview mit dem Magazin *Focus* vom 6.11.2011.

3 Dazu *E. Morozov*, The Net Delusion – How Not to Liberate the World, London: Penguin Books 2011, S. 148-167.

4 Zum Verbot der Persönlichkeitskatalogisierung zu statistischen Zwecken schon BVerfGE 27, 1 (6) – Mikrozensus; BVerfGE 65, 1 (48) – Volkszählung. Wenn *H.-H. Trute*, in: A. Roßnagel (Hrsg.), Handbuch Datenschutzrecht (2003), Kap. 2.5 Rn. 26, Persönlichkeitsprofile als scheinbar verobjektivierende „Mystifikationen" beschreibt, unterschätzt er damit die empirisch belegte Genauigkeit algorithmenbasierter Vorhersagen.

bezogenen Daten zunutze machen und nach Belieben bei den privaten „Datenfressern“[5] bedienen, aus den Fugen geraten lässt?

Erfolglos hat kürzlich ein Jugendrichter am AG Reutlingen versucht, die „Beschlagnahme“ des Facebook-Profils eines Angeklagten durchzusetzen, da er darin eine belastende Kommunikation zwischen dem Profilinhaber und dessen Bekannten zu finden vermutete.[6] Das Scheitern dieses Pionierversuchs hat eine Debatte dazu angestoßen, wie man Facebook auf der Grundlage des geltenden Rechts in Zukunft zu einer besseren Kooperation mit staatlichen Strafverfolgern und Gerichten bewegen könnte. Der Wunsch des Staates nach mehr „Kooperationsbereitschaft“[7] auf Seiten der Betreiber sozialer Netzwerke ist Ausdruck eines bedenklichen Trends, der schleichend in eine neue Form staatlicher Überwachung zu münden droht. Diese „neue Überwachung“ setzt nicht mehr unmittelbar beim einzelnen Nutzer an. Vielmehr macht sie sich gezielt die konzentrierte Informationsmacht privater Akteure zunutze.[8]

Die Architektur von Facebook und anderen sozialen Netzwerken (wie Jappy, werkennt-wen, studiVZ oder das Karrierenetzwerk XING) ist geradezu darauf ausgelegt, einen gewaltigen Informationsschatz zu akkumulieren. Die Nutzer werden durch das soziale Design angeregt, permanent miteinander zu kommunizieren und immer mehr persönliche Informationen preiszugeben.[9] Zwar dürften die oft im Ausland ansässigen Betreiberunternehmen sowohl nach dem völkerrechtlichen Wirkungsprinzip als auch nach europäischem Datenschutzrecht den datenschutzrecht-

5 Der Begriff „Datenfresser“ stammt von *C. Kurz/ F. Rieger*, Die Datenfresser – Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen, Frankfurt a.M. 2011.

6 AG Reutlingen StV 2012, S. 462.

7 Dazu auch *S. E. Schulz/C. Hoffmann*, Staatliche Datenerhebung in sozialen Netzwerken, DuD 2012, S. 7.

8 Gewisse Parallelen zur Kontroverse um die Verwertung der Ergebnisse sog. „Internal Investigations“ sind nicht zu übersehen. Auch hierbei macht sich der Staat in fragwürdiger Weise die Ergebnisse privater Informationssammlung zunutze. Nach h.M. sind Arbeitnehmer aufgrund ihrer arbeitsvertraglichen Treuepflicht gegenüber den vom Arbeitgeber beauftragten „Ermittlern“ zur wahrheitsgemäßen Auskunft verpflichtet, vgl. *R. Wimmer*, Die Verwertung unternehmensinterner Untersuchungen – Aufgabe oder Durchsetzung des Legalitätsprinzips?, in: L. Schulz/M. Reinhart/O. Sahan (Hrsg.), Festschrift für Imme Roxin, Heidelberg 2012, S. 537 (540 ff.). Während der Arbeitnehmer sich bei einer staatlich veranlassten Vernehmung auf den Grundsatz der Selbstbelastungsfreiheit berufen könnte, gilt dies im Rahmen der bei unternehmensinternen Ermittlungen üblichen informellen „Interviews“ nicht. Dies soll jedoch nach teilweise vertretener Auffassung einer spätere Beschlagnahme und strafprozessualen Verwertung der selbstbelastenden Einlassungen nicht entgegenstehen (so LG Hamburg NJW 2011, S. 942; nach Neufassung des § 160a StPO zu Recht anders LG Mannheim NStZ 1012, S. 713).

9 *J. Grimmelmann*, Saving Facebook, Iowa Law Review 94 (2009), S. 1137 (1151 f.); der freigiebige Umgang mit persönlichen Informationen dürfte auch dadurch verstärkt werden, dass die Freigiebigkeit der anderen Nutzer als Signal für die Sicherheit des Netzwerks interpretiert und die Wahrscheinlichkeit eines schädigenden Ereignisses nach unten korrigiert wird, vgl. *D. Kahneman*, Thinking, Fast and Slow, London: Penguin Books 2011, S. 166-174.

lichen Vorgaben der EU und ihrer Mitgliedstaaten unterliegen.[10] Dennoch ist der Vollzug europäischen Datenschutzrechts (trotz gewisser Spillover- oder „Brussels"-Effekte)[11] defizitär, ein Defizit, das eine de facto-Schutzlücke bewirkt und aufgrund geringerer Schutzstandards in den meisten Drittstaaten (etwa in den USA)[12] nicht kompensiert wird. Dies gilt insbesondere für das Informationsrecht im nicht-öffentlichen Bereich. Ausländische Unternehmen wie Facebook haben es sich zur Gewohnheit gemacht, Daten für unbestimmte Zeit zu speichern. Das Interesse der Strafverfolger, den entstandenen privaten Datenschatz zu heben und in Beweismittel für ein Strafverfahren umzumünzen, ist nachvollziehbar. Dass diesen Begehrlichkeiten Grenzen gesetzt werden müssen, wenn der Schutz der Privatsphäre und personenbezogener Daten nicht ausgehöhlt werden soll, steht jedoch gleichfalls außer Zweifel.

Im Folgenden möchten wir ausgehend vom Beschluss des AG Reutlingen aufzeigen, dass die Rechtspraxis hinsichtlich des Zugriffs auf elektronische Kommunikation auf eine abschüssige Bahn geraten ist (B). Schon die Judikatur zur Beschlagnahme von E-Mail-Nachrichten beim Provider wird verfassungsrechtlichen Vorgaben kaum gerecht und überstrapaziert das geltende Regelwerk der StPO (C). Sollte der dogmatisch hierauf aufbauende Reutlinger Beschluss zur „Beschlagnahme" von Nutzerprofilen in sozialen Netzwerken Schule machen, könnte der Schutz der Privatsphäre und des unbefangenen Gedankenaustauschs im Bereich der digitalen Kommunikation weiter ausgehöhlt werden (D). Im Ergebnis sehen wir den Gesetzgeber in der Pflicht, einen neuen, praxistauglichen Rechtsrahmen für den Zugriff auf digitale Kommunikation zu schaffen und einen angemessen Ausgleich von verfassungsrechtlichen Schutzpositionen und der Interesse an der Aufklärung von Straftaten zu schaffen (E).

10 Gem. Art. 4 Abs. 1 lit. c) der europäischen Datenschutzrichtlinie 95/46/EG ist mitgliedstaatliches Datenschutzrecht dann anwendbar, wenn der Verantwortliche zum Zwecke der Datenverarbeitung auf Mittel zurückgreift, die auf dem Hoheitsgebiet eines Mitgliedstaates belegen sind. Legt man die Bestimmung mit der *Art. 29 Data Protection Working Party* weit aus, ist richtlinienumsetzendes Datenschutzrecht dann auf Unternehmen mit Niederlassungen in Drittstaaten anwendbar, wenn die Unternehmen eine Tätigkeit in einem Mitgliedstaat ausüben und dabei die nach außen hin erkennbare Absicht der Datenverarbeitung haben, vgl. Opinion 8/2010 on applicable law (WP 179) v. 16.12.2010, S. 20. Gem. § 1 Abs. 5 BDSG dürften das BDSG und die §§ 11 ff. TMG daher auch für Facebook gelten. Zur Jurisdiktionsproblematik *A. Chander*, Facebookistan, North Carolina Law Review 90 (2012), S. 1807 (1834 f.).

11 *G. C. Shaffer*, Globalization and Social Protection: The Impact of EU and International Legal Rules in The Ratcheting Up of U.S. Data Privacy Standards, Yale Journal of International Law 25 (2000), S. 1 (55-79); *A. Bradford*, The Brussels Effect, Northwestern University Law Review 107 (2012), S. 1 (22-26).

12 *P. M. Schwartz*, The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures, Harvard Law Review 126 (2013), S. 1966 (1973 ff.).

B. Der „Pionier-Beschluss“ des AG Reutlingen

Bislang ist es in Deutschland – soweit ersichtlich – noch nicht zur Beschlagnahme eines Facebook-Accounts gekommen.[13] Am weitesten wagte sich kürzlich das AG Reutlingen auf dem juristisch wenig vermessenen, politisch aber äußerst verminten Terrain im Grenzbereich von IT- und Strafprozessrecht vor.[14] Per Beschluss ordnete es in einem Verfahren wegen Beihilfe zum Wohnungseinbruchsdiebstahl die „Beschlagnahme“ des Facebook-Benutzerkontos des heranwachsenden Angeklagten ohne dessen Wissen an.[15] Davon erfasst sein sollten nicht nur ein- und ausgehende Messages und Chats des Angeklagten, sondern auch sämtliche gelesenen und ungelesenen, bereits in seinem Postfach gespeicherten Messages und Chats, Entwürfe von Nachrichten im Gewahrsam des Providers, die Registrierungsdaten sowie die vollständigen (öffentlichen und nicht-öffentlichen) Datensätze, insbesondere „Messages“, „Friends“, „Notes“, „Chats“, „E-Mails“ und Lichtbilder. Der Beschluss verneint ausdrücklich die Annahme, eine derartige Maßnahme sei als Telekommunikationsüberwachung zu qualifizieren und daher an § 100a StPO zu messen. Stattdessen stützt er sich auf eine analoge Anwendung der Bestimmungen über die Postbeschlagnahme (§ 99 StPO). Da keine Katalogtat nach § 100a StPO angeklagt war, kam der Frage nach der richtigen Ermächtigungsgrundlage auch entscheidende Bedeutung zu.

Dass die von manchem erhoffte Klärung der Rechtslage bislang dennoch ausgeblieben ist, verdankt sich einerseits der Kooperationsbereitschaft des Angeklagten und andererseits der Widerspenstigkeit der Firma Facebook.[16] Facebook Deutschland verweigerte die Herausgabe der beschlagnahmten Daten mit der Erklärung, nur die europäische Zentrale des Unternehmens in Dublin habe darauf Zugriff. Ein Rechtshilfeersuchen des Gerichts an die irischen Behörden blieb ebenfalls erfolglos, da Facebook in Irland sich darauf berief, die Daten seien auf einem zentralen Server in den USA gespeichert. Das US-amerikanische Datenschutzrecht verbiete deren Weitergabe an das deutsche Gericht.[17] Inzwischen ist das Reutlinger Strafverfahren abgeschlossen, ohne dass es zur einer Machtprobe mit dem Unternehmen gekommen wäre – wohl auch weil der Angeklagte angeboten hatte, die verlangten Daten frei-

13 Praktiker aus dem Bereich des IT-Rechts berichten jedoch Beschlagnahmebeschlüssen gegen andere, in Deutschland basierte soziale Netzwerke; vgl. etwa AG Stuttgart, Beschl. v. 10.10.2011, Az. 29 Gs 2147/11; AG Stuttgart, Beschl. v. 21.11.2011, Az. 27 Gs 2269/11 oder auch AG Stuttgart, Beschl. v. 1.6.2011, Az. 1125/11, zitiert jeweils nach *R. Kitzberger*, Der „Fall Facebook“ – weder neu noch ungewöhnlich: Behörden greifen regelmäßig auf Profil-Inhalte zu, Eintrag v. 21.2.2012 (abrufbar unter: >http://rechtsportlich.net/?p=931<).

14 Jedenfalls erregte der Reutlinger Fall das größte öffentliche Interesse.

15 Vgl. AG Reutlingen StV 2012, S. 642.

16 Vgl. Heise online, Meldung vom 29.3.2012 (abrufbar unter: >http://heise.de/-1486586<).

17 Vgl. Heise online (Fn. 16). Befremdlich wirkt dagegen der erste Schritt des Amtsrichters, den Beschluss ins Englische übersetzen und der irischen Facebook-Niederlassung direkt zustellen zu lassen. Selbstverständlich kommt dem Beschluss eines deutschen Amtsgerichts jenseits der deutschen Grenzen keine Bindungswirkung zu. Auch innerhalb der EU kann er nur im Wege der Rechtshilfe (i.d.R. auf Grundlage eines an die zuständigen Behörden gerichteten Rechtshilfeersuchens) durchgesetzt werden.

willig herauszugeben.[18] Dass eine ähnliche Problematik deutsche Gerichte in absehbarer Zeit wieder beschäftigen wird, darf indes als sichere Wette gelten. Dann dürfte auch Facebooks datenschutzrechtliche Verteidigungsstrategie gegen justizielle Begehrlichkeiten herausgefordert werden.[19] Die Untersuchung der rechtlichen Rahmenbedingungen des staatlichen Zugriffs auf personenbezogene Daten aus sozialen Netzwerken bleibt daher aktuell.

Der Reutlinger Beschluss ist im Übrigen nicht in einem juristischen Vakuum entstanden. Seine intellektuelle Abstammung steht ihm gleichsam auf die Stirn geschrieben. Schon im Rubrum lässt er erkennen, dass seine dogmatischen Väter eher in Karlsruhe als in Reutlingen zu finden sind. Die dort genannten Rechtsnormen – § 99, 100 Abs. 1, Abs. 3 S. 3 StPO – sind dieselben, die nach einer vielbeachteten Entscheidung des BGH die Beschlagnahme von E-Mails beim Provider erlauben sollen. Und in der Tat ist die Erwartung gut begründet, dass der BGH – sollte er Gelegenheit dazu erhalten – die Beschlagnahme von Facebook-Konten nach den gleichen Grundsätzen behandeln würde wie die Beschlagnahme von E-Mails beim Provider.[20] Zumindest ein Mitglied des 1. Strafsenats hat sich im Rahmen seiner Kommentierungstätigkeit bereits ausdrücklich dahingehend geäußert.[21]

Zu begrüßen wäre diese Entwicklung nicht. Schon in Bezug auf E-Mail-Kommunikation ist die besagte Rechtsprechung mit guten Gründen kritisiert worden.[22] Die

18 Zeit Online, Meldung v. 29.3.2012 (abrufbar unter: >http://www.zeit.de/digital/internet/2012-03/facebook-prozess-datenschutz<).

19 Tatsächlich kaschiert der Verweis auf das Datenschutzrecht wohl andere Erwägungen des Unternehmens. Rechtlich ruht er auf eher tönernen Füßen. Zum einen enthält das US-amerikanische Datenschutzrecht keine Vorschriften, die eine Übermittlung von Daten an ausländische Gerichtsbarkeiten grundsätzlich verbieten. Zum anderen darf Facebook laut eigener Datenschutzerklärung bei Durchsuchungsanordnungen, gerichtlichen Verfügungen oder Zwangsmaßnahmen mit Strafandrohung „auf deine Daten zugreifen, diese aufbewahren oder an Dritte weitergeben, wenn wir guten Grund zur Annahme haben, dass wir rechtlich hierzu verpflichtet sind. Dies gilt auch für Reaktionen auf Aufforderungen rechtlicher Art von Gerichtsbarkeiten außerhalb der USA, wenn wir in gutem Glauben davon ausgehen dürfen, dass die entsprechende Reaktion nach dem Recht der betreffenden Rechtsordnung vorgeschrieben ist, die Nutzer in der betreffenden Gerichtsbarkeit betrifft und mit international anerkannten Standards übereinstimmt“ (vgl. >http://de-de.facebook.com/about/privacy/other<).

20 So etwa *M. Heim*, Justiz 2.0? – Die Beschlagnahme eines Facebook-Accounts, NJW-Spezial 2012, S. 184 (184).

21 Vgl. *J. P. Graf*, in: ders. (Hrsg.), Beck'scher Online-Kommentar StPO, § 100a Rn. 32k-l sowie den verlinkten Formularbeschluss “Überwachung und Beschlagnahme von Internet-Kommunikation in Sozialen Netzwerken (Facebook ua)”, dessen Ähnlichkeit zum Beschluss des AG Reutlingen kaum zu übersehen ist.

22 Kritisch etwa *D. Brodowski*, Strafprozessualer Zugriff auf E-Mail-Kommunikation. Zugleich Besprechung zu BVerfG, Beschl. v. 16.6.2009 – 2 BvR 902/06 sowie zu BGH, Beschl. v. 31.3.2009 – 1 StR 76/09, JR 2009, S. 402 (402 ff.); *P. W. Brunst*, Anmerkung zu BVerfG, Beschl. v. 16.6.2009 – 2 BvR 902/06, CR 2009, S. 591 (591 f.); vgl. auch *B. Gercke*, Anmerkung zu BGH, Beschl. v. 31.3.2009, StV 2009, S. 623 (625-626); *N. Härting*, Beschlagnahme und Archivierung von Mails, CR 2009, S. 581 (581 ff.); *H. Krüger*, Anmerkung zu BVerfG, Beschl. v. 16.6.2009, MMR 2009, S. 680 (680 f.); *B. Sankol*, Anmerkung zu BGH, Beschl. v. 31.3.2009, K&R 2009, S. 396 (396 f.); *W. Wohlers*, in: J. Wolter (Hrsg.), SK-StPO, Systematischer Kommentar zur Strafprozessordnung, Bd. II, 4. Aufl., 2010, § 100a Rn. 32 ff.

Facebook-Problematik bündelt die dagegen vorgebrachten Einwände geradezu wie ein Brennglas und lässt die Schwächen der höchstrichterlichen Entscheidungen besonders deutlich aufscheinen. Betrachten wir also zunächst die Rechtsprechung zur E-Mail-Beschlagnahme beim Provider und die daran geäußerte Kritik etwas näher und wenden wir uns dann dem heikleren Problem ihrer Übertragung auf den Bereich der sozialen Netzwerke und den Folgen zu.

C. Der staatliche Zugriff auf E-Mail-Kommunikation

I. Ausgangsproblem

Seit langem ist hochumstritten, unter welchen Voraussetzungen die Beschlagnahme von E-Mails beim Provider zulässig sein soll.[23] Die Frage stellt sich vor allem dann, wenn ein Zugriff beim Empfänger oder Absender der Nachricht aus technischen Gründen ausscheidet. Dies wird häufig bei Nutzung des sog. Internet Message Access Protocol (IMAP) oder eines Webmailers für die E-Mail-Kommunikation der Fall sein.[24] Die Nachrichten werden in diesen Fällen nämlich nicht lokal auf den Rechnern von Absender und Empfänger gespeichert, sondern nur beim Provider vorgehalten. Ihr Abruf erfordert den Aufbau einer Internetverbindung.

In der Diskussion um die Zulässigkeitsvoraussetzungen des Zugriffs auf E-Mail-Kommunikation hat sich eine getrennte Betrachtung verschiedener Phasen eingebürgert.[25] Weniger umstritten war schon länger, dass während der Erstellung der E-Mail auf dem Rechner des Absenders und der Speicherung auf dem Rechner des Empfängers der Schutz des Telekommunikationsgeheimnisses nicht greifen sollte, während die Phasen der Versendung und der Abholung der E-Mail in den Schutzbereich von Art. 10 Abs. 1 GG fielen.[26] Kontrovers diskutiert werden dagegen insbesondere drei Konstellationen: (1) Die Beschlagnahme beim Provider des Absenders, bevor die Nachricht an den Provider des Empfängers weitergeleitet wurde, (2) die Beschlagnahme beim Provider des Empfängers, wo die E-Mail nach der Übertragung bis zu

23 Zum Streitstand ausführlich *M. Gercke/ P. W. Brunst*, Praxishandbuch Internetstrafrecht, Stuttgart 2010, Rn. 808 ff. m.w.N.

24 Beim älteren POP3-Protokoll werden die E-Mails zum Lesen, Bearbeiten und Archivieren vollständig auf den Rechner des Benutzers heruntergeladen und dann meistens vom Provider gelöscht. Die Fortentwicklung IMAP wird heute von allen gängigen E-Mail-Programmen (Outlook, Thunderbird etc.) unterstützt. IMAP erlaubt es dem Nutzer, seine E-Mails dauerhaft auf dem Mail-Server des Providers zu belassen und von überall im Internet auf diese zuzugreifen, um einzelne Nachrichten zu lesen, zu bearbeiten oder zu löschen. Webmail unterscheidet sich von IMAP lediglich dadurch, dass der Nutzer auf seine E-Mails nicht über ein lokal installiertes E-Mail-Programm, sondern über die Online-Oberfläche des Webmail-Anbieters (wie GMX, Hotmail oder web.de) zugreift.

25 Vgl. mit deutlichen Unterschieden im Einzelnen: *Brodowski*, Strafprozessualer Zugriff (Fn. 22), S. 401 (402 ff.); *Graf* (Fn. 21), § 100a Rn. 27 (sieben Phasen); *W. Bär*, in: B. von Heintschel-Heinegg/H. Stöckel (Hrsg.), KMR – Kommentar zur Strafprozessordnung, § 100a Rn. 27; *Gercke/Brunst*, Internetstrafrecht (Fn. 23), Rn. 815 f. (vier Phasen); *A. Nack*, in: R. Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung: StPO, KK-StPO, 6. Aufl., 2008, § 101a Rn. 19; *F. Palm/R. Roy*, Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte, NJW 1996, S. 1791 (1791 ff.) (drei Phasen).

26 Ausführlich *Graf* (Fn. 21), § 99 Rn. 9 f.; *Gercke/Brunst*, Internetstrafrecht (Fn. 23), Rn. 816.

ihrem Abruf zwischengespeichert wird, sowie (3) der Zugriff auf bereits „zugestellte" und gelesene, aber beim Provider weiter archivierte E-Mails.

II. Die Rechtsprechung von BGH und BVerfG

1. Der 1. Strafsenat des BGH

Eine weitverbreitete Ansicht ging bislang davon aus, dass die Beschlagnahme von E-Mails zumindest in den Konstellationen (1) und (2) einen Eingriff in das Telekommunikationsgeheimnis darstelle und daher nur nach Maßgabe des § 100a StPO zulässig sei.[27] Der 1. BGH-Strafsenat, der sich im Jahre 2009 mit der Frage nach der richtigen Ermächtigungsgrundlage auseinandersetzen musste, ist dem nicht gefolgt. In einem ebenso knappen wie aufsehenerregenden Beschluss stellte der Senat fest, dass beim Provider (zwischen)gespeicherte Daten nicht mehr Gegenstand eines Kommunikationsvorganges seien. Sie seien vielmehr „in jeder Hinsicht" mit verkörperten, bei einem Post- und Telekommunikationsdienstleister lagernden Mitteilungen wie etwa Telegrammen vergleichbar.[28] Folglich könne § 99 StPO, der die Postbeschlagnahme regelt, entsprechend angewendet werden.[29] Damit bedarf es (anders als im Rahmen des § 100a StPO) nach Ansicht des Senats für die Sicherstellung und Beschlagnahme von E-Mails beim Provider weder eines qualifizierten Tatverdachtes noch einer Katalogtat. Vielmehr soll schon der Anfangsverdacht einer einfachen Straftat ausreichen.[30]

2. Der 2. Senat des BVerfG

Fast zeitgleich mit dem BGH hat das BVerfG zur Problematik der Beschlagnahme von E-Mails beim Provider Stellung genommen und dabei einen etwas anderen Weg eingeschlagen. Die Entscheidung überrascht zunächst durch die Feststellung, die Sicherstellung und Beschlagnahme von auf dem Mailserver eines Providers gespeicherten E-Mails sei an Art. 10 Abs. 1 GG zu messen. Zwar finde während des „Ruhens" der Nachricht auf dem Mailserver keine Telekommunikation i.S.d. § 3 Nr. 22 TKG statt. Doch sei dieser technisch begründete Telekommunikationsbegriff im Rahmen des Art. 10 Abs. 1 GG nicht maßgeblich. Vielmehr komme es auf die Schutzbedürftigkeit des Grundrechtsträgers an, die sich aus der Einschaltung Dritter in den

27 Vgl. etwa LG Hamburg 2009, S. 70 (70); LG Hanau MMR 2000, S. 175 (175); *K. Gaede*, Der grundrechtliche Schutz gespeicherter E-Mails beim Provider und ihre weltweite strafprozessuale Überwachung, StV 2009, S. 96 (97); *B. Gercke*, in: ders. et al. (Hrsg.), Heidelberger Kommentar zur StPO, HK-StPO, § 100a Rn. 14; *G. Schäfer*, in: P. Rieß (Hrsg.), Löwe/Rosenberg. Die Strafprozessordnung und das Gerichtsverfassungsgesetz, LR-StPO, 25. Aufl., 2004, § 100a Rn. 58; *M. A. Zöller*, Verdachtslose Recherchen und Ermittlungen im Internet, GA 200 (2000), S. 563 (573).

28 BGH NJW 2009, S. 1828 (1828).

29 So zuvor schon *W. Bär*, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen – Gesetzliche Neuregelungen zum 1.1.2008, MMR 2008, S. 215 (218).

30 Die zwangsweise Durchsetzung des Herausgabeanspruchs ist nach Ansicht des BGH auf den in § 95 Abs. 1, 2 StPO verankerten Grundsatz zu stützen, dass richterlichen Herausgabeanordnungen Folge zu leisten ist. Zur Durchsetzung könnten deshalb die in § 70 StPO erwähnten Zwangsmittel festgesetzt werden.

Kommunikationsvorgang ergebe.[31] Auf dem Server des Providers gespeicherte E-Mails befänden sich außerhalb des Herrschaftsbereiches des Nutzers. Gleich ob dieser die Nachrichten noch nicht gelesen oder nach dem Lesen zur Endspeicherung auf dem Server belassen habe, in jedem Fall bleibe der Provider in ihre Verwaltung involviert.[32] Der daraus resultierende, technisch bedingte Mangel an Beherrschbarkeit erfordere den besonderen Schutz des Telekommunikationsgeheimnisses.

Ungleich überraschender sind jedoch die sich anschließenden Ausführungen des BVerfG zu den strafprozessualen Eingriffsvoraussetzungen. Aus der Betroffenheit des Telekommunikationsgeheimnisses will das Gericht nämlich nicht folgern, dass der Zugriff den strengen Voraussetzungen des § 100a StPO zu unterwerfen wäre. Da „die Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers in der Regel nicht heimlich, sondern offen vollzogen wird, die Daten punktuell und auf den Ermittlungszweck begrenzt außerhalb eines laufenden Kommunikationsvorganges erhoben werden und der Betroffene Einwirkungsmöglichkeiten auf den von ihm auf dem Mailserver seines Providers gespeicherten E-Mail-Bestand hat“,[33] andererseits das Strafverfolgungsinteresse des Staates schwer wiege,[34] stellten die §§ 94 ff. StPO eine verhältnismäßige Grundlage für die Maßnahme dar.[35]

Was auf Schutzbereichsebene mithilfe teleologischen Begründungsaufwands gewonnen zu sein scheint, ist auf Rechtfertigungsebene also sogleich zerronnen. Und mehr: Das BVerfG senkt – trotz Eröffnung des Schutzbereiches von Art. 10 Abs. 1 GG – die generellen Eingriffsvoraussetzungen gegenüber dem BGH noch einmal ab.[36] Zugleich gibt das Gericht aber konkrete Hinweise zur Verhältnismäßigkeitsprüfung.[37] „Im Regelfall“ – d.h. wenn dadurch der Zweck des Zugriffs nicht verfehlt würde – sei der Postfachinhaber vor der Durchführung der Maßnahme zu unterrichten.[38] Zudem seien die Gewinnung für das Verfahren nicht erforderlicher Daten nach Möglichkeit zu vermeiden und der Schutz des Kernbereiches privater Lebensgestaltung zu gewährleisten.[39] Wo eine Selektion vor Ort nicht zu leisten ist, könne allerdings zunächst vorläufig der gesamte E-Mail-Bestand sichergestellt werden. Vor der

31 BVerfGE 124, 43 (55, 56).

32 BVerfGE 124, 43 (56).

33 BVerfGE 124, 43 (65).

34 BVerfGE 124, 43 (63, 64).

35 BVerfGE 124, 43 (61).

36 Der wesentliche Unterschied zwischen der Beschlagnahme nach §§ 94, 98 StPO einerseits und § 99 StPO andererseits liegt in der Regelung des § 100 Abs. 1 StPO. Danach liegt die Anordnungskompetenz für die Postbeschlagnahme grundsätzlich beim Ermittlungsrichter. Auch eine Durchsicht der Nachrichten ist der Staatsanwaltschaft nicht gestattet, vgl. *Nack* (Fn. 25), § 100a Rn. 22.

37 BVerfGE 124, 43 (66 ff.).

38 BVerfGE 124, 43 (71).

39 Das ist an sich nichts Besonderes, sondern lediglich eine richterliche Ausformulierung des Gebotes der Datensparsamkeit oder der Datenvermeidung, das sich aus dem verfassungsrechtlichen Übermaßverbot ableiten lässt, vgl. *P. Scholz*, in: S. Simitis (Hrsg.), BDSG, 7. Aufl., 2011, § 3a Rn. 19.

Entscheidung über die endgültige Beschlagnahme sei dann eine Durchsicht gem. § 110 StPO durchzuführen, in die der Inhaber der E-Mails „im Einzelfall" einzubeziehen sei.[40]

3. Der 3. Strafsenat des BGH

Schließlich hatte in kurzer Folge auch der 3. BGH-Strafsenat Gelegenheit, sich zur Problematik der E-Mail-Beschlagnahme beim Provider zu äußern.[41] Dessen Entscheidung hat vor allem wegen ihrer konkretisierenden Ausführungen zur Verhältnismäßigkeit des Zugriffs*umfanges* für Aufsehen gesorgt. Insbesondere beim Zugriff auf große Datenbestände sind demnach geeignete Maßnahmen zu treffen, um die Gewinnung für das Verfahren bedeutungsloser oder einem Beschlagnahmeverbot nach § 97 StPO unterliegender Daten zu vermeiden.[42] Die Beschlagnahme des gesamten E-Mail-Verkehrs verstößt nach Auffassung des 3. Strafsenats mangels zu erwartender Beweisbedeutung regelmäßig gegen das Übermaßverbot.

Der Beschluss hatte neben der Beschlagnahme der bereits im Postfach des Accounts eingegangenen E-Mails auch die fortlaufende Überwachung und Aufzeichnung der über einen E-Mail-Account geführten Kommunikation für einen zukünftigen Zeitraum zum Gegenstand. Der 3. Strafsenat differenziert zwischen beiden Abschnitten und wendet in Bezug auf zukünftige E-Mail-Kommunikation § 100a StPO an. Er erinnert im Anschluss an das BVerfG daran, dass es sich bei der Beschlagnahme um eine „offene Ermittlungsmaßnahme" handele, deren Anordnung dem Betroffenen bekannt zu machen sei. Eine Zurückstellung der Benachrichtigung wegen Gefährdung des Untersuchungszwecks analog § 101 Abs. 5 StPO komme aber nur bei den in § 101 Abs. 1 StPO abschließend aufgezählten heimlichen Ermittlungsmaßnahmen in Betracht.[43]

4. Ein Systematisierungsversuch

Die drei Entscheidungen erfordern den Versuch einer Systematisierung.

Eindeutig dürfte sein, dass die Rechtsprechung den *offenen* und *punktuellen* Zugriff auf beim Provider gespeicherte E-Mails künftig nach den allgemeinen Bestimmungen der §§ 94 ff. StPO zulassen wird. Dass entsprechende Maßnahmen daneben auch weiterhin auf andere Rechtsgrundlagen gestützt werden können, hat das BVerfG mit

40 BVerfGE 124, 43 (72).

41 Vgl. BGH NJW 2010, S. 1297.

42 Dazu schon oben, Fn. 38.

43 BGH NJW 2010, S. 1297 (1298); anders bisher *L. Meyer-Goßner*, Beck'scher Kurz-Kommentar zur StPO, 55. Aufl., 2012, § 98 Rn. 10; *Nack* (Fn. 25), § 98 Rn. 21; kritisch *W. Winkler*, Beschlagnahme von gespeicherten E-Mails, juris PraxisReport Strafrecht 10/2010, Anm. 3 lit. D).

Blick auf § 99 StPO und die Entscheidung des 1. Strafsenats ausdrücklich anerkannt.[44]

Weniger klar ist jedoch, was für die *verdeckte*[45] und/oder *laufende* Beschlagnahme von E-Mails gelten soll. Das Abgreifen noch nicht bei bestimmungsgemäßen Empfänger angelangter E-Mails, um das es auch in der Entscheidung des 3. Strafsenates ging, kann sinnvollerweise nie offen erfolgen, da ansonsten der Zweck der Maßnahme konterkariert würde. Eine laufende E-Mail-Beschlagnahme wird also in aller Regel zugleich eine verdeckte Maßnahme darstellen.[46] Namentlich *Graf* will auch in solchen Fällen weiterhin eine Anordnung nach § 99 StPO (analog) ausreichen lassen, da die zu beschlagnahmenden E-Mail-Sendungen nicht mehr Gegenstand eines aktuell andauernden Telekommunikationsvorgangs seien, sobald sie sich im Gewahrsam des Mail-Providers befänden.[47] Andere halten dies nach der Entscheidung des BVerfG nicht mehr für zulässig. Nach dieser Auffassung hat das BVerfG die Hürden für einen offenen Zugriff zwar gesenkt, für verdeckte Maßnahmen jedoch erhöht.[48]

Auch wenn die Ausführungen des BVerfG nicht durchgehend so eindeutig sind, wie es teilweise dargestellt wird,[49] sprechen die besseren Gründe dafür, dass die laufende verdeckte Beschlagnahme von E-Mails nur entsprechend § 100a StPO mit den Vorgaben des Gerichts vereinbar sein dürfte.[50] Diese Auffassung erfährt auch Bestätigung durch die zitierte Entscheidung des 3. Strafsenats, der zutreffend von einer „Überwachung" spricht[51] und diesbezüglich auf § 100a StPO zurückgreift. Das heimliche Abgreifen des E-Mail-Verkehrs über einen längeren Zeitraum ist das genaue Gegenteil des vom BVerfG für unbedenklich gehaltenen Falles.[52]

Im Ergebnis ist daher festzuhalten, dass nur der einmalige, punktuelle und offene Zugriff beim Provider nach §§ 94 ff. StPO zulässig ist, die heimliche und/oder lang-

44 BVerfGE 124, 43 (59); weiterhin für die Anwendung des § 99 StPO, da diese Norm der Bedeutung und Eingriffstiefe der Maßnahme besser gerecht werde, *Graf* (Fn. 21), § 100a Rn. 30; offen gelassen bei *Nack* (Fn. 25), § 100a Rn. 22.

45 Ein solcher Fall lag wohl der Entscheidung des 1. Strafsenats zugrunde, vgl. *Brodowski*, Strafprozessualer Zugriff (Fn. 22), S. 402 (407).

46 Umgekehrt gilt dies nicht. Auch punktuelle Zugriffe können heimlich erfolgen.

47 Vgl. *Graf* (Fn. 21), § 100a Rn. 30 und den verlinkten Musterbeschluss "Beschlagnahme von E-Mails für einen künftigen Zeitraum nach § 99 StPO".

48 *O. Klein*, Offen und (deshalb) einfach – Zur Sicherstellung und Beschlagnahme von E-Mails beim Provider, NJW 2009, S. 2996 (2999); vgl. auch *N. Szebrowski*, Anmerkung zu BVerfG, Beschl. v. 16.6.2009, K&R 2009, S. 563 (564).

49 Dazu *Brodowski*, Strafprozessualer Zugriff (Fn. 22), S. 402 (407).

50 *Brunst*, Anmerkung zu BVerfG (Fn. 22), S. 591 (592); *Klein*, Offen und (deshalb) einfach (Fn. 48), S. 2996 (2999); *Krüger*, Anmerkung zu BVerfG (Fn. 22), S. 680 (683).

51 So auch *Brodowski*, Strafprozessualer Zugriff (Fn. 22), S. 402 (406).

52 Vgl. *Meyer-Goßner* (Fn. 43), § 100a Rn. 6b.

fristige[53] E-Mail-Überwachung aber auch künftig nur unter den strengeren Voraussetzungen des § 100a, b StPO erlaubt sein dürfte.[54]

III. Kritik

Die Rechtsprechung von BGH und BVerfG ist mit guten Gründen kritisiert worden. Die Anwendung der Beschlagnahmevorschriften auf E-Mails stößt auf grundsätzliche Einwände. Zweifelhaft ist bereits, ob die Vorschriften über die Beschlagnahme überhaupt auf nicht-körperliche Gegenstände passen.[55] Das BVerfG hält eine derart weite Deutung für mit dem Wortsinn vereinbar. Beschlagnahmefähig seien grundsätzlich alle Gegenstände, die als Beweismittel für das Strafverfahren von Bedeutung sein können.[56] Und auch der BGH erachtet den Zugriff auf E-Mails als „in jeder Hinsicht vergleichbar" mit der Beschlagnahme verkörperter Postsendungen.[57] Dagegen ist mit Recht darauf hingewiesen worden, dass die §§ 94 ff. StPO erkennbar auf die körperliche Welt zugeschnitten sind.[58] Von der „Verwahrung" oder „Herausgabe" einer E-Mail zu sprechen, ergibt schon deshalb wenig Sinn, weil die Sicherstellung bzw. Beschlagnahme im Regelfall durch die Anfertigung einer Kopie erfolgen wird. Trotz „Beschlagnahme" einer E-Mail kann diese also im „Gewahrsam" des Empfängers verbleiben – eine in Bezug auf körperliche Gegenstände nicht denkbare Situation.

Diese grammatischen Argumente spiegeln tieferliegende normative Unterschiede zwischen dem staatlichen Zugriff auf elektronische Kommunikation und der Beschlagnahme körperlicher Gegenstände wider. Der Zugriff auf E-Mails ist einerseits milder als die klassische Beschlagnahme, weil dadurch dem Betroffenen die Möglichkeit zur Verfügung über gespeicherte Kommunikationsvorgänge in der Regel nicht genommen wird.[59] Andererseits kann er aber auch deutlich eingriffsintensiver ausfallen. Wird auf ein Bündel von E-Mails zugegriffen, ist der in die private Lebensgestaltung gewährte Einblick in der Regel umfassender als bei einer einfachen Postbeschlagnahme gem. § 99 StPO.

53 Dazu dürften auch wiederholt punktuelle Zugriffe gehören, da ansonsten die Umgehungsgefahr zu groß wäre. Irgendwann schlügen diese Wiederholungen in eine laufende Überwachung um.

54 *Gercke/Brunst*, Internetstrafrecht (Fn. 23), Rn. 820; *Klein*, Offen und (deshalb) einfach (Fn. 48), S. 2996 (2999); *Krüger*, Anmerkung zu BVerfG (Fn. 22), S. 680 (683).

55 Soweit bislang von der „Beschlagnahme von Daten" die Rede war, war damit primär die Beschlagnahme des Datenträgers gemeint; vgl. BVerfGE 115, 166 – Bargatzky; *W. Beulke*, Strafprozessrecht, 12. Aufl., 2012, Rn. 253b.

56 BVerfGE 124, 43 (60, 61).

57 BGH NJW 2009, S. 1828.

58 *Brunst*, Anmerkung zu BVerfG (Fn. 22), S. 591 (592); krit. auch *C. Roxin/B. Schünemann*, Strafverfahrensrecht, 27. Aufl., 2012, § 34 Rn. 4.

59 Ausgeblendet sei hier das *topische* Gegenargument, dass der Einzelne es auch bei körperlichen Gegenständen grundsätzlich in der Hand hätte, die Intensität der Beschlagnahme durch die Anfertigung von Kopien abzumildern. Digitale Informationen unterscheiden sich nämlich insofern von körperlichen Gegenständen, als ihre Vervielfältigung naturgemäß nur marginale Grenzkosten verursacht. Zur Gültigkeit *topischer* Argumente *I. Puppe*, Kleine Schule des Juristischen Denkens, 2008, S. 175 f.

Inkonsistent wirkt es, wenn das BVerfG zwar unter Verweis auf die Schutzbedürftigkeit (zwischen)gespeicherter E-Mails das Telekommunikationsgeheimnis als betroffen ansieht, in strafprozessualer Hinsicht jedoch keinerlei Konsequenzen hieraus ziehen will.[60] Nicht ganz zu Unrecht wurde dem Gericht vorgeworfen, auf diese Weise ein „Fernmeldegeheimnis light" zu schaffen.[61] Besonders deutlich wird der innere Widerspruch, wenn einerseits auf verfassungsrechtlicher Ebene die Eröffnung des Schutzbereiches von Art. 10 Abs. 1 GG mit der fehlenden Beherrschbarkeit der beim Provider lagernden E-Mails begründet wird, andererseits aber in strafprozessualer Hinsicht die dem Betroffenen offenstehende Möglichkeit, auf den eigenen E-Mail-Bestand einzuwirken, als Argument gegen den erhöhten prozeduralen Schutz des § 100a StPO angeführt wird.[62]

Wenig überzeugend ist überdies die Annahme, dass die Eingriffsintensität eines (1) punktuellen, (2) offenen, (3) außerhalb eines laufenden Kommunikationsvorgangs erfolgenden Zugriffs stets als gering anzusehen sei.

Hinter dem scheinbar klaren Begriff des „Punktuellen" kann sich ganz Unterschiedliches verbergen. Im Extremfall erstreckt sich ein „punktueller" Zugriff auf ein Archiv tausender, über Jahre hinweg ausgetauschter Nachrichten.[63] Dass eine Vorselektion anhand von Schlagwörtern, Zeitfenstern oder Absendernamen, wie sie sich die Rechtsprechung vorstellt, in der Praxis Fuß fassen wird, ist mit Recht bezweifelt worden. Eine granulare Sortierung digitaler Information ist (jedenfalls bis dato) schon aus technischen Gründen kaum zu bewerkstelligen.[64] Auch in Zukunft dürfte die vorläufige Sicherstellung zumindest eines großen Teils des Datenbestandes sowie dessen anschließende Sichtung zur Entscheidung über die endgültige Beschlagnahme der Regelfall bleiben.[65] Die Punktualität des Zugriffs zieht also nicht so sehr der zu erhebenden Informationsmenge Grenzen, sondern beschreibt nur die Einmaligkeit des Zugriffs.

Auch der Begriff der Offenheit, dem die Rechtsprechung große Bedeutung zumisst, entpuppt sich bei näherer Betrachtung als Mirage. Dem Grundsatz, dass heimliche Ermittlungsmaßnahmen an strengeren Maßstäben gemessen werden müssen als offen vollzogene, wird freilich niemand widersprechen. Er ist unmittelbar einleuchtend: Der Betroffene kann sich nur gegen eine Maßnahme wehren, von der er Kenntnis

60 *Härting*, Beschlagnahme (Fn. 22), S. 581 (583); *Krüger*, Anmerkung zu BVerfG (Fn. 22), S. 680 (682 f.).

61 *Härting*, Beschlagnahme (Fn. 22), S. 581 (583).

62 *Brunst*, Anmerkung zu BVerfG (Fn. 22), S. 591 (592); dies dürfte gegen das Gebot der Widerspruchsfreiheit verstoßen, s. dazu *Puppe*, Juristisches Denken (Fn. 59), S. 67-71.

63 *T. Schwabenbauer*, Kommunikationsschutz durch Art. 10 GG im digitalen Zeitalter, AöR 137 (2012), S. 1 (29).

64 Vgl. *Brunst*, Anmerkung zu BVerfG (Fn. 22), S. 591 (593).

65 *Gercke/Brunst*, Internetstrafrecht (Fn. 23), Rn. 822.

hat. Höchst fragwürdig ist allerdings die Annahme, die Beschlagnahme von E-Mails beim Provider sei in diesem Sinne „offen". Praktisch wird sie meist durch Erstellung einer Kopie der relevanten Nachrichten vollzogen. Der Nutzer hat keine Möglichkeit, dies zu erkennen.[66] Dass seine Anwesenheit während des Zugriffs nicht in jedem Falle erforderlich ist, hat das BVerfG zudem ausdrücklich festgehalten.[67] Die grundsätzlich vorgesehene *vorherige* Anhörung wird zudem regelmäßig nicht stattfinden, um den Ermittlungszweck nicht zu gefährden (§ 33 Abs. 4 StPO).[68] Auch wenn der 3. Strafsenat des BGH inzwischen klargestellt hat, dass eine noch weitergehende Zurückstellung auch der *nachträglichen* Benachrichtigung entsprechend § 101 Abs. 5 StPO bei der Beschlagnahme nicht in Betracht kommt, so werden dem Betroffenen doch wesentliche Rechtsschutzmöglichkeiten abgeschnitten. Die nachträgliche Information, dass der eigene E-Mail-Bestand beim Provider sichergestellt worden sei, lässt sich nicht mit dem Fall einer Hausdurchsuchung vergleichen, während deren der Betroffene stets einen Rechtsbeistand hinzuziehen und ggf. unmittelbar gegen eine Sicherstellung protestieren kann.[69]

Zweifelhaft ist schließlich auch die Feststellung, die Beschlagnahme beim Provider greife nicht in einen laufenden Kommunikationsvorgang ein. Die von der Rechtsprechung vollzogene Aufspaltung in statische und dynamische Phasen mutet beinahe sophistisch an. Von einer Beendigung der Übertragung kann technisch nicht gesprochen werden, wenn die Kenntnisnahme durch den Empfänger noch einen weiteren Telekommunikationsvorgang – den Abruf der E-Mail durch den Empfänger – voraussetzt.[70] Auch verringert sich die Schutzbedürftigkeit des Nutzers nicht dadurch, dass die E-Mail beim Provider „ruht". Das BVerfG erkennt dies selbst an, wenn es auch in diesen Phasen den Schutzbereich des Art. 10 Abs. 1 GG mit dem Hinweis auf die fortbestehende „spezifische Gefährdungslage" als eröffnet ansieht. Abgeschlossen kann die Nachrichtenübermittlung folglich erst dann sein, wenn die zur Übermittlung eingeschaltete dritte Stelle nicht mehr involviert ist.[71]

Die Gegenansicht misst technischen Zufälligkeiten eine ungebührlich große Bedeutung bei.[72] Zunehmend wird die Vorstellung einer statischen „Lagerungsphase"

66 *Brunst*, Anmerkung zu BVerfG (Fn. 22), S. 591 (592).

67 BVerfGE 124, 43 (72).

68 Vgl. die Formularbeschlüsse „Einmalige Beschlagnahme des E-Mail-Bestandes beim Provider nach §§ 94 StPO ff" und „Beschlagnahme von E-Mails für einen künftigen Zeitraum nach § 99 StPO", in: *Graf* (Fn. 21), Formulare.

69 *Brunst*, Anmerkung zu BVerfG (Fn. 22), S. 591 (592) weist zutreffend darauf hin, dass die der verfassungsgerichtlichen Entscheidung zugrundeliegende Konstellation – Beschlagnahmebeschluss während einer laufenden Durchsuchung und Einholung in Anwesenheit des Betroffenen – eher selten vorkommen dürfte.

70 *S. Schlegel*, „Beschlagnahme" von E-Mail-Verkehr beim Provider, HRRS 2007, S. 44 (47).

71 Zutreffend *Schlegel*, „Beschlagnahme" (Fn. 70), S. 44 (48).

72 *Gercke/Brunst*, Internetstrafrecht (Fn. 23) Rn. 825.

nämlich durch neue Techniken wie Push-Mail in Frage gestellt.[73] Bei diesem Verfahren wird eine eingehende Nachricht sofort vom Server an den E-Mail-Client (Mobiltelefon, IMAP-basiertes Mail-Programm auf dem Desktop) „weitergeschoben". Überzeugender wäre es daher gewesen, auch in strafprozessualer Hinsicht von einem einheitlichen Kommunikationsvorgang auszugehen, der staatliche Eingriffe nur nach Maßgabe des § 100a StPO erlaubt.[74]

D. Die Problematik sozialer Netzwerke

Wie bereits einleitend festgestellt, spricht alles dafür, dass die Rechtsprechung auch die „Beschlagnahme" von Facebook-Nutzerkonten nach den eben dargestellten Grundsätzen behandeln wird.[75] Zu begrüßen wäre dies nicht. Die Übertragung der von BGH und BVerfG in Bezug auf E-Mails entwickelten Ansätze auf Facebook-Profile lässt deren Unausgegorenheit noch deutlicher zu Tage treten. Sie lässt erkennen, welche Gefahren eine Rechtsanwendung birgt, die neue technologische Entwicklungen nach dem Prokrustesprinzip in die Auslegung altbekannter Rechtsnormen hineinzwängen möchte.[76] Facebook ist weit mehr als eine Plattform zum Austausch E-Mail-ähnlicher elektronischer Nachrichten. Die Vielfalt seiner kommunikativen Funktionen lässt diese Art des Austausches sogar beinahe in den Hintergrund treten.[77] Das Wort „Beschlagnahme" will deshalb in Bezug auf einen Facebook-Account noch weniger passen. Tatsächlich scheint auch manchen Richtern nicht ganz klar zu sein, was es eigentlich ist, das beschlagnahmt werden soll. Dies liegt weniger an mangelndem *technischem* Verständnis als an einem gering ausgeprägtem Gespür für die *soziale* Dimension der Technologie, einem Symptom der fehlenden Erfahrung mit ihrer alltäglichen Nutzung.[78]

Im Folgenden möchten wir zeigen, weshalb Nutzerkonten in sozialen Netzwerken die Sollbruchstellen der bisherigen Rechtsprechung zur E-Mail-Beschlagnahme noch klarer hervortreten lassen. Dabei beginnen wir mit der Beschlagnahme von über

73 *Brunst*, Anmerkung zu BVerfG (Fn. 22), S. 591 (592).

74 So ein Gutteil der Literatur, vgl. etwa *Brodowski*, Strafprozessualer Zugriff (Fn. 22), S. 402 (411); *Brunst*, Anmerkung zu BVerfG (Fn. 22), S. 591 (592); *Gercke* (Fn. 27), § 100a Rn. 14; *Krüger*, Anmerkung zu BVerfG (Fn. 22), S. 680 (682 f.); *Schäfer* (Fn. 27), § 100a Rn. 58; *Schlegel*, „Beschlagnahme" (Fn. 70), S. 44 (47); *M. Störing*, Strafprozessualer Zugriff auf E-Mailboxen, CR 2009, S. 475 (477 f.); *Schwabenbauer*, Kommunikationsschutz (Fn. 63), S. 1 (29).

75 So etwa *D. Neuhöfer*, Zugriff auf Facebook-Nachrichten im Strafverfahren, MMR-Aktuell 2012, 329250.

76 Die richterliche Pflicht, das praktische Rechtsproblem entscheiden zu müssen, sei dabei nicht geleugnet.

77 Dazu im nächsten (Unterschiedlichen Funktionen bei Facebook).

78 Wie sehr der grundrechtliche Schutz der Privatheit vom richterlichen Verständnis sozialer Medien abhängen kann, belegen jüngere Entscheidungen US-amerikanischer Gerichte in aller Deutlichkeit, vgl. *United States v. Jones* vom 23.1.2012, No. 10-1259, at 3-6 (*S. Sotomayor*, J., concurring). S. auch *T. Friedkin*, Do Judges Understand Technology? Does It Matter?, The Official Blog of the Hofstra Labor & Employment Law Journal v. 5.9.2012 (abrufbar unter: >http://thelejer.wordpress.com/2012/09/05/do-judges-understand-technology-does-it-matter-2/<).

Facebook ausgetauschten Mitteilungen und Chats, wie sie das AG Reutlingen anordnen wollte. Hier ist die Parallele zur E-Mail-Beschlagnahme auch am deutlichsten. Im darauffolgenden Abschnitt gehen wir kursorisch auf die Vielzahl anderer Funktionen ein, die ein Facebook-Nutzer in Anspruch nehmen kann. Daran sollte endgültig deutlich werden, dass jede Lösung, die neuen Wein in alte juristische Schläuche gießen will, mehr Probleme aufwirft als sie löst.

I. Messages und Chats

Dass der Austausch von Nachrichten über Facebook ebenso wie die Kommunikation via E-Mail *in toto* den Schutz des Art. 10 GG genießt, dürfte nach der Entscheidung des BVerfG nicht mehr kontrovers sein. Blickt man auf die Historie von Art. 10 Abs. 1 GG, liegt es außerdem nahe, seinen Schutzbereich auf die Kommunikation in sozialen Netzwerken wie Facebook auszudehnen.

Ursprünglich bestand das den Grundrechtsschutz begründende Risiko darin, dass die Post durch ein staatliches Monopol betrieben wurde, dem der Einzelne seine Briefsendungen anvertrauen musste. Da der Einzelne auf den monopolistisch organisierten Postverkehr angewiesen war, war die Entscheidungsfreiheit bei der Inanspruchnahme von Post- und Telekommunikationsdienstleistungen erheblich eingeschränkt.[79] Auch Facebook hat mittlerweile ein Monopol auf dem Markt für soziale Netzwerke und kann deshalb Bedingungen und Prozess der Kommunikation weitgehend autonom gestalten.[80] Selbst wenn die Aussage, der Einzelne sei in ähnlicher Weise auf Facebook angewiesen wie früher auf das Postamt, übertrieben anmuten mag, lässt sich angesichts von mehr als einer Milliarde Nutzer weltweit – und immerhin knapp 25 Millionen Nutzern in Deutschland[81] – die soziale Funktion des Netzwerks nicht einfach leugnen.

Doch was folgt daraus und aus der grundrechtlichen Gewährleistung für die einfachgesetzlichen Eingriffsvoraussetzungen? In seiner Entscheidung zur Vorratsdatenspeicherung hat das BVerfG betont, dass der Zugriff auf umfassende Datenbe-

79 *M. Pagenkopf*, in: M. Sachs (Hrsg.), Grundgesetz Kommentar, 5. Aufl., 2009, Art. 10 Rn. 13.

80 Gegenwärtig verfügt Facebook auf dem deutschen Markt für soziale Netzwerke über einen Marktanteil von 77,5 % (vgl. >http://www.socialmediastatistik.de/marktanteile-der-sozialen-dienste-statcounter/<). Insoweit dürfte Facebook jedenfalls nach deutschem Kartellrecht eine marktbeherrschende Stellung innehaben, da eine solche gem. § 19 Abs. 3 S. 1 GWB bei einem Marktanteil von einem Drittel vermutet wird, vgl. *N. Härting*, Facebook – ein „Monopol"?, Eintrag v. 1.3.2012 (abrufbar unter: >http://www.cr-online.de/blog/2012/03/01/facebook-ein-monopol/<). Im Übrigen bedingen die für Netzindustrien typischen Netzwerkeffekte einen starken *Lock-In*, der das Ausweichen auf Alternativangebote kostspielig macht, vgl. *C. S. Yoo*, When Antitrust Met Facebook, George Mason Law Review 19 (2012), S. 1147 (1148-1154). Aus diesem Grund wird momentan auch diskutiert, ob soziale Medien nicht als öffentliche Infrastrukturen (sog. *essential utilities*) qualifiziert und strengerer staatlicher Regulierung unterworfen werden sollten, vgl. *A. Thierer*, The Perils of Classifying Social Media Platforms as Public Utilities, Working Paper No. 12-11, March 2012.

81 Quelle: Statista (abrufbar unter: >http://de.statista.com/statistik/daten/studie/70189/umfrage/nutzer-von-facebook-in-deutschland-seit-2009/<).

stände, die verdachtslos gespeichert werden, nur unter besonders strengen Voraussetzungen zulässig sei darf.[82] Dies soll umso mehr gelten, wenn der Betroffene keine Möglichkeiten zur Einwirkung auf den Datenbestand hat.[83] Dass das Gericht in Bezug auf beim Provider gespeicherte E-Mails derartige Umstände nicht als gegeben ansah,[84] ist teilweise kritisiert worden.[85] Denn der Inhaber kann E-Mails, von denen er Kenntnis hat, zwar aus seinem Postfach löschen. Die Löschung von E-Mails auf dem Providerserver dürfte der Einzelne aber schwerlich beeinflussen können.[86]

A fortiori lässt sich dieses Argument in Bezug auf Facebook ins Feld führen. Denn ob und wann genau Facebook gespeicherte Nutzerdaten im Allgemeinen löscht, ist und bleibt die eigentliche Gretchenfrage in der Diskussion um die Beherrschbarkeit des Löschungsprozesses. Die Vorstellung, Facebook-Daten seien auf einem zentralen Server in Prineville, Oregon, gespeichert und könnten durch einen einfachen *actus contrarius* gelöscht werden, stammt aus einer Zeit, zu der das kommerzielle Internet noch im Entstehen begriffen war – den frühen 1990er Jahren. Nach aktuellen Schätzungen verfügt Facebook über rund 180 000 Server,[87] auf denen inzwischen über 100 Petabytes (100 000 000 MB) an Videos und Fotos gespeichert sind.[88] Erst kürzlich wurde bekannt, dass Facebook sämtliche Daten einiger Nutzer dauerhaft gespeichert hatte – und zwar obwohl die Betroffenen sie über die Benutzeroberfläche längst „gelöscht" hatten.[89] Das Bild des im Postverteilzentrum lagernden Telegramms passt mithin auf Facebook-Nachrichten noch schlechter als auf E-Mails. Facebook entspricht – zugespitzt formuliert – einem Postamt, wo jeder Brief geöffnet, kopiert und unbegrenzt archiviert wird.

Auch andere Möglichkeiten des Selbstschutzes sind nur beschränkt erfolgversprechend. Zwar garantieren die meisten E-Mail-Provider, dass der E-Mail-Verkehr zwischen dem Client des Nutzers und den Servern des Providers durch den Einsatz hybrider SSL- oder TLS-Protokolle verschlüsselt abläuft.[90] Die vollständige Verschlüsselung einer E-Mail vom Sender bis zum Empfänger ist hingegen keineswegs trivial. *Mutatis mutandis* dürften die wenigsten Facebook-Nutzer überhaupt wissen, dass das Netzwerk ihnen die Möglichkeit einräumt, ihre Facebook-Verbindung via

82 BVerfGE 121, 1 (19 ff.).

83 BVerfGE 121, 1 (20); 115, 166 (194).

84 So BVerfGE 124, 43 (63).

85 Vgl. etwa *Brodowski*, Strafprozessualer Zugriff (Fn. 22), S. 402 (406).

86 Dies außer Acht lassend *W. Durner*, in: Maunz/Dürig. Grundgesetz Kommentar, (EL 67, 2013), Art. 10 Rn. 99.

87 Vgl. >http://gigaom.com/cleantech/facebooks-number-of-servers-soar-to-an-estimated-180k/<.

88 Dies geht aus dem zur Börsenregistrierung bei der *US Securities and Exchange Commission* eingereichten S-1 Formular vom 1.2.2012 hervor.

89 Dies ergibt sich aus dem Bericht der irischen Datenschutzbehörde *Office of the Data Protection Commissioner of Ireland*, Report of Audit „Facebook Ireland Ltd" v. 21.12.2011, S. 69 ff.

90 Das Secure Sockets Layer-Protokoll (SSL) wird seit Version 3.0 als Transport Layer Security-Protokoll (TLS) weitergeführt.

HTTPS (Hypertext Transfer Protocol Secure) abzusichern. Nachrichten, Chats und Statusmeldungen werden ohne eine solche Verschlüsselung im Klartext übermittelt und können gerade bei der Nutzung öffentlicher Netzwerke problemlos abgefangen oder „überwacht" werden. Doch selbst Nutzer, die so weit in die Kontoeinstellungen vordringen, um die kryptographischen Standardeinstellungen manuell zu verändern, sind hierdurch kaum vor einem Eindringen in ihre Privatsphäre gefeit. Durch BEAST-Attacken (Browser Exploit Against SSL/TLS) können inzwischen auch via HTTPS chiffrierte Verbindungen (bspw. bei Twitter, Gmail oder Dropbox) problemlos „gehackt" werden.

Wenn die eingeschränkte technische Beherrschbarkeit der eigenen Daten mit dem Argument für unbeachtlich erklärt wird, der Nutzer habe „sich aus freien Stücken entschlossen, das seit längerer Zeit umstrittene und in der öffentlichen Diskussion stehende Angebot der Fa. Facebook zu verwenden",[91] kann dies nicht überzeugen. Das Argument erinnert an die US-amerikanische Konzeptionalisierung des Rechts auf Privatheit unter dem *Fourth Amendment*. Immer öfter greifen US-amerikanische Strafverfolgungsbehörden auf Informationen aus sozialen Netzwerken zurück.[92] Die rechtlichen Grenzen des staatlichen Zugriffs auf persönliche Informationen aus sozialen Medien sind allerdings unscharf, da Gesetzgeber und Rechtsprechung bisher ausschließlich den Zugriff auf den E-Mail-Verkehr und IP-Adressen im Blick hatten.[93] So kam in jüngeren Entscheidungen wiederholt die Frage auf, ob der Einzelne sich auch dann auf den Schutz durch das *Fourth Amendment* berufen kann, wenn Beweisanordnungen an den Betreiber sozialer Netzwerke gerichtet sind. Gemäß der verfassungsrechtlichen *state action doctrine* entfaltet das *Fourth Amendment* grundsätzlich nur Schutz, soweit der Einzelne eine berechtigte Erwartung der Privatheit (*reasonable expectation of privacy*) hat.[94] Dieser auch vom EGMR bei der Auslegung von Art. 8 EMRK eingesetzte Test[95] setzt nach der Rechtsprechung des *US Supreme Court* voraus, dass der Einzelne subjektiv einen Schutz der Privatsphäre erwartet und diese Erwartung nach der vorherrschenden sozialen Anschauung als objektiv be-

91 So das AG Reutlingen StV 2012, S. 642 und wortlautgleich *Graf* (Fn. 21), Musterbeschluss „Überwachung und Beschlagnahme von Internet-Kommunikation in Sozialen Netzwerken (Facebook ua)".

92 Im Fall *People v. Liceaga* (Mich. Ct. App. 2009) wurden Bilder aus dem sozialen Netzwerk des Angeklagten als Belastungsbeweis des Vorsatzes und des Tatplans zugelassen. Im Fall *Clark v. State*, 915 N.E.2d 126, 130 (Ind. 2009), erachtete der *Indiana Supreme Court* Informationen aus einem MySpace-Profil des Angeklagten als ausreichenden Entlastungsbeweis an (sog. *character evidence* zugunsten des Angeklagten).

93 Krit. *D. Levine*, Facebook and Social Networks: the Government's Newest Playground for Information and the Laws That Haven't Quite Kept Pace, Hastings Communications and Entertainment Law Journal 33 (2011), S. 481 (496). Im Fall *United States v. Steven Warshak* (6th Cir. 2010), stellte das Gericht fest, dass das *Fourth Amendment* auch vor staatlichem Zugriff auf E-Mails schützt (bspw. vor einer Beweisanordnung nach 18 USC § 2703(d)).

94 *D. Solove*, Understanding Privacy (2008), S. 71 f.; *S. Chahal*, Balancing the Scales of Justice: Undercover Investigations on Social Networking Sites, Journal on Telecommunications and High Technology Law 9 (2011), S. 285 (292).

95 EGMR NJW 2004, S. 2647 (2650) – von Hannover/Deutschland.

rechtigt eingestuft werden kann.[96] Der Vorteil dieses rechtsdogmatischen Konzepts liegt, in „seiner Flexibilität und Anpassbarkeit an technologische und soziale Veränderungen, die sich auf soziale Privatsphärennormen auswirken".[97] In der Praxis hat sich die im *reasonable expectation of privacy*-Test angelegte normative Kraft des Faktischen allerdings äußerst korrosiv auf den Grundrechtsschutz ausgewirkt. Wie der *US Supreme Court* im Fall *United States v. Miller* ausgeführt hat, besteht keine berechtigte Erwartung, wenn der Einzelne bewusst und willentlich das Risiko eingeht, dass ihn betreffende Informationen an Dritte weitergegeben werden.[98] Dies bedeutet, dass das *Fourth Amendment* kein subjektives Recht gewährt, wenn der Einzelne ihn betreffende Informationen zuvor einem anderen anvertraut hat. Eine Informationspreisgabe etwa gegenüber Facebook wird daher als Generaleinwilligung ohne jegliche Zweckbindung interpretiert.[99] Der Einzelne kann folglich keinen Rechtsschutz gegen Beweisanordnungen geltend machen, die an Betreiber sozialer Netzwerke gerichtet sind (sog. *third party doctrine*).[100] Zwar sind Strafverfolgungsbehörden verpflichtet, vor dem Zugriff auf in sozialen Netzwerken gespeicherte Inhaltsdaten einen richterlichen Beschluss (*warrant, court order*) einzuholen.[101] Zugriffe auf Verkehrs- und Bestandsdaten sind aber nach freiem Ermessen auf Grundlage exekutiver Beweisanordnungen (*subpoenas*) ohne judikative ex ante-Kontrolle zulässig.[102] Nach eigenen Angaben gehen bei Facebook in den USA täglich zehn bis zwanzig derartiger Beweisanordnungen ein.[103] Im Fall *Clapper v. Amnesty International USA* hat der *US Supreme Court* jüngst allerdings die empirisch zweifelhafte Feststellung getroffen, dass die bloße Gefahr einer Abhörmaßnahme nicht ausreichend ist, um einen Abschreckungseffekt (*chilling effect*) und so eine Verletzung des *Fourth Amendment* zu begründen.[104]

Mit Recht hat das BVerfG vergleichbaren Ansätzen hierzulande bislang einen Riegel vorgeschoben. Die theoretische Möglichkeit, von einem Kommunikationsmedium keinen Gebrauch zu machen, kann nicht dazu führen, dass dem Einzelnen der grund-

96 *US Supreme Court, Katz v. United States*, 389 U.S. 347, 361 (1967). Ob die Gesellschaft eine Erwartung für berechtigt hält, bemisst sich nach Präzedenzfällen in der Rechtsprechung.

97 *L. Strahilevitz*, A Social Networks Theory of Privacy, University of Chicago Law Review 72 (2005), S. 919 (937).

98 *US Supreme Court, United States v. Miller*, 425 U.S. 435, 440 (1976).

99 Dies gilt nach der Entscheidung *People v. Harris* (N.Y. Crim. Ct. 2012), wohl erst recht gegenüber Twitter, da *tweets* nach den Grundeinstellungen öffentlich sind (s. dazu unten, Fn. 128).

100 Krit. *Chahal*, Balancing (Fn. 94), S. 285 (296 f.); *M. Kaminski*, Reading Over Your Shoulder: Social Readers And Privacy Law, Wake Forest Law Review Online 2 (2012), S. 13 (20). In der Entscheidung *United States v. Jones* v. 23.1.2012, No. 10-1259, at 3-6 (*S. Sotomayor*, J., concurring) hat Richterin *Sotomayor* darauf hingewiesen, dass der empirische Befund des freigiebigen Umgangs mit persönlichen Informationen den verfassungsrechtlichen Schutz der Privatsphäre durch den *reasonable expectation of privacy*-Test weiter schwächen könnte.

101 Gem. 18 USC § 2703 a, b.

102 Gem. 18 USC § 2703 c (2) und 18 USC § 3122, der den *Patriot Act* umsetzt.

103 *Chahal*, Balancing (Fn. 94), S. 285 (295).

104 *US Supreme Court, Clapper v. Amnesty International USA* v. 26.2.2013, No. 11-1025, at 2.

rechtliche Schutz entzogen wird. Vielmehr hat die Gewährleistung des Art. 10 Abs. 1 GG den genau umgekehrten Zweck, eine unbefangene Nutzung der Fernkommunikation *trotz* deren erhöhter Risiken zu ermöglichen.[105] So soll das Grundrecht freiheitsbeeinträchtigenden Abschreckungseffekten vorbeugen,[106] also dem Risiko, dass „der Meinungs- und Informationsaustausch mittels Fernmeldeanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten".[107] Niemand würde ernstlich für den vereinfachten Zugriff auf TK-Verbindungsdaten ins Feld führen, dass schließlich jeder Telefonkunde um deren anlasslose Speicherung wisse und sich trotzdem für die Nutzung eines Telefonanschlusses entschieden habe. Entsprechend begibt sich auch der Inhaber eines Facebook-Accounts, der die Datenspeicherpolitik des Unternehmens kennt, nicht seines Grundrechtsschutzes. Die Nutzung eines Kommunikationsmittels im Wissen um dessen Sicherheitslücken kann nicht als Einwilligung in den erleichterten Datenzugriff durch Dritte interpretiert werden.

Grundsätzlich ist mithin festzuhalten, dass der staatliche Zugriff auf Facebook-Accounts einen schwerwiegenden Eingriff in das Telekommunikationsgeheimnis bedeutet, der nicht etwa dadurch abgemildert wird, dass der Nutzer sich des Risikos bewusst ist. Die rechtlichen und faktischen Unsicherheitsbedingungen („Unter welchen Voraussetzungen ist eine Maßnahme zulässig? Findet eine Maßnahme statt?"), unter denen Kommunikationsentscheidungen getroffen werden, dürften bei vielen Menschen dazu führen, dass sie sich für die sichere Alternative, ein Unterlassen der digitalen Kommunikation entscheiden.[108] Dies würde an sich nahelegen, staatliche Zugriffe auf Facebook-Nutzerprofile nur unter den strengen Voraussetzungen des § 100a StPO zuzulassen. Soll gleichwohl unter bestimmten Bedingungen eine „Beschlagnahme" nach § 99 StPO – oder gar nach §§ 94, 98 StPO – zulässig sein, wäre darzutun, weshalb ein Eingriff ausnahmsweise von geringerer Intensität sein soll.

105 BVerfG 100, 313 (363) – Telekommunikationsüberwachung; *Durner* (Fn. 86), Art. 10 Rn. 1 ff m.w.N.

106 Zu dieser aus dem US-amerikanischen Verfassungsrecht stammenden Figur: *F. Schauer*, Fear, Risk and the First Amendment: Unraveling the "Chilling Effect", Boston University Law Review 58 (1978), S. 685; zum schwierigen Nachweis solcher Freiheitsbeeinträchtigungen *L. Kendrick*, Speech, Intent and the Chilling Effect, William & Mary Law Review 54 (2013), S. 1633 (1675 f.); *K.-H. Ladeur*, Toward a Network oriented Law of the Internet! The Necessity to Find a New Balance Between Risk and Opportunity in Network Communication, German Law Journal 10 (2009), S. 1201 (1207-1208).

107 BVerfGE 100, 313 (359) – Telekommunikationsüberwachung; ähnlich BVerfGE 34, 238 (246 f.) -Tonbandbeschluss; vgl. auch *M. Baldus*, in: V. Epping/C. Hillgruber (Hrsg.), Beck'scher Online-Kommentar Grundgesetz, Art. 10 Rn. 8.

108 Zu Risiko- und Ambiguitätsaversion bei Entscheidungen über die Privatsphäre *A. Acquisti/J. Grossklags*, Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting, in: L. J. Camp/S. Lewis (Hrsg.), The Economics of Information Security, Boston: Kluwer 2004, S. 165 (165 f.); *A. Acquisti/J. Grossklags*, Uncertainty, Ambiguity, and Privacy, 4th Annual Workshop on Economics and Information Security (WEIS 2005), March 6, 2005.

Teilweise – so auch im Reutlinger Beschluss – wird dies in Anlehnung an die E-Mail-Rechtsprechung für punktuelle, offene Zugriffe in Ruhephasen angenommen. Überzeugend ist diese Annahme jedoch nicht, da auch das Wissen um die Überwachungsmaßnahme die Kommunikationsentscheidung beeinflussen und abschreckende Wirkung entfalten dürfte.

Trägt die Differenzierung zwischen dynamischen und Ruhephasen schon in Bezug auf E-Mails nicht, mutet sie im Fall der Kommunikation über Facebook nachgerade willkürlich an. Die Plattform erlaubt zwei unterschiedliche Formen des Nachrichtenaustausches. Die Nutzer können nicht nur asynchron (funktional einer E-Mail vergleichbare) „Messages" austauschen, sondern haben daneben auch die Möglichkeit, in Echtzeit miteinander zu „chatten". Im Chat erwartet der Nutzer nicht nur eine direkte Antwort, sondern kann sogar sehen, wie sein Gesprächspartner daran schreibt. Facebook hat die Messaging- und Chatfunktion mittlerweile integriert. Ist der angeschriebene Nutzer gerade offline, wird die Nachricht in seinem Postfach abgelegt. Ist er online, kann er direkt in eine Echtzeit-Kommunikation (ähnlich wie bei einem IRC-Chat) eintreten. Auch in diesem Fall aber speichert Facebook ausgetauschte Chat-Nachrichten anschließend im Postfach beider Nutzer ab. Es entsteht also ein bleibendes Protokoll des Chats, das sich der Form nach kaum von asynchron ausgetauschten und archivierten Messages unterscheidet.

Dass die Überwachung von schriftlicher Echtzeit-Kommunikation (*Instant Messaging*) nur nach § 100a StPO zulässig ist, wird kaum bestritten.[109] Umso mehr befremdet die Selbstverständlichkeit, mit der eine Beschlagnahme von Facebook-Chats unter geringeren Voraussetzungen für möglich gehalten wird. Warum sollten sich die Ermittler überhaupt noch die Mühe einer TK-Überwachung nach § 100a StPO machen, wenn sie eine Sekunde nach Beendigung der Unterhaltung ein vollständiges Wortprotokoll als einfachen Datensatz beschlagnahmen können (§§ 94 ff. StPO)? Man stelle sich vor, von jedem Telefongespräch entstünde automatisch eine schriftliche Aufzeichnung. Auch wenn der Anschlussinhaber selbst diese sofort vernichtete, verblieben immer noch identische Kopien bei seinem Gesprächspartner und dem Telefonanbieter. Dass ein Abhören nur unter den Voraussetzungen des § 100a StPO möglich sein sollte, auf die verkörperten Kommunikationsprotokolle aber nach den allgemeinen Vorschriften zugegriffen werden kann, sobald der Hörer aufgelegt wurde, ist bei teleologischer Interpretation von Art. 10 Abs. 1 GG nur schwer zu be-

109 Vgl. *Brunst*, Anmerkung zu BVerfG (Fn. 22), S. 591 (592). Folgt man dem von Graf vertretenen Ansatz und wendet auch auf die längerfristige Überwachung von E-Mail-Kommunikation § 99 StPO an, hätte das im Extremfall zur Folge, dass die Ermittlungsbehörden eine Echtzeitkommunikation im Chat gleichsam mitlesen könnten, ohne dafür eine Anordnung nach § 100a StPO zu benötigen. Sie müssten nur beim Provider zugreifen.

gründen.[110] Denn der Abschreckungseffekt ist für den Einzelnen nicht größer, wenn er mit dem Abhören seiner Kommunikation in Echtzeit rechnen muss, als wenn *post hoc* auf das Kommunikationsprotokoll zugegriffen wird. Auch das BVerfG hat dies erkannt, wenn es in der Entscheidung zur Online-Durchsuchung feststellt, dass die Erhebung von Kommunikationsdaten „mittelbar die Freiheit der Bürger [beeinträchtigt], weil die Furcht vor Überwachung, auch wenn diese erst nachträglich einsetzt, eine unbefangene Individualkommunikation verhindern kann".[111]

Der Vergleich des Facebook-Chats mit abgehörten Telefonaten ist keineswegs abwegig. Bei textbasierten Formen der elektronischen Echtzeitkommunikation ist aufgrund ihrer Spontaneität regelmäßig eine vergleichbare Gefährdungslage gegeben wie bei der mündlichen Kommunikation am Telefon oder via „Voice over IP" (VoIP). Eine hastig getippte Antwort im Chat ist eben kein Brief, den der Absender mit Bedacht verfasst und erst nach nochmaligem Durchlesen zur Post gibt.

Selbst wenn man dieser Argumentation entgegenhalten wollte, eine Aufhebung der Trennung von Kommunikationsprozess und -produkt schaffe letztlich ein auf elektronisch übertragene Daten und Inhalte gemünztes „Dauerschutzrecht", das den Gehalt von Art. 10 Abs. 1 GG überdehne,[112] ist dies in erster Linie ein dogmatischer Einwand. Die erhöhte Schutzbedürftigkeit, die sich aus dem fortwirkenden Persönlichkeitsbezug der Kommunikationsinhalte ergibt, lässt sich damit nicht überzeugend bestreiten.

Allerdings wäre es durchaus denkbar, anstelle des Telekommunikationsgeheimnisses auf das vom BVerfG entwickelte Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme abzustellen.[113] Dieses ist subsidiär anzuwenden, wenn auf Systeme zugegriffen werden soll, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, die einen Einblick in wesentliche Teile der Lebensgestaltung einer Person oder ein aussagekräftiges Bild der Persönlichkeit gewähren.[114] Heimliche Zugriffe, die das Grundrecht berühren, sind jedenfalls im Bereich des Ge-

110 Ähnlich *Schwabenbauer*, Kommunikationsschutz (Fn. 63), S. 1 (29): „Es besteht kein struktureller Unterschied zwischen etwa dem Abhören laufender Telekommunikation (§ 100a StPO) und der Lektüre (typischerweise) über Jahre archivierter E-Mails".

111 BVerfGE 120, 274 (323) – Online-Durchsuchung.

112 So *Krüger*, Anmerkung zu BVerfG (Fn. 22), S. 680 (682).

113 Das aus der hohen Eingriffsintensität hergeleitete Bedürfnis eines neuen Grundrechts kritisiert *M. Eifert*, Informationelle Selbstbestimmung im Internet – Das BVerfG und die Online-Durchsuchungen, NVwZ 2008, S. 521 (521), allerdings zu Recht. Folgt man der verfassungsgerichtlichen Argumentationslogik bei der Online-Durchsuchung, ergeben sich die besonderen Persönlichkeitsgefährdungen in erster Linie aus dem *breiten Spektrum an Nutzungsmöglichkeiten*, die informationstechnische Systeme bieten, und der mit der *Vernetzung verbundenen Erweiterung dieser Nutzungsmöglichkeiten*, vgl. BVerfGE 120, 274 (305) – Online-Durchsuchung. Dabei bleibt aber unklar, weshalb das Risiko höher und stärkerer Grundrechtsschutz erforderlich sein soll, wenn der Nutzer seinen mit dem Internet verbundenen Computer bedient als wenn er über E-Mail kommuniziert.

114 BVerfGE 120, 274 (314) – Online-Durchsuchung.

fahrenabwehrrechts nur unter strengen Voraussetzungen (insbesondere bei *konkreter* Gefahr für ein *überragend* wichtiges Rechtsgut) zulässig.[115] Zwar trifft das BVerfG keine Aussage zu den Rechtfertigungsvoraussetzungen im repressiven Bereich. Doch dürften sowohl die Anforderungen an das zu schützende Rechtsgut als auch die Anforderungen an den Verdachtsgrad im Strafprozessrecht höher anzulegen sein als im Gefahrenabwehrrecht. Aus diesem Grund wären die verfassungsrechtlichen Rechtfertigungsvoraussetzungen strafprozessual wohl in eine mindestens das Schutzniveau von § 100a StPO gewährleistende Vorschrift zu übersetzen.

Auch das Kriterium des „punktuellen" Eingriffs begründet nicht automatisch eine geringere Eingriffsintensität. Wie schon in Bezug auf E-Mail ausgeführt, dürfte eine Selektion der ausgetauschten Nachrichten an Ort und Stelle kaum möglich sein. Da auch Nachrichten sensiblen Inhalts betroffen sein können, sind gesteigerte Anforderungen an die Eingriffsvoraussetzungen zu stellen. Je näher der Kommunikationsinhalt an den Kernbereich privater Lebensgestaltung rückt, desto höher liegt die Eingriffsschwelle. Das aus der Menschenwürdegarantie gem. Art. 1 Abs. 1 GG abgeleitete Kernbereichskonzept prägt nicht nur den innersten Schutz von Art. 2 Abs. 1 GG, sondern auch den von Art. 10 Abs. 1 GG.[116] Dies wird durch § 100a Abs. 4 S. 1 StPO einfachrechtlich dahingehend konkretisiert, dass eine Überwachung gem. § 100a Abs. 1 StPO unzulässig ist, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch eine solche Überwachung allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Kommunikationsinhalte des höchstpersönlichen Bereichs dürfen daher auch nicht gespeichert werden und sind unverzüglich zu löschen, falls sie ausnahmsweise doch erhoben wurden.[117]

Scharfen Widerspruch verdient die in diesem Kontext teilweise zu lesende Behauptung, in sozialen Netzwerken würden für gewöhnlich überhaupt keine Nachrichten mit vertraulichem oder intimem Inhalt ausgetauscht, sodass „Überlegungen im Hinblick auf den Schutz von Elementen des Kernbereichs im Zweifel nicht anzustellen" seien.[118] Tatsächlich dürften über Facebook nicht weniger intime oder vertrauliche Nachrichten ausgetauscht werden als in Briefen oder via E-Mail.[119] Gerade die Dynamik und Spontaneität der fast ungehemmten Echtzeit-Kommunikation legt dies sogar ausgesprochen nahe. Dass Liebesbeziehungen via Facebook begonnen, beendet

115 BVerfGE 120, 274 (326) – Online-Durchsuchung.

116 BVerfGE 113, 348 (391) – Präventive Telekommunikationsüberwachung; BVerfGE 115, 166 (182); vgl. *Pagenkopf* (Fn. 79), Art. 10 Rn. 7.

117 BVerfGE 124, 43 (69, 70).

118 *Graf* (Fn. 21), § 100a Rn. 32k.

119 Allein auf ihren Profilen geben die meisten Nutzer sozialer Netzwerke große Mengen teilweise sehr persönlicher Informationen preis, vgl. nur *T. Taraszov et al.*, Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook profiles as an example, International Journal of Media and Cultural Politics 6 (2010), S. 81.

und vor allem – in allen emotionalen und sexuellen Details – mit Freunden diskutiert werden, ist keine Seltenheit.[120]

Schließlich gilt auch hinsichtlich der „Offenheit" der Beschlagnahme beim Dienstanbieter nichts anderes als bei E-Mails. In aller Regel wird die vorherige Anhörung des Betroffenen unter Verweis auf den sonst gefährdeten Ermittlungszweck entfallen (§ 33 Abs. 4 StPO), wie es auch der Beschluss des AG Reutlingen vorgesehen hatte. Dem Betroffenen, der nicht zufällig im Moment des Vollzugs anwesend ist, verbleibt folglich nur die Möglichkeit des nachträglichen Protests gegen die Maßnahme.

Im Ergebnis ist daher festzuhalten, dass die Beschlagnahme von beim Dienstanbieter Facebook „ruhender" Nachrichten und Chats unter keinem erkennbaren Gesichtspunkt eine geringere Eingriffsqualität aufweist als während des Übertragungsvorgangs. Soweit die Gegenmeinung gleichwohl §§ 94 ff. StPO als Eingriffsgrundlage ausreichen lassen will, stützt sie sich auf technisch bedingte Zufälligkeiten und Topoi, deren normativer Gehalt bei Lichte betrachtet die Differenzierung nicht zu tragen vermag.[121]

II. Sonstige kommunikative Funktionen bei Facebook

Das AG Reutlingen wollte nicht nur auf die Messages und Chats des Angeklagten zugreifen, sondern ordnete auch die „Beschlagnahme" einer Reihe weiterer Datensätze an. Der von *Graf* vorgeschlagene Formularbeschluss zur Beschlagnahme von Internet-Kommunikation in sozialen Netzwerken geht noch weiter und listet knapp 30 beschlagnahmefähige Datensätze auf.[122] Groben Schätzungen zufolge speichert Facebook sogar 70 verschiedene Datenkategorien.[123] Insofern überrascht die Unbekümmertheit, mit der die zahlreichen Funktionen, die Facebook seinen Nutzern bietet, und die die dabei anfallenden Daten teilweise über einen juristischen Kamm geschoren werden.

Facebook bietet eine bunte Vielfalt an Funktionen, die das klassische Angebot von Post- und Telekommunikationsdienstleistern i.S.v. Art. 10 Abs. 1 GG bei Weitem in den Schatten stellt. So können die Nutzer synchron oder asynchron Nachrichten an

120 Für einen Überblick über Art und Menge der bei Facebook preisgegebenen Informationen *R. Gross/A. Acquisti*, Information Revelation and Privacy in Online Social Networks, Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, S. 71.

121 *T. Singelnstein*, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, S. 593 (600), hält § 100a StPO für die einzige zulässige Ermächtigungsgrundlage bei Zugriffen, die kein Überwinden technischer Sicherungen erfordern. Das Erfordernis einer gesetzlichen Spezialermächtigung sieht er hingegen nicht.

122 Vgl. *Graf* (Fn. 21), Formularbeschluss „Überwachung und Beschlagnahme von Internet-Kommunikation in Sozialen Netzwerken (Facebook ua)".

123 Dazu die von *Max Schrems* gegründete Initiative *europe-v-facebook.org*: >http://europe-v-facebook.org/DE/Datenbestand/datenbestand.html<; vgl. *Grimmelmann*, Saving Facebook (Fn. 9), S. 1137 (1149); *Graf* (Fn. 21), § 100a Rn. 321, der „nur" 39 verschiedene Datensätze benennt.

andere Nutzer versenden,[124] andere Nutzer „anstupsen", Pinnwandeinträge und Fotos „posten", Statusmeldungen abgeben (vergleichbar mit Microblogging-Diensten wie Twitter), an Gruppenforen teilnehmen oder über *social plug-ins* einfach eine Seite „liken".[125] Gemein ist all diesen Funktionen, dass sie der Kommunikation dienen.[126] Dabei verhalten sich die Nutzer meist so, als seien sie auf einer „digitalen Cocktailparty"[127] mit dem Motto „Selbstdarstellung".[128] Schon deshalb sind viele Kommunikationsinhalte bei Facebook an einen nicht individualisierbaren Personenkreis, sondern an alle potentiell anwesenden „Partygäste" gerichtet. Dies ist dann der Fall, wenn Kommunikationsinhalte durch Suchmaschinen indexiert oder jedenfalls registrierten Facebook-Nutzern zugänglich sind.[129] Dabei handelt es sich mangels Individualisierungsintention – ähnlich wie bei *tweets* auf der Microblogging-Plattform Twitter[130] – um öffentliche Kommunikation, die von Art. 5 Abs. 1 S. 1 GG, nicht hingegen von Art. 10 Abs. 1 GG geschützt ist.[131] Ein Grundrechtseingriff scheidet hier regelmäßig aufgrund der in der freiwilligen öffentlichen Preisgabe liegenden Einwilligung aus.[132]

Schwieriger ist die rechtliche Bewertung, wenn der Nutzer sich entscheidet, seine Informationen nur mit bestimmten Personen zu teilen, etwa nur mit Freunden. Die Grenzen zwischen öffentlicher und privater, i.e. individualisierter Facebook-Kommunikation verschwimmen hier.[133] Wann eine den Grundrechtsschutz ausschließende Einwilligung vorliegt, ist in diesen Fällen nicht immer klar. Die Architektur von Facebook stimuliert zwar die individuelle Kommunikation zwischen zwei Personen; zugleich ist es nach den sozialen Normen der meisten *virtual communities* aber üblich, die Aufmerksamkeit anderer Nutzer – eines größeren Personenkreises – auf

124 *H. Redeker*, in: T. Hoeren/U. Sieber (Hrsg.), Handbuch Multimedia-Recht (EL 33, 2012), Kap. 12 Rn. 416.

125 Zu den verschiedenen Kommunikationsfunktionen bei Facebook *A. Ebersbach/M. Glaser/R. Heigl*, Social Web, 2. Aufl., 2011, S. 105 f.; *Grimmelmann*, Saving Facebook (Fn. 9), S. 1137 (1150 f.).

126 Zum Kommunikationsbegriff *T. Vesting*, Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, in: W. Hoffmann-Riem/E. Schmidt-Aßmann/A. Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. II, 2008, § 20 Rn. 28.

127 *Position Paper No. 1* über *Security Issues and Recommendations for Online Social Networks* (2007) der European Network and Information Security Agency (ENISA), S. 6.

128 *D. Heckmann*, in: ders. (Hrsg.), juris PraxisKommentar Internetrecht, 3. Aufl., 2011, Kap. 1.7. Rn. 195; zur dramaturgischen Selbstinszenierung *E. Goffman*, The Presentation of Self in Everyday Life, New York, NY: Anchor 1959.

129 *Graf* (Fn. 21), § 100a, Rn. 32g-32h, bezeichnet den zweiten Fall als "facebook-öffentlich".

130 Die Grundeinstellungen (*default rules*) von Twitter sehen vor, dass Nachrichten (*tweets*) öffentlich sind, vgl. *Chahal*, Balancing (Fn. 94), S. 285 (291).

131 *Schwabenbauer*, Kommunikationsschutz (Fn. 63), S. 1 (9, 11); *Durner* (Fn. 86), Art. 10 Rn. 92.

132 BVerfGE 120, 274 (344-345) – Onlinedurchsuchung (bei gezielter Zusammenführung allgemein zugänglicher Inhalte ist hingegen eine gesetzliche Ermächtigung erforderlich); *W. Hoffmann-Riem*, Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, AöR 134 (2009), S. 513 (529); *Singelnstein*, Strafprozessuale Ermittlungsmaßnahmen (Fn. 121), S. 593 (600).

133 *Durner* (Fn. 86), Art. 10 Rn. 93; *K.-H. Ladeur/T. Gostomzyk*, Der Schutz von Persönlichkeitsrechten gegen Meinungsäußerungen in Blogs, NJW 2012, S. 710 (712).

Vorgang und Produkt individueller Kommunikation zu ziehen.[134] Ein Beispiel für diese hybride Kommunikationsform ist die Pinnwand-Funktion. Dadurch dass das kommunikative Hin-und-Her auf den Pinnwänden einer größeren Zahl von Nutzern sichtbar gemacht wird, entsteht eine Quasi-Öffentlichkeit, die die Kommunikationsteilnehmer zur Einhaltung der sozialen Norm des Reziprozierens anregt.[135] Die Pinnwandfunktion ist, wie alle anderen sozialen Kommunikationsfunktionen bei Facebook, so gestaltet, dass der Kommunikationsfluss permanent aufrechterhalten und Facebook permanent mit personenbezogenen Daten versorgt wird. Dieser sanfte Kommunikationsdruck wird durch einen dezentral „überwachenden" Personenkreis generiert (*liquid surveillance*),[136] in der Regel Facebook-Freunde, die über eine entsprechende Zugangsberechtigung verfügen.[137] Durch die Annahme einer Freundschaftsanfrage und den damit verbundenen Zugang zum eigenen Profil signalisiert der Nutzer seine Bereitschaft zu reziprokem Vertrauen darauf, dass Kommunikation nicht von unautorisierten Dritten zur Kenntnis genommen wird.[138] Auch wenn dieses Vertrauen nicht selten unberechtigt ist, kann der Freundschaftsmechanismus grundsätzlich nicht als „technisch so anfällig und unvollkommen" qualifiziert werden, dass der kommunikative Austausch über das eigene Facebook-Profil als öffentlich anzusehen ist.[139] Denn das Erfordernis der Freundschaftsannahme und die Passwortsicherung begründen Zugangshindernisse, die von der Allgemeinheit nicht ohne weiteres überwunden werden können. Kommunikationsinhalte sind nach der Nutzerintention deshalb allein für einen über die Facebook-Freundschaft individualisierten Personenkreis bestimmt.[140] Das BVerfG hat E-Mails, Mail-Dienste, geschlossene Chats und nicht-öffentliche Diskussionsforen als von Art. 10 Abs. 1 GG geschützt

134 *Grimmelmann*, Saving Facebook (Fn. 9), S. 1137 (1156); zur Verhaltenssteuerung durch Architektur im Cyberspace *L. Lessig*, Code: Version 2.0, New York, NY: Basic Books 2006, S. 5 f.

135 *Grimmelmann*, Saving Facebook (Fn. 9), S. 1137 (1156); zur privaten Öffentlichkeit *J. Zittrain*, The Future of the Internet – And How to Stop It, New Haven, CT: Yale University Press 2008, S. 212 f.

136 *Z. Bauman/D. Lyon*, Liquid Surveillance: A Conversation, Cambridge: Polity Press 2013.

137 Zum Kriterium der Zugangsberechtigung *T. Böckenförde*, Auf dem Weg zur elektronischen Privatsphäre, JZ 2008, S. 925 (936 ff.); *Durner* (Fn. 86), Art. 10 Rn. 94, bezeichnet das Zugangshindernis als maßgebliches Indiz für den Ausschluss der Allgemeinheit.

138 Allein dieses Vertrauen ist von Art. 10 Abs. 1 GG geschützt, nicht hingegen das personengebundene Vertrauen in den Kommunikationspartner: BVerfGE 120, 274 (340-341) – Onlinedurchsuchung; vgl. *E. Gurlit*, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, S. 1035 (1036-1037).

139 Nach *Pagenkopf* (Fn. 79), Art. 10 Rn. 14a, ist der Schutz durch Art. 10 Abs. 1 GG in diesen Fällen zweifelhaft.

140 Man kann darin auch eine Anwendung der Zweifelsregel sehen, wonach der Schutzbereich von Art. 10 Abs. 1 GG im Zweifel auch dann eröffnet ist, wenn trotz fehlender intersubjektiver Kommunikation eine vertrauliche Kommunikation möglich ist: *Durner* (Fn. 86), Art. 10 Rn. 95; im Ergebnis wohl anders *Ladeur/Gostomzyk*, Persönlichkeitsrechte (Fn. 133), S. 710 (712).

angesehen;[141] dies gilt auch für die Kommunikation auf zugangsgesicherten Facebook-Profilen.[142]

Doch erschwert die bunte Vielfalt an teilweise hybriden Kommunikationsfunktionen nicht nur die Abgrenzung zwischen privater und öffentlicher Kommunikation. Bei der Facebook-Nutzung fallen neben Inhaltsdaten auch unzählige Bestands- und Verkehrsdaten an, die nur auf Grundlage spezifischer gesetzlicher Ermächtigungen erhoben werden dürfen.

Bestandsdaten sind alle personenbezogenen Daten eines Nutzers, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich sind (§ 3 Nr. 3 TKG, § 14 Abs. 1 TMG), etwa zur Nutzung von Facebook.[143] Dazu gehören der Klarname,[144] die E-Mail-Adresse, das Passwort,[145] Geschlecht und Geburtsdatum. Diese Daten sind für das Verhältnis des Nutzers zum Diensteanbieter zwar relevant, lassen den Telekommunikationsvorgang als solchen aber unberührt. Als „Umstände der Bereitstellung von Telekommunikationsdienstleistungen" sind sie nicht durch Art. 10 GG geschützt;[146] vielmehr fallen sie in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[147] Die gesetzliche Befugnis der Ermittlungsbehörden zur Erhebung von Bestandsdaten ergibt sich regelmäßig aus §§ 161 Abs. 1 S. 1, 163 StPO.[148] Eine Besonderheit gilt, wie das BVerfG jüngst ausgeführt hat, allerdings für die Erhebung von Passwörtern und anderen Zugangsdaten. Danach ist es Ermittlungsbehörden verwehrt, Zugangscodes unabhängig von den Anforderungen an deren Nutzung zu erheben.[149] Dadurch soll verhindert werden, dass die Abfrage von Zugangscodes an leichtere Voraussetzungen geknüpft wird als deren geplante Nutzung.[150] Im Übrigen wird hierdurch ein gewisser Gleichlauf der Anforderungen an mittelbare und unmittelbare Zugriffe auf Kommunikationsinhalte hergestellt: Keine kluge Ermittlungsbehörde würde unter hohen Voraussetzungen direkt auf Kommunikationsinhalte zugreifen, wenn sie unter geringeren Voraussetzungen auf den

141 BVerfGE 120, 274 (341) – Onlinedurchsuchung.

142 Im Ergebnis auch *Schwabenbauer*, Kommunikationsschutz (Fn. 63), S. 1 (20); vgl. *Heckmann* (Fn. 128), Kap. 1.7. Rn. 196.

143 Dazu *P. Schmitz*, in: T. Hoeren/U. Sieber (Hrsg.), Handbuch Multimedia-Recht (EL 33, 2012), Kap. 16.2 Rn. 170 ff.

144 Punkt 4.1 der Erklärung der Rechte und Pflichten bei Facebook.

145 Personenbezogene Berechtigungskennungen werden zwar in § 96 Abs. 1 Nr. 1 TKG als Verkehrsdaten typisiert; eine Erhebung ist dennoch unter den für Bestandsdaten geltenden Voraussetzungen gem. §§ 161 Abs. 1 S. 1, 163 StPO zulässig, vgl. *Nack* (Fn. 25), § 100a Rn. 9.

146 BVerfGE 130, 151 (180).

147 BVerfGE 130, 151 (184).

148 *Nack* (Fn. 25), § 100a Rn. 7.

149 BVerfGE 130, 151 (209); dazu *M. Kutscha*, in: ders./S. Thomé (Hrsg.), Grundrechtsschutz im Internet?, 2013, S. 1 (64).

150 *Ibid.*

Schlüssel zugreifen dürfte, mit dem die Tür zu den Kommunikationsinhalten geöffnet werden kann. Soll also ein Facebook-Passwort abgefragt werden, um eine laufende Chat-Kommunikation zu überwachen, ist der Maßstab des § 100a StPO anzulegen.

Problematischer ist der staatliche Zugriff auf Verkehrsdaten. Dies sind gem. § 3 Nr. 30 TKG Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.[151] Dazu gehören Daten über die Umstände der Telekommunikation, wie die Nummer oder Kennung der beteiligten Anschlüsse, bei mobilen Anschlüssen auch die Standortdaten, Datenmengen, Datum, Uhrzeit, den vom Nutzer in Anspruch genommenen Telekommunikationsdienst oder die Endpunkte von festgeschalteten Verbindungen (§ 96 Abs. 1 TKG).[152] Das besondere Risiko liegt hier in der Aggregation enormer Datenmengen; eine Zusammenführung der auf den Facebook-Servern gespeicherten Verkehrsdaten lässt unter Umständen „erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten zu".[153] Soweit diese Daten einen konkreten Telekommunikationsvorgang betreffen, unterliegen sie deshalb dem besonderen Schutz von Art. 10 GG.[154] Die Einholung einer Auskunft ist hier nur unter den erhöhten Voraussetzungen von § 100g StPO zulässig.[155]

Die vom BVerfG festgestellte Teilnichtigkeit von § 100g Abs. 1 S. 1 StPO[156] sperrt einen Zugriff auf die bei Facebook gespeicherten Verkehrsdaten allerdings nicht. Zwar speichert Facebook tatsächlich Daten auf „Vorrat". Dies ist aus datenschutzrechtlichen Gründen (Datensparsamkeit, Erforderlichkeit) fragwürdig, geschieht aber nicht auf staatliche Veranlassung gem. §§ 113a, 113b TKG. Im Übrigen ist Facebook überwiegend nicht als Telekommunikationsdienst, sondern als Telemediendienst einzustufen.[157] Die Normen des TKG finden lediglich auf den Nachrichtenaustausch in der Chat-Funktion Anwendung.[158] Im Ergebnis ist daher festzuhalten, dass eine angemessene Bestimmung der jeweiligen Rechtfertigungsvoraussetzungen ohne empirische Analyse des Kommunikationsverhaltens in sozialen Netz-

151 Dazu *J. Kühling/C. Seidel/A. Sivridis*, Datenschutzrecht, 2. Aufl., 2011, S. 250.

152 *Nack* (Fn. 25), § 100a Rn. 8.

153 BVerfGE 107, 299 (319).

154 BVerfGE 67, 157 (172) – G 10; BVerfGE 130, 151 (179); *Kutscha*, Grundrechtsschutz (Fn. 149), S. 1 (68-70).

155 *Nack* (Fn. 25), § 100a Rn. 8; *Schmitz* (Fn. 143), Kap. 16.2 Rn. 178. Der staatliche Zugriff auf Nutzungsdaten – Daten, die erforderlich sind, um dem Nutzer die Inanspruchnahme der Telemediendienste zu ermöglichen und abzurechnen (§ 15 Abs. 1 TMG) ist gem. §§ 161 Abs. 1 S. 1, 163 StPO oder, falls es sich nicht zugleich um Bestandsdaten handelt, gem. § 100g StPO zulässig, vgl. *Nack* (Fn. 25), § 100a Rn. 12.

156 BVerfGE 125, 260 ff. – Vorratsdatenspeicherung; dazu *Graf* (Fn. 21), § 100a, Rn. 16.

157 So *Redeker* (Fn. 124), Kap. 12 Rn. 429.

158 *Ibid.*

werken nicht möglich ist und für den Zugriff auf in sozialen Netzwerken preisgegebene Informationen unterschiedliche Ermächtigungsregime gelten.[159]

III. Exkurs: Strafprozessualer Zugriff durch die nachrichtendienstrechtliche Hintertür?

Berichte über die massenhafte Erhebung von Verbindungsdaten durch die National Security Agency (NSA) mithilfe von PRISM (Planning Tool for Resource Integration, Synchronization and Management) und durch die britischen Government Communications Headquarters (GCHQ) mithilfe von Tempora belegen, dass das Telekommunikationsgeheimnis nicht nur unter Beschuss der Strafverfolgung steht.[160] Zwar dürften die Ängste vor den freiheitsbeschränkenden Wirkungen der Überwachung durch die inländischen Geheimdienste auch wegen fehlenden Wissens über die tatsächlichen und rechtlichen Voraussetzungen der nachrichtendienstlichen Überwachung verschwörungstheoretisch überladen sein.[161] Besondere Risiken ergeben sich aber in der Tat aus der denkbaren Übermittlung nachrichtendienstlich erlangter Daten an die Strafverfolgungsbehörden. Problematisch ist zum einen, dass es grundsätzlich in der Hand der Nachrichtendienste liegt, darüber zu entscheiden, welche Informationen weitergeleitet werden; den Strafverfolgungsbehörden steht in der Regel kein entsprechendes Auskunftsrecht zu.[162] Daher kann in Übermittlungsfällen kaum sichergestellt werden, dass die Strafverfolgungsbehörden alle relevanten und nicht nur belastende Informationen erhalten (vgl. § 160 Abs. 2 StPO). Problematisch ist zum anderen, dass die Anforderungen an den Verdachtsgrad im Nachrichtendienstrecht teilweise geringer sind und unklar ist, inwiefern die nachrichtendienstrechtlichen Abfrageermächtigungen in Einklang mit dem sog. Doppeltürprinzip[163] auch entsprechende Auskunftspflichten der Telekommunikations- und Telemediendienstleister begründen.

So sieht das G10 Befugnisse zur individuellen und strategischen Kontrolle der Telekommunikation durch alle deutschen Verfassungsschutzämter (BfV und LfV), den Bundesnachrichtendienst (BND) sowie den Militärischen Abschirmdienst (MAD)

159 Jedes Rechtsproblem und jeder rechtliche Maßstab, an dem dieses Problem zu messen ist, wird erst durch die Analyse des Sachverhalts definiert, s. dazu *P. Mastronardi*, Juristisches Denken, 2. Aufl., 2003, S. 196.

160 *N. Härting*, Warum die Erhebung von „Metadaten" durch den BND verfassungswidrig ist, CRonline v. 6.8.2013 (abrufbar unter: http://www.cr-online.de/blog/2013/08/06/warum-die-erhebung-von-metadaten-durch-den-bnd-verfassungswidrig-ist/) geht davon aus, dass die Erhebung von Verbindungsdaten durch den BND verfassungswidrig ist; weiterführend *N. Härting*, Zusammenarbeit von BND und NSA: 7 Fragen, 7 Antworten, CRonline 3.8.2013 (abrufbar unter: http://www.cr-online.de/blog/2013/08/03/zusammenarbeit-von-bnd-und-nsa-7-fragen-7-antworten/).

161 *C. R. Sunstein/A. Vermeule*, Conspiracy Theories: Causes and Cures, Journal of Political Philosophy 17 (2009), S. 202.

162 *N. Bergemann*, Nachrichtendienste und Polizei, in: Lisken/Denninger. Handbuch des Polizeirechts, 5. Aufl. (2012), H 124.

163 BVerfGE 130, 151 (202, 203).

vor.[164] Zwar ist eine Überwachung in Einzelfällen gem. § 3 G10 nur zulässig, wenn „tatsächliche Anhaltspunkte" den Verdacht rechtfertigen, dass verfassungsfeindliche Straftaten in Planung sind oder begangen werden (oder wurden). Demgegenüber ist die strategische Überwachung, die allerdings nur dem BND zusteht, gem. § 5 G10 auch verdachtsunabhängig zulässig. Schließlich sind BfV, BND und MAD gem. §§ 8a Abs. 2 Nr. 4, 5 BVerfSchG, 2a BNDG, 4a MADG ermächtigt, umfassend Daten (unter den erleichterten Voraussetzungen gem. § 8a Abs. 1 BVerfSchG auch Bestandsdaten) bei TK-Unternehmen und Telemediendienstleistern zu erfragen, soweit „tatsächliche Anhaltspunkte" oder „Tatsachen" die Annahme rechtfertigen, dass schwerwiegende Gefährdungen bestimmter Schutzgüter vorliegen.[165] All diese Maßnahmen stehen den Nachrichtendiensten in Einklang mit dem sog. Trennungsgebot[166] (vgl. Art. 87 Abs. 1 S. 2 GG) grundsätzlich nur zur Früherkennung bestimmter Gefahren zu, nicht aber zur Verfolgung von Straftaten.[167]

Aus diesem Grund wird die Einführung nachrichtendienstlich erhobener Daten in das Strafverfahren für alle Nachrichtendienste beschränkt. Verhältnismäßig weitreichende Beschränkungen, die dem Grundrechtsschutz und dem Trennungsgebot hinreichend Rechnung tragen dürften, sieht das G10 vor (§§ 4 Abs. 4 Nr. 2; 7 Abs. 4 S. 2 G10).[168] Problematisch ist allerdings, dass die Einspeisung in das strafprozessrechtliche Ermittlungsverfahren unter dem BVerfSchG sowie dem BNDG und dem MADG (die beide auf das BVerfSchG verweisen) teilweise unter relativ geringen Voraussetzungen zulässig ist (§§ 18 ff. BVerfSchG, 9 ff. BNDG, 8 ff. MADG). So sind die Nachrichtendienste verpflichtet, personenbezogene Daten zu übermitteln, wenn „tatsächliche Anhaltspunkte" dafür bestehen, dass die Übermittlung zur Verfolgung bestimmter Staatsschutzdelikte erforderlich sind (§ 20 Abs. 1 S. 1 BVerfSchG) und schutzwürdige Interessen des Betroffenen das Allgemeininteresse an der Übermitt-

164 *Bergemann*, Polizeirecht (Fn. 162), H 67.

165 Diese Ermächtigungsgrundlage ist durch das Terrorismusbekämpfungsgesetz (TBG), BGBl. I 2002, S. 361, 3142, und das Terrorismusbekämpfungsergänzungsgesetz (TBEG), BGBl. I 2007, S. 2, eingeführt worden; *Härting*, Metadaten (Fn. 160), hält eine Erhebung von Verbindungsdaten auf Grundlage von § 2a BNDG für unzulässig. Dies wird allerdings nur für die massenhafte und strategische Erhebung von Verbindungsdaten gelten, nicht aber für die Erhebung von Verbindungsdaten im Einzelfall, vgl. § 8a Abs. 2 Nr. 4, 5 BVerfSchG. Auch eine Unvereinbarkeit mit dem vom BVerfG entwickelten „Doppeltürprinzip" ist nicht ersichtlich, wenn man die Auskunftspflicht der Telekommunikations- und Telemediendienstleister als von den Vorschriften über die Abfrage der entsprechenden Daten mitumfasst sieht.

166 Dazu *E. Denninger*, „Streitbare Demokratie" und Schutz der Verfassung, in: E. Benda/W. Maihofer/H.-J. Vogel (Hrsg.), Handbuch des Verfassungsrechts, 2. Aufl., 1994, § 16 Rn. 53; zur verfassungsrechtlichen Verankerung *F. Roggan/N. Bergemann*, Die „neue Sicherheitsarchitektur" der Bundesrepublik Deutschland – Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz, NJW 2007, S. 876 (876); zur einfachgesetzlichen Verankerung §§ 8 Abs. 3 BVerfSchG, 2 Abs. 3 BNDG, 4 Abs. 2 MADG.

167 BVerfGE 100, 313 (370) – Telekommunikationsüberwachung = EuGRZ 1999, S. 389 = NJW 2000, S. 55; *M. Kutscha*, Neue Grenzmarken des Polizeiverfassungsrechts, NVwZ 2005, S. 1231 (1233 ff.).

168 Dazu *B. Huber*, Das neue G 10-Gesetz, NJW 2001, S. 3296 (3299).

lung nicht überwiegen (§ 23 Nr. 1 BVerfSchG).[169] Zu den Staatschutzdelikten gehören allerdings nicht nur die in den §§ 74a, 120 GVG enumerierten Delikte, sondern auch Taten, bei denen „tatsächliche Anhaltspunkte" dafür bestehen, dass sie gegen die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit von Bund oder Ländern oder die auswärtigen Belange des Bundes gerichtet sind (§ 20 Abs. 1 S. 2 BVerfSchG). Daher sind bei entsprechender Motivlage auch Informationen über einfache Delikte, etwa eine Sachbeschädigung, von der Übermittlungspflicht erfasst.[170] Besondere Risiken ergeben sich allerdings daraus, dass die Vorschrift umfassende Übermittlungspflichten auslösen kann[171] und die sehr viel weiterreichende Befugnis zur Datenübermittlung aus § 19 Abs. 1 BVerfSchG von § 20 BVerfSchG unberührt bleibt.[172] Denn nach § 19 Abs. 1 BVerfSchG ist eine Übermittlung schon dann zulässig, wenn der Empfänger sie zum Schutz der freiheitlichen demokratischen Grundordnung oder zu Zwecken der öffentlichen Sicherheit benötigt. Obwohl der Wortlaut hier eine Befugnis zur Übermittlung lediglich zu Zwecken der Gefahrenabwehr vermuten lässt, soll auch eine Übermittlung an die Strafverfolgungsbehörden zulässig sein.[173] Da die nachrichtendienstliche Tätigkeit meist im Vorfeld des Verdachts einer Straftat erfolgt und einen weiten Personenkreis betrifft, steigt mit einer Übermittlung das Risiko, unschuldig in ein Strafverfahren verwickelt zu werden.[174] Deshalb muss sichergestellt werden, dass die nachrichtendienstlichen Befugnisse „nicht zur gezielten Erlangung von Zufallsfunden für nicht nachrichtendienstliche Zwecke eingesetzt werden".[175]

Nimmt man es mit dem Telekommunikationsgeheimnis ernst, genügt es nicht, dass die Anforderungen aus § 100a StPO in diese Abwägung eingestellt werden. Es wäre mit Art. 10 GG nicht zu vereinbaren, wenn die Nachrichtendienste unter erleichterten Voraussetzungen – aber zu nachrichtdienstrechtlich zulässigen Zwecken – Daten aus sozialen Netzwerken erhöben und diese an die Strafverfolgungsbehörden weiterleiteten, obwohl eine Erhebung mit entsprechenden Methoden zu strafprozessualen Zwecken unzulässig gewesen wäre.[176] Vielmehr muss auch hier sichergestellt

169 Zum Streit um Ermittlungsermessen oder -pflicht *Bergemann*, Polizeirecht (Fn. 162), H 112.

170 *B. Droste*, Handbuch des Verfassungsschutzrechts, 2007, S. 543, nennt das Besprühen von Wänden mit verfassungswidrigen Kennzeichen oder die Schändung jüdischer Friedhöfe.

171 So *Bergemann*, Polizeirecht (Fn. 162), H 113.

172 *Droste*, Verfassungsschutzrecht (Fn. 170), S. 543; a.A. *Schünemann*, Die Liechtensteiner Steueraffäre als Menetekel des Rechtsstaats, NStZ 2008, S. 305 (306).

173 *Bergemann*, Polizeirecht (Fn. 162), H 115; *Droste*, Verfassungsschutzrecht (Fn. 170), S. 519.

174 Krit. auch *Bergemann*, Polizeirecht (Fn. 162), H 116.

175 *Droste*, Verfassungsschutzrecht (Fn. 170), S. 520.

176 *E. Denninger/R. Poscher*, in Lisken/Denninger. Handbuch des Polizeirechts, 5. Aufl. (2012), B 124; *Bergemann*, Polizeirecht (Fn. 162), H 113.

werden, dass die Schwelle aus § 100a StPO nicht unterschritten wird.[177] Eine Übermittlung ist daher nur zulässig, wenn die Strafverfolgungsbehörden mit denselben Mitteln auf die Daten aus dem sozialen Netzwerk hätten zugreifen dürfen. Die Grundsätze über die Amtshilfe sind nicht so auszulegen, dass sie der amtshilfeersuchenden Behörde die Tore zu einem „Befugnisshopping" öffnen[178] oder die zu nachrichtendienstlichen Zwecken erhobenen Daten zu einem „Allzweck-Datenpool" zusammengeführt werden dürfen. Oder einfacher: Die Strafverfolgungsbehörden dürfen nur die von den Nachrichtendiensten aus sozialen Netzwerken erlangten Informationen erheben, die sie auch verwenden dürfen.

E. Fazit und rechtspolitische Konsequenzen

Die gegenwärtige Rechtslage hinsichtlich des staatlichen Zugriffs auf Facebook-Profile ist alles andere als befriedigend.[179] Einerseits versagen die staatlichen Stellen in Deutschland bei der Durchsetzung datenschutzrechtlicher Bestimmungen gegenüber dem US-amerikanischen Unternehmen, wofür nicht zuletzt die unklare Rechtslage verantwortlich ist. Facebook fühlt sich in Europa nur an die Vorgaben der irischen Datenschutzbehörde gebunden. Das irische Datenschutzrecht gilt indes als deutlich unternehmensfreundlicher als das deutsche. Nachdem der irische *Data Protection Commissioner* Facebook in einem jüngst veröffentlichten Prüfbericht beachtliche Fortschritte im Umgang mit sensiblen Daten attestierte,[180] wurde dieser Befund von deutschen Datenschützern bezeichnenderweise scharf angegriffen.[181] Andererseits aber gestattet die höchstrichterliche Rechtsprechung Gerichten und Ermittlungsbehörden, auf den gewaltigen Datenschatz schon aus verhältnismäßig geringfügigem Anlass (Anfangsverdacht einer einfachen Straftat) zuzugreifen. Die dafür angeführte Rechtfertigung wird weder dem Telekommunikationsgeheimnis gerecht, noch über-

177 BVerfGE 100, 313 (394) = EuGRZ 1999, S. 389 = NJW 2000, S. 55. Obwohl § 5 G10 bestimmte Datenerhebungen zulässt, die dem Anschein nach eine Zweckänderung zu Zwecken der Strafverfolgung mitumfassen, hat der EGMR einen Verstoß gegen Art. 8 II EMRK abgelehnt, vgl. EGMR NJW 2007, S. 1433 – Weber u. Saravia/Deutschland.

178 *Denninger/Poscher*, Polizeirecht (Fn. 176), B 118, 130, warnen vor der zunehmenden Überschneidung der Methoden von Aufklärung, Vorbeugung, Gefahrenabwehr und Strafverfolgung.

179 *Singelnstein*, Strafprozessuale Ermittlungsmaßnahmen (Fn. 121), S. 593 (606), spricht sich aus diesem Grund für eine restriktive Auslegung bestehender Befugnisnormen und eine stärkere Durchsetzung strafprozessualer und verfassungsrechtlicher Grenzen in der Rechtsanwendung aus.

180 Data Protection Commissioner, Facebook Ireland Report of Re-Audit v. 21.9.2012 (abrufbar unter: >http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf<).

181 Exemplarisch die Erklärung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vom 21.9.2012 (abrufbar unter: >https://www.datenschutzzentrum.de/presse/20120921-irisches-facebook-audit.htm<). Dort heißt es: „Wir müssen feststellen, dass der über einjährige Versuch des irischen Kollegen, über freundliche Empfehlungen zu einem grundsätzlichen Wandel bei der Datenschutzpolitik von Facebook zu kommen, erfolglos blieb. […] Das ULD konnte in der bisherigen über einjährigen Auseinandersetzung mit den Unternehmensteilen in Irland und Deutschland nicht feststellen, dass Facebook einen konstruktiven Ansatz in Sachen Datenschutz verfolgt.".

zeugt sie dogmatisch. Das Ergebnis des Zusammentreffens beider Entwicklungen ist rechtstaatlich bedenklich.

Freilich darf man bei der Bewertung nicht übersehen, dass Diensteanbieter wie Facebook und Twitter selbst einen Anreiz haben, in einer Weise auf staatliche Zugriffe zu reagieren, dass das Vertrauen der Nutzer in die grundsätzliche Vertraulichkeit der Kommunikation nicht wegbricht und der Markt für soziale Medien funktionsfähig bleibt. Dadurch kann die Intensität des staatlichen Eingriffs bisweilen selbstregulativ abgefedert werden. So hat Facebook in den USA die Strategie entwickelt, Informationen bei Gerichtsbeschlüssen (*warrants*) und Beweisanordnungen lokaler Behörden zwar herauszugeben, den Begriff des Inhaltsdatums dabei aber zugunsten der Nutzer extensiv auszulegen.[182] Natürlich bleibt die Entscheidung über die Kooperation mit den Strafverfolgungsbehörden gemäß den Facebook-Datenverwendungsrichtlinien dem Diensteanbieter anvertraut, ohne dass Facebook sich zu einer Gegenleistung an die Nutzer verpflichtet.

Andere Anbieter aus dem Bereich sozialer Medien wie etwa Twitter haben die *Blaming-by-Naming*-Strategie entwickelt, die Heimlichkeit des Zugriffs öffentlich zu beanstanden. Im Januar 2011 wurde bekannt, dass US-amerikanische Staatsanwälte mehrere Beweisanordnungen (*subpoena*) gegen Twitter erwirkt hatten.[183] Durch die Anordnungen sollte Twitter gezwungen werden, den Strafverfolgungsbehörden Profiliniformationen (Verkehrsdaten) von fünf Personen auszuhändigen, die im Verdacht standen, als Verschlusssache eingestufte Drahtberichte US-amerikanischer Diplomaten an WikiLeaks übermittelt zu haben.[184] Zwar sollte der Zugriff heimlich erfolgen. Twitter konnte jedoch einen Gerichtsbeschluss zur Aufhebung der Geheimhaltungspflicht erstreiten und setzte die fünf Nutzer unverzüglich über den Beschlagnahmebeschluss in Kenntnis.

Derartige Maßnahmen seitens der betroffenen Marktteilnehmer können mittelfristig ein Tätigwerden des Gesetzgebers allerdings nicht ersetzen. Die für Gegenstände der körperlichen Welt konzipierten Beschlagnahmevorschriften der StPO passen auf die Kommunikation im virtuellen Raum nur noch begrenzt. Mehr schlecht als recht behelfen sich Rechtsprechung und Lehre deshalb mit Analogien. So wird die E-Mail zum Brief, der Provider zum Postamt. Die Grenzen dieses Denkens in funktionalen Äquivalenten sind schon in Bezug auf die E-Mail-Beschlagnahme erkennbar. Natürlich wird ein Teil der Kommunikation, der früher in Brief- oder Telegrammform

182 *Levine*, Facebook and Social Networks (Fn. 93), S. 481 (487-488). Für den staatlichen Zugriff auf Inhaltsdaten gelten in den USA höhere Rechtfertigungsanforderungen als für andere Formen der Datenerhebung.

183 Dazu *R. MacKinnon*, Consent of the Networked, New York, NY: Basic Books 2012, S. 84; *S. Shane/J. F. Burns*, U.S. Subpoenas Twitter Over WikiLeaks Supporters, New York Times v. 8. 1. 2011 (abrufbar unter: >http://www.nytimes.com/2011/01/09/world/09wiki.html?pagewanted=all<).

184 Dazu nur *Y. Benkler*, A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate, Harvard Civil Rights-Civil Liberties Law Review 46 (2011), S. 311 (351 ff.).

stattfand, heute via E-Mail abgewickelt. Aber das macht die E-Mail nicht zu einem Brief. Ausgeblendet würden sonst nicht nur die technischen Besonderheiten der elektronischen Post, sondern auch der Umstand, dass diese Besonderheiten ihrerseits unser Kommunikationsverhalten verändern. Sekundenschnelle Zustellung, sofortige Abrufbarkeit auf dem Mobiltelefon, unbegrenzte Möglichkeiten der Speicherung außerhalb der eigenen Herrschaftssphäre – all dies prägt die Art und Weise, wie wir kommunizieren.

Es wäre jedoch ein Fehler und würde den legitimen Bedürfnissen der Strafverfolgungsorgane nicht gerecht, wollte man daraus den umgekehrten Schluss ziehen, dass künftig sämtliche Zugriffe auf elektronische Kommunikation pauschal an § 100a StPO zu messen seien.[185] Für eine Übergangsphase mag dies, wie wir argumentiert haben, die vorzugswürdige und konsistentere Lösung darstellen. Aber eine E-Mail oder ein Facebook-Posting sind eben auch nicht „in jeder Hinsicht" mit dem Abhören eines Telefons vergleichbar. Der virtuelle Raum hat völlig neue Formen der sozialen Interaktion und Kommunikation hervorgebracht, die eines funktionalen Äquivalents in der analogen Welt entbehren. Am Beispiel von Facebook wird dies – *pars pro toto* – augenfällig. Mit dem Netzwerk in die Alltagssprache eingezogene Neologismen wie der Begriff „liken" spiegeln die Andersartigkeit der Kommunikationsformen wider. Ein „Facebook-Freund" kann ein echter Freund sein, muss es aber nicht. Und ob eine Nachricht über Facebook oder als herkömmliche E-Mail verschickt wird, folgt komplexen sozialen Mustern.

Der Gesetzgeber ist gut beraten, sich den Besonderheiten der virtuellen Welt zu stellen. Zwar können die damit verbundenen technischen und sozialen Entwicklungen durch den dynamischen und entwicklungsoffenen Schutzbereich von Art. 10 Abs. 1 GG aufgefangen werden.[186] Entscheidend ist jedoch, was auf einfachgesetzlicher Ebene hieraus folgt. Das Demokratieprinzip (Art. 20 Abs. 2 GG) und das Rechtsstaatsprinzip (Art. 20 Abs. 3 GG) verpflichten den Gesetzgeber, diesbezüglich Rechtsicherheit mittels bestimmter, die beteiligten Interessen wahrender Regelungen zu schaffen.

Dazu gehört zuvörderst die Schaffung einer eigenständigen strafprozessualen Rechtsgrundlage für den Zugriff auf digitale Kommunikation in ihren unterschiedlichen Ausprägungen.[187] Die legislative Ambition sollte es nicht sein, sich dabei möglichst dicht an existierenden analogen Vorbildern zu orientieren. Vielmehr gilt es, die neuen Formen des digitalen Austausches in ihrer sozialen Bedeutung zu erfassen und damit ihre besondere Schutzbedürftigkeit korrekt abzuschätzen. Gerade das Beispiel Face-

185 Für eine konsequente Anwendung von § 100 a f. StPO hingegen *Neuhöfer* (Fn. 75), 329250.

186 Vgl. *C. Gusy*, in: von Mangoldt/Klein/Starck. Kommentar zum Grundgesetz: GG, 6. Aufl. (2010). Art. 10 Rn. 23; *Pagenkopf* (Fn. 79), Art. 10 Rn. 6.

187 Ähnlich in Bezug auf die E-Mail-Beschlagnahme auch *Wohlers* (Fn. 22), § 100a Rn. 35.

book demonstriert, wie nötig auch eine Verzahnung mit datenschutzrechtlichen Regelungen ist.[188] Denn die Beherrschbarkeit der mit der Facebook-Nutzung verbundenen Risiken und damit auch die Anforderungen an einen strafprozessualen Zugriff hängen maßgeblich davon ab, wie gut das Datenschutzrecht den Einzelnen schützt und mit welchem Grad an Autonomie der Einzelne von den ihm bereitgestellten Rechten Gebrauch macht. So kann ein Recht auf Vergessenwerden,[189] wie es in Art. 17 des Entwurfs über eine EU-Datenschutzverordnung[190] verankert ist, die Intensität des strafprozessualen Eingriffs erheblich abmildern – gerade dann, wenn das Recht durch eine fristgebundene automatische Löschung umgesetzt wird. Der Gesetzgeber hat es in der Hand, durch eine schutzfördernde Architektur des Datenschutzrechts[191] und einen geeigneten Instrumentenmix, die Intensität des strafprozessualen Zugriffs abzumildern. Eine grundlegende Neuregelung lässt sich freilich nicht herbeizaubern. Gleichwohl wäre es wünschenswert, wenn die Voraussetzungen für den Zugriff auf einen der größten Datenspeicher der Welt und damit Rechtssicherheit nach gründlicher Beratung im Parlament geschaffen würden – und nicht in Karlsruhe oder Reutlingen.

188 *J. Masing*, Herausforderungen des Datenschutzes, NJW 2012, S. 2305 (2309) plädiert dafür, dass die StPO „datenschutzrechtlich neu durchgesehen und in konsistenterer Weise ausdifferenziert" wird.

189 Weiterführend *V. Mayer-Schönberger*, Delete – The Virtue of Forgetting in the Digital Age, Princeton, NJ: Princeton University Press 2009; *N. Nolte*, Zum Recht auf Vergessen im Internet, ZRP 2011, S. 236 (236 f.); *A.-B. Kaiser*, Rechtlich gefordertes Nichtwissen im virtuellen Raum – Der Schutz der Privatsphäre im Web 2.0, in: H. *Hill/U. Schliesky (Hrsg.)*, Die Vermessung des virtuellen Raums. E-Volution des Rechts- und Verwaltungssystems III, 2012, S. 55.

190 Vorschlag über eine Europäische Datenschutz-Grundverordnung v. 25. 1. 2012 COM(2012) 11 final (abrufbar unter: >http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf<).

191 Dazu *L. Tien*, Architectural Regulation and the Evolution of Social Norms, Yale Journal of Law and Technology 7 (2005), S. 1; *Lessig*, Code (Fn. 134).