Soziale Netzwerke als Ort der Kriminalität und Ort von Ermittlungen

Wie wirken sich Online-Durchsuchung und Quellen-TKÜ auf die Nutzung sozialer Netzwerke aus?

*von Prof. Dr. Carsten Momsen und Philipp Bruckmann, B.A.**

Abstract
Mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens wurde das in der Strafprozessordnung normierte repressive Arsenal der Ermittlungsbehörden um Online-Durchsuchung und Quellen-TKÜ erweitert. Damit soll u.a. der weithin gängigen Verschlüsselungspraxis begegnet werden, an der die Überwachung von Online-Kommunikation auf Basis bisheriger Befugnisse vielfach scheitert. Diese Form der "digitalen" Strafverfolgung erfasst auch und gerade die Kommunikation mittels „Social Media".

Dabei ist das Verhältnis der Verlagerung eines erheblichen Anteils der Kommunikation in den virtuellen Raum und der staatlichen Reaktion in Gestalt der §§ 100a Abs. 1 S. 2, 100b StPO n.F. kein einseitiges: Die neuen behördlichen Befugnisse sind mit Blick auf ihre Reichweite ihrerseits nicht nur für Menschen von Bedeutung, die aufgrund eigener Aktivitäten damit rechnen müssen, als Beschuldigte in den Fokus der Strafverfolgung zu geraten. Der Kreis potenziell betroffener Dritter ist um ein Vielfaches größer als im Fall herkömmlicher Kommunikationsbeziehungen. Zugrunde liegt dem der spezifische Charakter der Kommunikation in sozialen Medien.

Die Auseinandersetzung mit der Frage, was dies für ein verantwortliches Online-Verhalten auch des „Normalnutzers" bedeutet, legt nahe, dass ein Grundmaß an Sicherheit, nicht als Beifang in den Fokus der Behörden zu geraten, vor diesem Hintergrund allenfalls um den Preis des Verzichts auf die oder der ganz erheblichen, deren Wesen zuwiderlaufenden Einschränkung der Kommunikation in sozialen Medien zu erreichen ist.

Auch eine „Flucht" ins Darknet, den anonymisierten und vermeintlich überwachungssichereren Bereich des Internets, erscheint dabei aufgrund der demselben eigenen erhöhten Gefahren und eingeschränkten Möglichkeiten bei aller Notwendigkeit anonymisierter Kommunikationswege gegenwärtig für den „Normalnutzer" nicht als Alternative.

I. Einleitung

Dass die digitale Revolution das Leben in allen Facetten erfasst und teilweise sehr gründlich verändert hat und permanent weiter verändert, ist ein Allgemeinplatz. Dass diese Entwicklung sich permanent beschleunigt, ist möglicherweise ein Eindruck, der eher auf das eigene vorgerückte Lebensalter hindeutet. Ganz sicher aber potenzieren sich die Möglichkeiten, Straftaten zu begehen. Dies zwingt die Strafverfolgungsbehörden dazu, sich anzupassen. In dem Bemühen, dem Verbrechen nicht immer einen Schritt hinterherzulaufen, sondern auf Ballhöhe zu bleiben oder sogar einmal einen Schritt voraus zu sein, schießen die Methoden gelegentlich über das Ziel hinaus und begründen Gefahren eigener Art, insbesondere für die sogenannten „bürgerlichen Freiheiten". Gerade das Internet entwickelte sich zu einem allgemeinen Kommunikationsraum unter dem Ideal der Freiheit, teilweise auch der Konventionsfreiheit, mit dem Anspruch der Überwachungsfreiheit und der Freiheit des Zugangs zu Informationen. Dass diese Freiheitsideale nicht oder doch nur teilweise eingelöst wurden und mehr und mehr unter Druck geraten, hat sehr verschiedene Ursachen. Eine davon ist, dass nicht nur Kommunikation ins Internet verlagert wurde, sondern damit zugleich auch mehr und mehr rechtlich geschützte Interessen (Strafrechtler versuchen immer noch, den Begriff des Rechtsguts in die digitale Zeit mitzunehmen).[1] Deren Schutz verlangt Einschränkungen einer ungezügelten Freiheit, um das digitale Faustrecht zu verhindern. Der Gesellschaftsvertrag gilt als Idee ohne jede Einschränkung auch im Internet. Ziel der folgenden Ausführungen ist es, auszuloten, welche Gefahren durch die Nutzung sozialer Netzwerke von „digitalen Straftaten" einerseits und von „digitalen Ermittlungen" andererseits ausgehen. Sollte das Verhalten im Internet sich nicht den Gefahren anpassen, um unnötige Risiken zu vermeiden, genau wie man es ohne näher darüber nachzudenken auch in der analogen Welt macht? Sollte man anders als zumeist in der

---

* *Prof. Dr. Carsten Momsen* leitet den Arbeitsbereich „Strafrecht, Strafverfahrensrecht, Wirtschafts- und Umweltstrafrecht" an der Freien Universität Berlin, *Philipp Bruckmann*, B.A., ist Mitarbeiter am Arbeitsbereich. Der Text folgt einem Vortrag, den der Verfasser *Momsen* im Rahmen des Berliner Forschungsverbunds „Recht im Kontext" am 5.11.2018 unter dem Titel „Soziale Netzwerke als Ort der Kriminalität und Ort von Ermittlungen – wie wirken sich Online-Durchsuchung und Quellen-TKÜ auf die Nutzung sozialer Netzwerke aus?" an der Humboldt Universität zu Berlin gehalten hat. Die Vortragsform wurde weitgehend beibehalten.

[1] S. aus jüngerer Zeit nur *Kahler/Hoffmann-Holland*, KriPoZ 2018, 267.

analogen Welt im digitalen Raum nicht die „dunklen Gassen" meiden, sondern sie gerade aufsuchen, um sich zu schützen – vor Kriminalität, aber auch den kollateralen Folgen der Kriminalitätsbekämpfung?

II. Charakter der Kommunikation in sozialen Medien

Wer sich in sozialen Netzwerken bewegt, ist an Kommunikation interessiert. Man chattet, postet, liked und shared. Das Spektrum der Inhalte, die Gegenstand des Austauschs werden, reicht von Katzenbildern und Party-Einladungen bis hin zu komplexen politischen Analysen. Neben dem Austausch mit bereits bekannten Freundinnen, Freunden und Kollegen liegt der Reiz von Plattformen wie Facebook, Google Plus und Co. dabei gerade auch in der Möglichkeit, vermittelt über gemeinsame Interessen, Themen oder Freunde neue Bekanntschaften zu knüpfen.

Auf der einen Seite ergeben sich daraus gänzlich neue Chancen, wenn es darum geht, bestimmte Themen in den Fokus der öffentlichen Aufmerksamkeit zu rücken und Probleme zu lösen. Sei es die Suche nach geeigneten Blut-, Stammzellen- oder Knochenmarkspendern, Crowdfunding-Projekte oder die Organisation politischer Protestaktionen verschiedenster Art – soziale Netzwerke bieten vielfach ein wertvolles Forum.

Auf der anderen Seite begibt man sich im Zuge der vermehrten Kommunikation mit individuellen Unbekannten, vor allem aber auch mit einer Öffentlichkeit, deren Grenzen kaum klar zu ziehen sind, der Möglichkeit, Kommunikationspartner sorgfältig auszuwählen. Wie sich schon darin ausdrückt, dass sämtliche Kontakte nicht etwa zunächst „Bekannte" oder ähnliches, sondern von Beginn an – mit einem Klick – „Freunde" sind, lässt sich die Vielschichtigkeit analog entstehender sozialer Beziehungen, das Nach-und-nach des Kennenlernens online kaum entsprechend abbilden. Zwar halten Netzwerke regelmäßig die Option vor, die Reichweite einzelner Äußerungen personengenau zu bestimmen und so beim Teilen privater Informationen zwischen verschiedenen „Freunden" zu differenzieren. Auch wäre es sicher falsch, pauschal zu behaupten, diese Möglichkeit würde nie genutzt. Mindestens ebenso falsch wäre es jedoch, sie als Nutzungsstandard zu bezeichnen.

Wollte man die Öffentlichkeitsdimension, die Postings, Likes und Shares in sozialen Netzwerken demnach vielfach zukommt, auf die analoge Welt übertragen, hätte man sich vorzustellen, dass Menschen in einer belebten Fußgängerzone immer wieder unvermittelt stehen bleiben und ungefragt lautstarke Mitteilungen machen wie „Ich mag die Rolling Stones" und „Vielleicht (oder sicher) besuche ich ihr Konzert nächsten Monat im Olympiastadion". Das mutet zunächst befremdlich und etwas amüsant, in Bezug auf Äußerungen wie die genannten aber auch recht harmlos an. Anders, wenn es um kontroverse politische Äußerungen geht. So werden Menschen etwa für kritische Äußerungen über die türkische Politik bei Reisen in die Türkei häufig von den dortigen Strafverfolgungsbehörden belangt.[2] Dass dies oftmals noch Jahre später geschieht, verweist auf einen entscheidenden Unterschied zwischen Postings in sozialen Netzwerken und Auftritten in einer Fußgängerzone: Während letztere nicht notwendigerweise dokumentiert werden, sind erstere, wenn einmal getätigt, nicht so leicht wieder aus der Welt zu schaffen. In der Zusammenschau mit dem Umstand, dass in beiden Konstellationen kaum sicher kontrolliert werden kann, wer alles Zeuge des jeweiligen Verhaltens wird, wird unschwer erkennbar, worin die Attraktivität und Erfolgschance neuer Ermittlungsmaßnahmen und -befugnisse im virtuellen Raum aus Sicht der Strafverfolgungsbehörden liegt. Kommt die Vorstellung, alle je getätigten Äußerungen würden dauerhaft aufgezeichnet und wären für einen unbestimmten Personenkreis potenziell jederzeit nachvollzieh- und abrufbar, in Bezug auf die analoge Welt einer Orwell'schen Dystopie gleich, so ist sie in Bezug auf soziale Medien Realität.

Gleiches gilt für die Idee des verdeckten Ermittlers. Man stelle sich vor, dass ein Polizeibeamter einem Verdächtigen unter einer innerhalb weniger Minuten zusammengeschusterten falschen Identität – also quasi mit einer mehr schlecht als recht ausgeschnittenen Papiermaske – als potenzieller Freund gegenübertritt. Auf der Straße kaum denkbar. In sozialen Netzwerken? *Technisch* kein Problem. Vor diesem Hintergrund stellen sich diverse Fragen. Gibt es bspw. effektive Möglichkeiten, sich gegen einen per Facebook-Chat platzierten Trojaner zu schützen? Denn für den Verdächtigen ist es im virtuellen Raum ungleich schwerer zu erkennen, ob er nicht statt mit dem beabsichtigten Gesprächspartner mit einer Ermittlungsbehörde kommuniziert. Nun mag diese Frage primär für Personen von Interesse sein, die aufgrund eigener krimineller Aktivitäten die Möglichkeit in Betracht ziehen müssen, tatsächlich selbst zum Ziel strafverfolgungsbehördlicher Überwachungsbestrebungen zu werden. Sofern diese über die Möglichkeiten der Ermittlungsbehörden im Bilde sind, kann davon ausgegangen werden, dass sie soziale Netzwerke wie Facebook, in denen sich die Frage der Öffentlichkeit in besonderem Maße stellt, wohl nicht primär zur Kommunikation über ihre Geschäfte nutzen.

Doch auch für Userinnen und User, die nicht davon ausgehen, in den Fokus der Strafverfolgungsbehörden zu geraten – man könnte sagen, Normalnutzer –, sind die insofern veränderten Vorzeichen, unter denen Kommunikation in sozialen Netzwerken stattfindet, von Interesse. Denn der Kreis potenziell mitbetroffener Kommunikationspartner eines überwachten Verdächtigen in sozialen Netzwerken ist um ein Vielfaches größer ist als bei herkömmlicher Telekommunikationsüberwachung. Damit

---

[2] S. statt vieler nur http://www.spiegel.de/politik/ausland/tuerkei-angebliche-erdogan-beleidigung-bringt-deutschen-ins-gefaengnis-a-1230946.html (zul. abgerufen am 01.10.2018). Auf die Praxis willkürlicher Inhaftierungen auch deutscher Staatsangehöriger „in Zusammenhang mit regierungskritischen Stellungnahmen in sozialen Medien" weisen auch die Reise- und Sicherheitshinweise des Auswärtigen Amts zur Türkei vom 4.10.2018 hin (https://www.auswaertiges-amt.de/de/aussenpolitik/laender/tuerkei-node/tuerkeisicherheit/201962, zul. abgerufen am 4.10.2018).

steigt die Zahl der ins Visier der Ermittlungsbehörden geratenden völlig unverdächtigen Personen exponentiell an. Unter der Prämisse, dass es nicht um den Versuch gehen kann, gleichsam die Uhr zurückzudrehen und die Wiederabschaffung oder auch nur das umfassende Meiden sozialer Medien zu propagieren, muss die Kernfrage demnach lauten: Welche Konsequenzen ergeben sich aus modernen Ermittlungsmethoden und -befugnissen der Strafverfolgungsbehörden aus Sicht des Normalnutzers für ein verantwortliches Nutzungsverhalten in sozialen Medien? Spielen internationale Entwicklungen im Bereich des Datenschutzes bzw. des Zugriffs von Ermittlungsbehörden auf Daten dabei eine Rolle? Abschließend wird die Frage gestellt, ob der weitgehend anonymisierte Bereich des Internets keine vergleichbaren Nachteile für die Nutzer sozialer Medien aufweisen würde. Würde also eine Flucht ins Darknet am Ende als ernsthafte Alternative in Betracht kommen? Dabei sind diese Überlegungen aus zwei Gründen eher theoretischer Natur. Zum einen lassen sich die Bedürfnisse, die durch Social Media angesprochen werden, nicht ohne weiteres in anonymisierter Form befriedigen. Nach derzeitigem Stand der Technik lassen sich beide Bereiche jedenfalls nicht so miteinander kombinieren, dass die Anonymität nicht spätestens an der Schnittstelle zum „offenen" Internet aufgehoben würde. Zum anderen würde eine Verlagerung der massenhaften Online-Kommunikation ins Darknet dieses vorhersehbar ins Zentrum der Aufmerksamkeit sämtlicher Überwachungsinteressen rücken.

III. Quellen-TKÜ und Online-Durchsuchung

Die Beantwortung dieser Frage setzt die Auseinandersetzung mit den einschlägigen strafprozessualen Eingriffsermächtigungen voraus. Zentrale Normen sind hier die sogenannte Quellen-TKÜ, seit August 2017 in § 100a der Strafprozessordnung normiert, und die mit demselben Gesetz in § 100b StPO geregelte Online-Durchsuchung. Was dürfen Ermittlungsbehörden? Welche Grenzen sind ihnen gesetzt?

1. Die Quellen-TKÜ – § 100a Abs. 1 S. 2, 3 StPO

Während der öffentlich zugängliche Anteil geteilter Profil-Informationen – etwa das Profilbild – ebenso wie der „Facebook-öffentliche", also der von jedem Inhaber eines Facebook-Accounts einsehbare Teil, auch von Strafverfolgungsbehörden ohne besondere Ermächtigungsgrundlage im Rahmen ihrer allgemeinen Ermittlungskompetenz gem. §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 1 StPO wahrgenommen und im Strafverfahren verwertet werden kann,[3] bedarf der behördliche Zugriff auf Messenger-Nachrichten, sofern diese nicht gerade an einen unter Klarnamen auftretenden oder nach § 110a StPO zulässigerweise verdeckt operierenden Ermittler gerichtet werden, gesonderter Ermächtigung zur Telekommunikationsüberwachung. Eine solche Ermächtigung stellt die herkömmliche TKÜ i.S.d. § 100a Abs. 1 S. 1 StPO dar. Diese gestattet Ermittlungsbehörden unter bestimmten Voraussetzungen den Zugriff auf Kommunikationsinhalte, die sich auf dem Weg von einer Partei zur anderen befinden.

Was, soweit es um das Abhören von Telefonaten, das Mitlesen von SMS und dergleichen geht, grundsätzlich völlig ausreicht, stößt im Bereich der Messenger-Kommunikation über soziale Netzwerke oder auch der Internet-Telefonie schnell an seine Grenzen. Denn sämtliche nennenswerten sozialen Netzwerke versehen die private Kommunikation ihrer Nutzer mit End-zu-End-Verschlüsselung,[4] die nach dem Stand der Technik auch von Strafverfolgungsbehörden nicht umgangen werden kann.

Hier kommt die Quellen-TKÜ ins Spiel: Anders als die herkömmliche TKÜ ermöglicht sie es, Kommunikationsinhalte abzufangen und auszuleiten, *bevor* sie vom informationstechnischen Gerät ihres Absenders verschlüsselt und verschickt werden. Gleiches gilt für das Gerät des Empfängers, wo die Kommunikationsinhalte wieder entschlüsselt dargestellt und gespeichert werden. Ungeachtet aller Verschlüsselungsbemühungen sind für die Ermittlungsbehörden dadurch sämtliche Inhalte darstell- und abgreifbar.

Nur am Rande sei erwähnt, dass die Quellen-TKÜ ebenso wie die Online-Durchsuchung in verschiedener Hinsicht verfassungsrechtlichen Bedenken begegnet, die bereits mit dem Gesetzgebungsprozess beginnen: Im Wege eines Änderungsantrags gem. § 82 Abs. 1 GOBT wurde ihre Grundlage gleichsam so spät wie möglich – und im Fall der Online-Durchsuchung nicht nur ohne Empfehlung, sondern entgegen ablehnender Tendenzen der Expertenkommission[5] – zum Gegenstand eines bereits laufenden Gesetzgebungsverfahrens gemacht, zu dessen sonstigen Inhalten sie in keiner besonderen Beziehung steht. Manche sagen, hinein „geschmuggelt"[6] wie ein Virus im Anhang einer Mail.

Verfassungsrechtliche Zweifel werden auch mit Blick auf die identischen Eingriffsvoraussetzungen von klassischer und Quellen-TKÜ angemeldet. Moniert wird insoweit die offensichtlich erhöhte Eingriffsintensität letzterer Maßnahme:[7] Anders als herkömmliche TKÜ, die lediglich das Fernmeldegeheimnis gem. Art. 10 GG tangiert – das Abgreifen der Daten erfolgt für gewöhnlich beim Kommunikationsdienstleister –, infiltriert die Quellen-TKÜ das informationstechnische System des Betroffenen und greift somit in sein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[8] ein. Schwer zu leugnen ist zudem ein gewisser Widerspruch zwischen der etwa in § 3 Abs. 1 S. 1 BSIG niedergelegten Verpflichtung des Staates, auf die Förderung der Sicherheit informationstechnischer Systeme hinzuwirken, und sei-

---

3 *Graf,* in: BeckOK-StPO, Stand 15.10.2018, § 100a Rn. 87.
4 So auch BT-Drs. 18/12785, S. 51.
5 Bericht der Expertenkommission zur effektiveren und praxistauglicheren Ausgestaltung des allgemeinen Strafverfahrens und des jugendgerichtlichen Verfahrens (https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Abschlussbericht_Reform_StPO_Kommission.pdf?__blob=publicationFile&v=2, zul. abgerufen am 4.10.2018), S. 73 ff.; vgl. *Schiemann*, KriPoZ 2018, 338 f.
6 *Rubbert*, Editorial StV 9/2017, I.
7 Vgl. *Schiemann*, KriPoZ 2018, 338 (341).
8 Vgl. BVerfGE 120, 274.

nem in Konsequenz strafverfolgungsbehördlicher Kompetenzen wie der Quellen-TKÜ notwendig gegebenen Interesse daran, Sicherheitslücken in ebendiesen Systemen offenzuhalten, die behördliche Infiltration erst ermöglichen.[9]

a) Eingriffsvoraussetzungen

Die erwähnte Parallelität der Eingriffsvoraussetzungen für herkömmliche und Quellen-TKÜ ergibt sich aus dem Normaufbau des § 100a StPO, der die Quellen-TKÜ unter denselben Voraussetzungen wie die herkömmliche gestattet, wenn dies – so § 100a Abs. 1 S. 2 StPO – notwendig ist, um die Überwachung und Aufzeichnung von Kommunikationsinhalten insbesondere in unverschlüsselter Form zu ermöglichen.

aa) Subsidiarität gegenüber herkömmlicher TKÜ
Die Rolle der Quellen-TKÜ gegenüber der herkömmlichen TKÜ ist insofern subsidiär: Der Zugriff auf das informationstechnische Gerät eines Beschuldigten ist nur zulässig, sofern klassische TKÜ-Maßnahmen keinen Erfolg versprechen.[10] Über die Möglichkeiten letzterer hinausgehend berechtigt § 100a Abs. 1 S. 3 StPO zur Erfassung von Kommunikationsinhalten und -umständen nicht nur während der laufenden Kommunikation, sondern auch, wenn diese auf dem informationstechnischen Gerät gespeichert sind. Die Beschränkung dieser Möglichkeit auf solche Inhalte und Umstände, die auch während der laufenden Kommunikation per Zugriff auf das öffentliche Telekommunikationsnetz in verschlüsselter Form hätten erhoben werden können, soll nach Darstellung des Gesetzgebers die „funktionale Äquivalenz mit der herkömmlichen Telekommunikationsüberwachung“[11] gewährleisten. Auch darf nur auf solche Kommunikation zugegriffen werden, die nach Anordnung der Maßnahme erfolgt ist.[12] Angesichts dessen, dass der Nachweis der Notwendigkeit von Quellen-TKÜ-Maßnahmen dabei lediglich die begründete Annahme seitens der Strafverfolgungsbehörden verlangt, ein Beschuldigter kommuniziere verschlüsselt – was er, sofern es um soziale Medien geht, wie dargestellt ganz ohne eigenes Zutun ganz automatisch tut –, wird die Eignung dieser Subsidiaritätsklausel, begrenzende Wirkung im Sinne des Verhältnismäßigkeitsgrundsatzes zu entfalten, mit gutem Grund bestritten.[13]

bb) Verdacht einer schweren Straftat aufgrund bestimmter Tatsachen
Gem. § 100a Abs. 1 S. 2 StPO ist die Überwachung der Telekommunikation – und damit auch die Quellen-TKÜ – zulässig, wenn bestimmte Tatsachen den Verdacht einer schweren Straftat i.S.d. Abs. 2 begründen, die auch im Einzelfall schwer wiegt, und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre. Es müssen also konkrete Umstände vorliegen, die nach der (kriminalistischen) Lebenserfahrung erheblich darauf hindeuten, dass jemand als Täter oder Teilnehmer eine Katalogtat begangen hat.[14] Wenngleich die Anforderungen an einen solchen Verdacht gegenüber dem normalen Anfangsverdacht etwas gesteigert sind, ist weder ein hinreichender noch ein dringender Tatverdacht erforderlich.[15] Die Qualifikation einer Tat als „schwer“ i.S.d. § 100a Abs. 2 StPO sieht das *BVerfG* mit Blick auf die mittels des jeweiligen Straftatbestands geschützten Rechtsgüter wie etwa die Funktionsfähigkeit des Staates oder seiner Einrichtungen als vom Gestaltungsspielraum des Gesetzgebers umfasst.[16] Unter Verweis auf das Fehlen einer plausiblen dogmatischen Struktur wird der Anlasstatenkatalog nichtsdestoweniger teils als „partiell unverhältnismäßig“ bezeichnet.[17]

b) Verfahren

aa) Anordnung, § 100e Abs. 1 StPO
Zur Anordnung der Quellen-TKÜ ist gem. § 100e Abs. 1 S. 1 StPO grundsätzlich nur das zuständige Gericht, gem. Abs. 1 S. 2 bei Gefahr im Verzug jedoch auch die Staatsanwaltschaft befugt.

bb) Technische Beschränkung, Schutz und Rückgängigmachung, § 100a Abs. 5 StPO
Jede geschaffene Zugriffsmöglichkeit ist gem. § 100a Abs. 5 S. 1 StPO so zu beschränken, dass nur die kommunikationsbezogenen Inhalte erfasst werden *können*, die nach der Ratio des § 100a StPO erfasst werden *sollen*. Vorgenommene Änderungen sind nach Beendigung der Maßnahme – soweit technisch möglich – automatisiert wieder rückgängig zu machen. Ebenso auf den *state of the art* beschränkt ist die von Abs. 5 S. 2 statuierte Pflicht zum Schutz des eingesetzten Programms gegen unbefugte Nutzung und Kenntnisnahme durch Dritte. Schon die Formulierung „nach dem Stand des technisch Möglichen“ erkennt dabei an, dass geöffnete Sicherheitslücken den Betroffenen unter Umständen durchaus auch dem erhöhten Risiko eines solchen unbefugten Eindringens – bspw. durch Kriminelle – aussetzen können.

cc) Protokollierung, § 100a Abs. 6 StPO
§ 100a Abs. 6 StPO gibt für jeden Fall der TKÜ und Quellen-TKÜ umfangreiche Protokollierungspflichten vor. Festzuhalten sind das eingesetzte technische Mittel, der Einsatzzeitpunkt, Angaben zum infiltrierten informationstechnischen System und daran vorgenommenen Änderungen, zur Möglichkeit der Feststellung der erhobenen Daten sowie zur verantwortlichen Organisationseinheit.

dd) Kernbereichsschutz, § 100d StPO
§ 100d schützt „Erkenntnisse aus dem Kernbereich privater Lebensgestaltung“. Insbesondere erklärt Abs. 1 Maßnahmen für unzulässig, die nur solche zu erbringen versprechen. Im Rahmen ansonsten zulässiger Maßnahmen

---

9 *Roggan*, StV 2017, 821 (829).
10 BT-Drs. 18/12785, S. 51; *Schiemann*, KriPoZ 2018, 338 (341); *Singelnstein/Derin*, NJW 2017, 2646 (2648).
11 BT-Drs. 18/12785, S. 51.
12 BT-Drs 18/12785, S. 50 f.; *Singelnstein/Derin*, NJW 2017, 2646 (2648).
13 S. etwa *Roggan*, StV 2017, 821 (822), der prognostiziert, „angesichts sich wandelnder Kommunikationsgewohnheiten“ werde sich die Quellen-TKÜ „als standardmäßige TKÜ-Methode etablieren und […] die ‚klassischen‘ TKÜ-Maßnahmen sogar quantitativ überholen“.
14 Graf, in: BeckOK-StPO, § 100a Rn. 100.
15 *BGH,* Beschl. v. 11.8.2016 – StB 12/16 (BeckRS 2016, 15673, Rn. 9).
16 *BVerfG*, NJW 2011, 833 (836).
17 *Eschelbach*, in: SSW-StPO, 3. Aufl. (2018), § 100a Rn. 10.

gewonnene Erkenntnisse aus diesem Bereich sind gem. Abs. 2 S. 1 nicht verwertbar.

c) Möglichkeiten und Umstände des Betroffenseins Dritter

Als mögliche Betroffene nennt § 100a Abs. 3 StPO neben dem Beschuldigten nur solche Personen, von denen zu vermuten ist, dass sie für den Beschuldigten als Nachrichtenmittler auftreten oder dass dieser – mit oder ohne ihr Wissen – ihr informationstechnisches System benutzt. Doch liegt es im Wesen der Überwachung jeder Kommunikation, dass auch Kommunikations-Partner des oder der Überwachten von der Maßnahme nicht unberührt bleiben. Anders als etwa bei einem traditionellen Telefongespräch, dem bilderbuchmäßigen Anwendungsbeispiel herkömmlicher TKÜ, trifft dies in sozialen Medien oftmals nicht nur einen, sondern eine Vielzahl von Gesprächspartnern. Neben der Kommunikation etwa in Facebook-Gruppen, die Ermittlungsbehörden unverschlüsselt zugänglich ist, denke man nur an all die Gruppenchats über WhatsApp, Telegramm oder einen beliebigen anderen Messenger-Dienst, deren Teil man oft genug ohne eigene Entscheidung qua Hinzufügung durch irgendeinen Kontakt wird.

Im Ganzen findet Kommunikation in sozialen Medien ja – wie eingangs erwähnt – gerade nicht nur mit engen Bekannten statt. Nun verzichtet man gerade im Zusammenhang gerade erwähnter Gruppenchats oftmals ohnehin auf den Versuch, sich einen Eindruck von allen Teilnehmern zu verschaffen. Mit Blick auf den Katalog „schwerer Straftaten" des § 100a Abs. 2 StPO, der keineswegs nur Straftaten gegen die Landesverteidigung oder den öffentlichen Frieden etc., sondern auch Tatbestände enthält, über deren mögliche Verwirklichung durch einen Gesprächspartner ein kurzer oder auch längerer Blick auf Profilbilder, Likes etc. – geschweige denn auf eine Telefonnummer! – wohl keinen Aufschluss gibt, bringt das den Nutzer sozialer Medien in die prekäre Situation, nie sichergehen zu können, nicht zufällig seinerseits in den ermittlungsbehördlichen Fokus zu geraten. Denn ob jemand etwa als Arzt schon einmal einem Minderjährigen ein Dopingmittel verschrieben hat (§ 100a Abs. 2 Nr. 3 StPO, § 4 Abs. 4 Nr. 2 lit. b AntiDopG) oder schon einmal Geschlechtsverkehr mit einer erheblich alkoholisierten Person hatte, ohne sich zuvor ihrer ausdrücklichen Zustimmung zu versichern (§ 100a Abs. 2 Nr. 1 lit. f StPO, § 177 Abs. 2 Nr. 2, 6 Nr. 1 StGB), ist ihm schon im analogen Kontakt kaum an der Nasenspitze anzusehen. Das Risiko, als eigentlich nichtbetroffener Gesprächspartner von Ermittlungsbehörden unter gewissen Umständen miterfasst zu werden, das im Grundsatz wie gesagt auch von der herkömmlichen TKÜ für das Leben außerhalb Sozialer Medien und die Kommunikation außerhalb des Internets ausgeht, gilt mit Blick auf die Quellen-TKÜ somit aufgrund der spezifischen Natur der Kommunikation in Sozialen Netzen und ihrer verringerten Möglichkeit, Beziehungen zu verschiedenen Personen verschieden eng zu gestalten, in ungleich erhöhtem Maß.

Um als *User* sicherzugehen, Kommunikationsinhalte nicht mit Strafverfolgungsbehörden teilen zu müssen, reicht es demnach schon mit Blick auf die Quellen-TKÜ keineswegs aus, sich von potenziellen Gesprächspartnern fernzuhalten, die den Eindruck erwecken, eventuell nach §§ 129 ff. StGB verfolgt zu werden. Und selbst im Bereich des Terrorismus ließe sich nicht einmal auf der Basis primitivster Vorurteile entscheiden, wer als Kommunikationspartner ausscheidet.

2. Die Online-Durchsuchung – § 100b StPO

Im Zuge desselben Gesetzgebungsverfahrens wie die Quellen-TKÜ wurde 2017 auch die Online-Durchsuchung mit § 100b StPO n.F. ausdrücklich in das ermittlungsbehördliche Arsenal aufgenommen. Nach der Legaldefinition des § 100b Abs. 1 S. 1 StPO erfolgt sie durch Eingriff in ein und Datenentnahme aus einem informationstechnischen System mit technischen Mitteln ohne Wissen des Betroffenen. Über den auf kommunikationsbezogene Inhalte beschränkten Rahmen der Quellen-TKÜ geht sie bei technisch nahezu identischem Vorgehen hinaus und erfasst „alle auf einem IT-System gespeicherten Inhalte", also „gespeicherte Mails unabhängig vom Zeitpunkt ihres Empfangs, SMS- und WhatsApp-Nachrichten, Fotodateien, Social-Media-Kontakte etc.".[18]

a) Eingriffsvoraussetzungen

Die materiellen Eingriffsvoraussetzungen des § 100b Abs. 1 StPO entsprechen den bereits erläuterten Voraussetzungen des § 100a Abs. 1 StPO zur (Quellen-)TKÜ. Den Anlasstatenkatalog des § 100b Abs. 2 StPO indes teilt die Online-Durchsuchung gem. § 100c Abs. 1 Nr. 1 StPO mit dem großen Lauschangriff, der akustischen Wohnraumüberwachung. Diese Parallelität erklärt sich daraus, dass die Online-Durchsuchung in das Grundrecht des Betroffenen auf Integrität und Vertraulichkeit informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eingreift[19] und in ihrer Eingriffsintensität insofern der Wohnraumüberwachung gleichkommt.[20] Der Anlasstaten-Katalog setzt sich dabei zusammen aus Taten, die mit Blick auf betroffenes Rechtsgut und angedrohte Strafe besonders schwer wiegen, aber auch aus solchen, deren Verfolgung typischerweise größeren Schwierigkeiten in der Beschaffung belastbarer Beweise begegnet.[21]

b) Verfahren

aa) Anordnung, § 100e Abs. 2 StPO
Wie grundsätzlich auch bei der Quellen-TKÜ ist die Anordnung der Online-Durchsuchung gem. § 100e Abs. 2 S. 1 StPO dem zuständigen Gericht vorbehalten. Anders als bei jener aber geht sie auch bei Gefahr im Verzug nicht auf die Staatsanwaltschaft über, sondern kann lediglich nach § 100e Abs. 2 S. 2 StPO vom Vorsitzenden selbständig ausgeübt werden. Auch insoweit entsprechen die Regelungen zur Online-Durchsuchung jenen zum großen Lauschangriff. Nicht klar geregelt ist indes das Subsidiaritätsverhältnis zwischen diesen beiden Eingriffen. Da die Onlinedurchsuchung zumindest technisch Eingriffe ermöglicht, die der Zielrichtung nach auch §§ 100a, 100c

18 *Roggan*, StV 2017, 821 (825).
19 *Graf*, in: BeckOK-StPO, § 100b Rn. 8.
20 BT-Drs. 18/12785, S. 54 unter Verweis auf *BVerfG*, Urt. v. 27.2.2008 – 1 BvR 370/07, Rn. 200; *Eschelbach*, in: SSW-StPO, § 100b Rn. 3.
21 *Eschelbach*, in: SSW-StPO, § 100b Rn. 11.

und 97 StPO erfolgen könnten, spricht vieles dafür, § 100b StPO als die insgesamt eingriffsintensivste und potentiell grundrechtsinvasivste Maßnahme anzusehen. Dementsprechend würde Subsidiarität gegenüber allen vorgenannten Eingriffen bestehen.

bb) Kernbereichsschutz, § 100d StPO

Auch hier sind Maßnahmen gem. § 100d Abs. 1 StPO unzulässig, wenn sie nur den Gewinn von Erkenntnissen aus dem Kernbereich privater Lebensgestaltung versprechen. Im Rahmen zulässiger Maßnahmen gewonnene Kernbereichserkenntnisse dürfen gem. § 100d Abs. 2 S. 1 StPO nicht verwertet werden. Über die Restriktionen zur TKÜ hinaus ist bei der Online-Durchsuchung gem. § 100d Abs. 3 StPO auch – im Rahmen des Möglichen – technisch sicherzustellen, dass Kernbereichsdaten gar nicht erst erhoben werden (S. 1). Geschieht dies doch, sind sie unverzüglich zu löschen oder dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit vorzulegen (S. 3).

cc) Technische Beschränkung und Protokollierung, § 100b Abs. 4 i.V.m. § 100a Abs. 5, 6 StPO

Auch Maßnahmen der Online-Durchsuchung sind technisch zu beschränken. § 100b Abs. 4 StPO verweist insofern auf § 100a Abs. 5 und 6 StPO. Von diesem Verweis ausgenommen ist lediglich die Einschränkung auf den Bereich laufender Telekommunikation. Bezüglich der Pflicht zur Protokollierung sämtlicher Maßnahmen gilt § 100a Abs. 6 StPO gem. § 100b Abs. 4 StPO entsprechend.

c) Möglichkeiten und Umstände des Betroffenseins Dritter

Wenngleich sich die Online-Durchsuchung gem. § 100b Abs. 3 S. 1 StPO nur gegen den Beschuldigten richten darf, können auch hier Dritte betroffen sein. Dies zum einen, wenn bestimmte Tatsachen nahelegen, dass der Beschuldigte ein ihnen gehörendes informationstechnisches System nutzt oder ein Eingriff in dessen informationstechnisches System nicht ausreicht (Abs. 3 S. 2). Zum anderen aber – und das ist vor dem Hintergrund der Frage nach den Implikationen von Quellen-TKÜ und Online-Durchsuchung für „Normalnutzer" in erster Linie von Interesse – können Dritte im Rahmen einer zulässigen Maßnahme gem. § 100b Abs. 3 S. 3 StPO auch betroffen sein, wenn dies „unvermeidbar" ist. Denn wenngleich die Unvermeidbarkeit im Einzelfall zu prüfen ist,[22] ist es diese Norm, aufgrund derer die Online-Durchsuchung auch Informationen vollständig unbeteiligter Dritter erfassen kann, die etwa durch soziale Medien mit einem Beschuldigten in Kontakt stehen.[23]

Dies wird kritisiert als „‚Ausuferung' der eingriffsintensivsten Maßnahme auf absolut Unverdächtige".[24] Wie bei der Quellen-TKÜ gilt hier aus Sicht von „Normalnutzern", für die sich Ermittlungsbehörden vermeintlich nicht interessieren, dass es kaum möglich ist, sich mit ansatzweiser Sicherheit aus dem behördlichen Fokus herauszuhalten. Denn wie dargestellt entspricht es nicht dem Wesen sozialer Medien, dort gepflegte Kontakte auf enge Bekannte aus dem analogen Leben zu beschränken, über deren strafrechtliche Unverdächtigkeit man fortlaufend informiert ist.

Auch in dieser Hinsicht geht die Online-Durchsuchung über die Quellen-TKÜ noch hinaus und greift selbst in den Bereich des Offline-Verhaltens über, was sich schon daraus ergibt, dass zu all den auf einem PC gespeicherten, der Online-Durchsuchung zugänglichen und für Ermittlungsbehörden potenziell interessanten Daten nicht zuletzt Bilddateien gehören, die wiederum Personen, die gemeinsam mit dem Beschuldigten abgebildet sind, aus behördlicher Sicht ihrerseits potenziell interessant werden lassen. Man verdeutliche sich nur die Wege, die Schnappschüsse von einer zufällig mitabgebildeten Person über die Smartphone-Kamera der Fotografin, das Einstellen in einem sozialen Netzwerk und mehrfaches Teilen inklusive *Likes* und Kommentaren zurücklegen, wobei jede einzelne Station einen potenziellen Zugriffspunkt im Rahmen der Online-Durchsuchung des Geräts eines beliebigen Beteiligten darstellt – oder auch eines Unbeteiligten Dritten, in dessen *Newsfeed* ein Bild qua „Freundschaft" mit irgendeinem Beteiligten auftaucht.

Technisch ohne weiteres möglich ist es zudem, mittels eines nun ebenfalls rechtlich zulässigerweise einsetzbaren „*Keyloggers*" – man wird sich an die Diskussion um den sog. „Bundestrojaner" erinnern – die ggf. erforderlichen Passwörter auszuspähen, um ohne Kenntnis des Betroffenen dessen Social-Media-Kommunikation zu übernehmen. Das ist eine interessante neue Variante der verdeckten Ermittlung sowie des Einsatzes von *Agents Provocateurs*. Für Kommunikationspartner gibt es dabei – abgesehen vom Rückgriff auf klassische analoge Techniken wie den Einsatz von Sprachcodes o.ä. – praktisch keine Möglichkeit, festzustellen, mit wem sie wirklich kommunizieren.

3. Social Media: Disclose or abstain

Aus Sicht des „Normalnutzers" sozialer Medien zwingen ermittlungsbehördliche Befugnisse wie Online-Durchsuchung und Quellen-TKÜ demnach zu einer grundsätzlichen Entscheidung. Will man soziale Netzwerke ihrem Wesen entsprechend nutzen, schließt dies auch bei völlig gesetzestreuem Verhalten in gegenüber herkömmlichen Überwachungsmaßnahmen *außerhalb des virtuellen Raums* erheblich potenziertem Maß die Möglichkeit aus, eigene Inhalte und Daten einigermaßen sicher aus dem Fokus ermittlungsbehördlicher Aufmerksamkeit herauszuhalten. Während dies im Zusammenhang mit der Quellen-TKÜ auf Kommunikation im eigentlichen Sinne beschränkt ist, gilt es hinsichtlich der Online-Durchsuchung für jedes Social-Media-Verhalten, das vom Account eines von der Maßnahme betroffenen Beschuldigten aus sichtbar wird, also etwa in seinem Facebook-*Newsfeed* angezeigt wird. Selbst, wenn die strafrechtliche Verwertbarkeit von in diesem Zusammenhang erlangten Daten Dritter – also etwa mit dem Beschuldigten online verkehrender „Normalnutzer" – erheblichen Zweifeln unterliegt,[25] legt schon der mit ihrer Erfassung immer zwingend verbundene Eingriff in das Recht auf informationelle Selbstbestimmung nahe, dass dieses „Heraushalten" mit einem

22 *Graf*, in: BeckOK-StPO, § 100b Rn. 24.
23 *Soiné*, NStZ 2018, 497 (502).
24 *Schiemann*, KriPoZ 2018, 338 (342).
25 *Eschelbach*, in: SSW-StPO, § 100b Rn. 21.

schützenswerten Interesse verknüpft ist. Dass die dargestellten Begrenzungsmechanismen, mit denen der Gesetzgeber Online-Durchsuchung und Quellen-TKÜ ausgestattet hat, diesem Interesse nur unzureichend gerecht werden können, liegt in der Natur der Sache. Will man dies nicht in Kauf nehmen, steht man damit letzten Endes vor der Wahl, sein Nutzungsverhalten als identifizierbarer User in Netzwerken des Clear Web erheblich einzuschränken, dort ausschließlich unter Pseudonym zu verkehren – was etwa von Facebook bekanntlich nach Kräften unterbunden wird – oder auf andere Kommunikationsnetze auszuweichen, in denen es möglich ist, seine Identität geheim zu halten. In welchem Umfang Online-Durchsuchung und Quellen-TKÜ derzeit zum Einsatz kommen, hält das Bundeskriminalamt derweil unter Verschluss,[26] so dass sich Spekulationen über Häufigkeit und Intensität tatsächlicher Grundrechtseingriffe insoweit erübrigen. Soweit Antworten auf parlamentarische Anfragen, die lediglich Einsätze in abgeschlossenen Ermittlungsverfahren betreffen, darauf hindeuten, dass sich die Einsatzpraxis bislang in engen Grenzen hält,[27] ist dies eine Frage technischer Einsatzfähigkeit, die für die Untersuchung der Rechtsrealität zwar durchaus von Interesse ist. Die kritische Analyse der Reichweite geltender behördlicher Befugnisse indes tut gut daran, sich zu technischen Fragen in ein ebenso abstraktes Verhältnis zu setzen wie die – mit Blick auf den bekanntermaßen zügigen technischen Fortschritt durchaus geduldigen – Normen, die sie zum Gegenstand hat.

4. DSGVO und US C.L.O.U.D. Act

Nun ist die Strafprozessordnung nicht das einzige Gesetz, das in jüngster Zeit Änderungen erfahren hat, die für Nutzer sozialer Medien von potenzieller Relevanz sind. Seit Mai dieses Jahres gilt die europäische Datenschutz-Grundverordnung, bereits seit März der US-amerikanische *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act). Erstere trifft bezüglich der Weitergabe von Nutzerdaten durch Dienstleister an Ermittlungsbehörden keine Regelung, die hier von wesentlichem Interesse ist. Zentrale deutsche Regelungen im Zusammenhang mit Strafverfolgung sind insoweit § 23 Abs. 1 Nr. 4 BDSG und § 100a Abs. 4 StPO.[28] Der CLOUD Act dagegen ist aus Nutzersicht durchaus relevant, denn er verpflichtet US-amerikanische Unternehmen – und damit einen Großteil aller nennenswerten Anbieter sozialer Medien –, von ihnen gespeicherte Daten auf einfach-behördliche Anordnung auch dann an US-amerikanische Ermittlungsbehörden herauszugeben, wenn diese auf Servern außerhalb der USA gespeichert sind. Dies gilt explizit unabhängig vom Recht des jeweiligen Drittstaats und betrifft etwa, um nur ein Beispiel zu nennen, die Nutzerdaten aller europäischen Facebook-Nutzer, die bekanntlich auf irischen Servern liegen. Abzuwarten bleibt insoweit das Ergebnis des Konflikts zwischen dem CLOUD Act und der DSGVO, deren Art. 44 die Zulässigkeit der Weitergabe von Daten an Drittländer von der Prüfung des dortigen Datenschutzniveaus auf Vergleichbarkeit mit jenem der DSGVO durch die EU-Kommission abhängig macht. Ein Abkommen, das den dadurch entstehenden Konflikt von DSGVO und CLOUD Act auflöst, besteht zum jetzigen Zeitpunkt noch nicht. US-amerikanische Dienstleister stecken demnach insofern in der Zwickmühle, als sie sich gegebenenfalls entscheiden müssen, entweder gegen den CLOUD Act oder aber gerade durch dessen Befolgung gegen die DSGVO verstoßen zu müssen. Fest steht jedenfalls: Sämtliche aufgeworfenen Fragen und Probleme des „Normalnutzers", um den es hier geht, der von der StPO betroffen ist und sich zumindest überwiegend in Deutschland aufhält, erlangen durch den CLOUD Act eine erhebliche internationale Dimension, die dadurch noch verschärft wird, dass dieser Abkommen mit anderen Staaten vorsieht, die wechselseitigen Datenzugriff ermöglichen. Auch die Implikationen von DSGVO, CLOUD Act und möglicher E-Evidence-Richtlinie auf die strafrechtlichen Rechtshilfeabkommen zwischen den USA und Deutschland sowie der EU sind noch nicht einmal ansatzweise ausgelotet.

5. Konkret: Implikationen für verantwortliches Nutzungsverhalten

Um nach dem kurzen Rundgang durch StPO, CLOUD Act und DSGVO den Kreis zu schließen und vor der Beantwortung der Frage, ob angesichts des Ausmaßes ermittlungsbehördlicher Befugnisse eine „Flucht ins Darknet" als ernsthafte Alternative erscheinen muss, sollen die Implikationen für Grundlinien eines verantwortlichen Nutzungsverhaltens in sozialen Medien anhand konkreter dort gängiger Verhaltensweisen überprüft werden. Die wesentlichen drei Punkte sind dabei:

Zum Ersten ist es bei Nutzung sozialer Medien in einem Rahmen, der ihrer Natur entsprechend über die bloße Verlagerung ansonsten analog geführter Kommunikation in den virtuellen Raum hinausgeht, effektiv nicht möglich, sich vom Einzugsbereich ermittlungsbehördlicher Maßnahmen mit Sicherheit fernzuhalten.

Zum Zweiten umfasst das Spektrum dabei potenziell betroffener Inhalte dabei jedenfalls bei der Online-Durchsuchung sämtliche Vorgänge, die im Newsfeed eines Beschuldigten abgebildet werden.

Zum Dritten muss sich der Nutzer vorbehaltlich der weiteren Entwicklung im Verhältnis von DSGVO und CLOUD Act nicht nur mit deutschen Ermittlungsbehörden und herkömmlichen Rechtshilfeabkommen, sondern möglicherweise auch unmittelbar mit US-amerikanischen und – qua zu schließender Abkommen – diversen anderen Ermittlungsbehörden auseinandersetzen.

Nun kann man die Sichtbarkeit seiner Freundesliste auf

[26] https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html (zul. abgerufen am 12.12.2018). Dass die Zurückhaltung der Informationen mit dem Verweis begründet wird, es handele sich um einen „äußerst sensiblen Bereich der verdeckten strafprozessualen und polizeilichen Informationsgewinnung", ist einerseits nachvollziehbar, entbehrt andererseits mit Blick auf das angesichts der äußersten Sensibilität potenziell betroffener, grundrechtlich geschützter Bereiche gesteigerte bürgerliche Informationsinteresse indes nicht einer gewissen Ironie.

[27] Netzpolitik.org veröffentlicht Auskünfte der Bundesregierung auf Anfragen verschiedener Parteien, die die Häufigkeit des repressiven Einsatzes von Maßnahmen der Quellen-TKÜ bzw. Online-Durchsuchung *in bereits abgeschlossenen Verfahren* im einstelligen Bereich verorten (https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/#Antwort-Drucksache-19-2907-NfD – zul. abgerufen am 18.12.2018).

[28] Näher zu den Verpflichtungen der Telekommunikationsdienstleister im repressiven Kontext *Eschelbach*, in: SSW-StPO, § 100a Rn. 23.

„only me" stellen. Doch kann man nicht verhindern, dass man in der eigenen Kontrolle entzogenen Freundeslisten Dritter öffentlich sichtbar angezeigt wird. Man kann seine Posts nur „Freunden" zugänglich machen und die darüber hinaus gehende Öffentlichkeit ausschließen. Man kann die Sichtbarkeit sogenannter *tags* – Markierungen auf Fotos – begrenzen. Doch gilt all das nur für das eigene Profil. Dass man *getagged* wird, lässt sich präventiv nicht verhindern, sondern ist – jeweils im Einzelfall – nur im Nachhinein mit einigem Aufwand wieder zu beheben. Selbstverständlich kann man auch von vornherein überlegen, mit wem man sich auf Fotos zeigt, die früher oder später in sozialen Netzen landen könnten. Man kann die Kontrolle über seine Kontakte ernstnehmen und grundsätzlich überlegen, wie ratsam es im Einzelfall ist, Kontakt zu Personen zu knüpfen, die man im realen Leben nicht kennt. Mit der Kontrolle über die Freundesliste stehen und fallen diverse Möglichkeiten, sich durch Folgeeinstellungen weiter zu schützen. So kann man etwa die Aufnahme von Messenger-Kommunikation – Quellen-TKÜ! – oder die Einsicht *gelikeder* Pages und getätigter Posts – Online-Durchsuchung! – Freunden vorbehalten.

Solche Maßnahmen können das Risiko, unvermeidlich Mitbetroffener von Ermittlungsmaßnahmen in sozialen Medien zu werden, gewiss verringern. Im Ganzen bleibt es – wenig überraschend – dabei, dass es auszuschließen nur unter der Voraussetzung wäre, jederzeit und umfassend über alle potenziellen Aktivitäten i.S.d. §§ 100a Abs. 2, 100b Abs. 2 StPO aller Kontakte informiert zu sein. Das ist nicht nur schwerlich denkbar. Es ist auch kaum wünschenswert. Abschließend sei deshalb gefragt, ob eine „Flucht ins Darknet" als erwägenswerte Alternative in Betracht kommt.

6. Ausblick: „Flucht ins Darknet"?

Der als Darknet bekannte, also der dem Zugriff herkömmlicher Suchmaschinen entzogene, etwa mittels des Tor-Browsers anonymisiert zugängliche Bereich des Netzes ist dem Großteil gewöhnlicher deutscher Internetnutzer allenfalls ein vager Begriff und von eher gemäßigtem Interesse. Gelegentlich liest man von Erfolgen der Ermittlungsbehörden, die Plattformen für illegale Güter und Dienstleistungen stilllegen und ähnliches.[29] Davon bestimmt ist, was mit dem Begriff Darknet verbunden wird: Kriminalität, Drogen- und Waffenhandel, Auftragsmord und Kinderpornographie. Tatsächlich sind entsprechende Vorstellungen keinesfalls unbegründet. Man geht davon aus, dass knapp 60 Prozent der Aktivitäten im Darknet als kriminell einzustufen sind.[30] Nun ist ein Anteil von 60 Prozent zweifellos hoch und die damit einhergehenden Gefahren nicht zu unterschätzen. Gerade in Bezug auf den florierenden Onlinehandel mit Betäubungsmitteln erleichtert das Darknet insbesondere jungen Nutzerinnen und Nutzern den Zugang zu gesundheitsgefährdenden und –schädigenden Substanzen erheblich. Geschäfte mit Schusswaffen finden in quantitativ wesentlich geringerem Umfang statt. Qualitativ bergen auch diese nichtsdestoweniger erhebliches Gefahrenpotential. So nutzte bekanntermaßen etwa der Attentäter, der im Juli 2016 im Umfeld des Münchener Olympia-Einkaufszentrums neun Menschen tötete und schließlich sich selbst erschoss, das Darknet zur Beschaffung seiner Tatwaffe. Dennoch verbleiben daneben gut 40 Prozent an Inhalten, die allzu schnell aus dem Fokus geraten und in deren Rahmen die Möglichkeiten des Darknets zum Schutz vor staatlicher und sonstiger Überwachung durchaus Raum für anderweitige Nutzung bieten. Hier kommunizieren Journalisten mit anonymen Quellen, werden Whistleblower aktiv und vernetzen sich Menschen, die in autoritären Staaten leben und an politischer Veränderung – oder auch nur unzensierter und nicht überwachter Kommunikation oder der ungehinderten Nutzung sozialer Netze – interessiert sind. So war es das Darknet, das Aktivisten des sog. Arabischen Frühlings die Vernetzung untereinander ebenso wie das Unterhalten staatlich unabhängiger Informationsangebote ermöglichte, die sich auch an die weltweite Öffentlichkeit richteten. Besonders drastisch deutlich wird die essentielle Rolle des Darknets als Schnittstelle der Bereitstellung von Informationen durch auf den Schutz der Anonymität angewiesene Quellen und Multiplikatoren auch am Beispiel der Initative „*Raqqa is being slaughtered silently*", die selbst in der Hochphase des „Islamischen Staats" in Syrien aus dessen Herrschaftsgebiet berichtete. Zunehmend drängen auch Anbieter sozialer Netzwerke in diesen Bereich. So kooperiert etwa Facebook bereits seit einigen Jahren mit den Betreibern des Tor-Netzwerks und hält einen eigenen, für den Zugang über dasselbe optimierten *hidden service* bereit.[31]

Dass die Berührungspunkte von „Normalnutzern" mit dem Darknet hierzulande bei alldem überschaubar bleiben, deutet darauf hin, dass bei der Abwägung zwischen Chancen und Risiken des Darknets, anders als es in autoritären Staaten naheliegt, die den Zugang zu sozialen Netzwerken sperren oder der freien Meinungsbildung, Information und Kommunikation ihrer Bürger mittels rigider Überwachung und Zensur entgegenwirken, die Risiken des undurchsichtigeren Bereichs des Netzes noch stark ins Gewicht fallen. Hierzu zählt etwa das relativ hohe Risiko, im Darknet Opfer von Viren und *Keyloggern* zu werden. Tatsächlich kann zudem ein Anfangsverdacht auch bezüglich höchst delikater Straftaten schnell gegeben sein. Schon ungewollte Suchergebnisse, die in Form von *Thumbnails* (kleinen Bildchen) ausgeworfen und zumindest temporär auf dem Endgerät gespeichert werden, können unter Umständen ausreichen. Die bequeme und insofern absichernde Filterfunktion, die der eingeschränkte Einzugsbereich gewöhnlicher Suchmaschinen im Clear Web mit sich bringt, ist dem Darknet fremd. Jedenfalls, wer seinen Rechner dem Tor-Netzwerk als Ausgangsrelais zur Verfügung stellt, also zulässt, dass seine Adresse als letzte in der Reihe zur Verschleierung des Nutzungsverkehrs angewählter Stationen vor dem Zugriff auf den Zielinhalt fungiert, riskiert auch, zumindest vorübergehend als Verdächtiger für strafbares Tun Dritter zu

[29] Ein prominentes Beispiel ist der Schlag des FBI gegen *Silkroad* 2013, s. https://www.golem.de/news/silk-road-drogenhandel-abgeschaltet-1310-101947.html (zul. abgerufen am 23.10.2018).

[30] So zitiert etwa die Bundeszentrale für politische Bildung (*Tzanetakis*) zwei britische Studien, die ca. 50 bzw. 57 Prozent der Inhalte des Tor-Netzwerks als (nach dortigem Maßstab) strafrechtlich relevant einstufen: http://www.bpb.de/apuz/259147/drogenhandel-im-darknet (zul. abgerufen am 12.12.2018).

[31] Zugänglich per Tor-Browser unter facebookcorewwwi.onion.

erscheinen. Abgesehen davon aber, dass auch das Clear Web von Kriminalität bekanntlich nicht gerade frei ist, verhält es sich mit dem virtuellen Raum letztlich wohl nur unwesentlich anders als mit dem tatsächlichen Leben. Der „Normalbürger" hat eine Vorstellung von der Kriminalitätsbelastung bestimmter Gegenden und weiß, dass es stärker und weniger stark belastete Gebiete gibt. Daran orientiert er seine Bewegungsmuster. Weiß man, dass es potenziell gefährlich ist, zu einer bestimmten Uhrzeit durch eine bestimmte *dunkle* Straße zu laufen, wird man im Zweifel darauf verzichten. Wenn knapp 60 Prozent aller Aktivitäten im Darknet als kriminell eingestuft werden, ist das einerseits ein veritabler Grund, diese „Gegend" des Internets zu meiden (und sei es nur, um sich keine Viren zu fangen etc.). Nehmen auf der anderen Seite die Möglichkeiten ab, sich in offeneren, helleren Straßen unbehelligt zu bewegen, kommt irgendwann der Punkt, an dem die Abwägung auch den „Normalbürger" in die dunkle Straße führt. Die Ausweitung des ermittlungsbehördlichen Überwachungspotenzials durch Befugnisse wie Online-Durchsuchung und Quellen-TKÜ ist – bei allem Verständnis für die Bedürfnisse der Strafverfolgungsbehörden – ein Schritt in diese Richtung. Abseits dessen, was wir im Alltag über das Darknet hören, ist aber von einzelnen Ermittlungsbehörden zu erfahren, dass der auch insofern präventiv repressiv agierende Staat diesen Schritt anders als der Großteil seiner Bürger bereits zu machen im Begriff ist. Wie effizient die hier aufgezeigten Maßnahmen im Darknet einsetzbar sein werden, ist derzeit noch nicht abschätzbar. Sollte die Effektivität sich aber als eingeschränkt erweisen, so darf man in Fortschreibung der Kriminalpolitik der letzten Regierung davon ausgehen, dass einmal mehr die Sicherheit der Bürger bemüht werden wird, um noch deutlich weiterreichende Ermittlungseingriffe zu fordern.