Surfen im Internet und Cloud Computing zwischen Telekommunikationsüberwachung und Online-Durchsuchung

Von Prof. Dr. **Manfred Heinrich**, Kiel

I. Neben den höchst zahlreich in der StPO geregelten Ermächtigungen zu „offenen" Eingriffen, wie insbesondere zu vorläufiger Festnahme (§§ 127 ff. StPO) und Untersuchungshaft (§§ 112 ff. StPO),[1] aber auch zu nicht freiheitsentziehenden Maßnahmen wie körperliche Untersuchung (§ 81a StPO), Durchsuchung (§§ 102 ff. StPO) und Beschlagnahme (§§ 94 ff. StPO),[2] steht den Strafverfolgungsbehörden mittlerweile auch ein ganzes Arsenal von Möglichkeiten zur Verfügung, „verdeckt" zu ermitteln:[3] von der Rasterfahndung (§ 98a StPO) bis zum Einsatz Verdeckter Ermittler (§ 110a StPO), von der Postbeschlagnahme (§ 99 StPO) bis zur Telekommunikationsüberwachung (§ 100a StPO), von der längerfristigen Observation (§ 163 f. StPO) über die Ausschreibung zur Beobachtung bei polizeilichen Kontrollen (§ 163e StPO) bis hin zur akustischen Wohnraumüberwachung (§ 100c StPO).

Gerade im Bereich des mittlerweile immer stärker in den Fokus auch der Ermittlungsbehörden gelangten Internetgeschehens hat der Gesetzgeber in den letzten Jahren zahlreiche spezifische Eingriffsnormen geschaffen, mit deren Hilfe es möglich ist, auf nahezu jedem nur erdenklichen Weg auch in der digitalen Welt effizient zu ermitteln. Die passgenauen Regeln etwa zur Bestandsdatenauskunft (§ 100j StPO), zur Erhebung von Verkehrsdaten (§ 100g StPO), zur Lokalisierung von Mobilfunkendgeräten (§ 100i StPO) und letztens auch zur Quellen-TKÜ (§ 100a Abs. 1 S. 2, 3 StPO) sowie zur Online-Durchsuchung (§ 100b StPO) scheinen kaum mehr nennenswerte Lücken im einschlägigen Regelungskonzept unserer StPO zu belassen.

Bei genauerem Hinsehen ist dem jedoch keineswegs so, und zwar gerade auch im Hinblick auf ganz grundlegende Verhaltensweisen des heutigen Internetnutzers. So ist es noch längst nicht ausdiskutiert, ob bzw. inwieweit und unter Heranziehung welcher Eingriffsnormen man auf das wohl als Regelverhalten aller Internet-Nutzer anzusprechende „Surfen im Internet" strafverfolgerischen Zugriff nehmen darf;[4] und nichts anderes gilt auch für das zwar noch nicht ubiquitär anzutreffende, aber doch in immer weiter zunehmendem Maße genutzte sog. Cloud Computing[5] – was letztlich nichts anderes meint, als die Möglichkeit, sowohl Daten wie auch ganze Datenverarbeitungsprozesse auf im Netz für diese Zwecke verfügbar gestellte fremde Server auszulagern.[6]

Nun ist es durchaus nachvollziehbar, dass die Strafverfolgungsbehörden ein gehobenes Interesse daran haben, im Rahmen ihrer Ermittlungstätigkeit ggf. auch in diesen soeben benannten Richtungen hin tätig zu werden.[7] Dabei ist aus dem Instrumentarium der StPO heraus an eben die beiden im Titel dieses Beitrags erwähnten Eingriffsermächtigungen zu denken: zum einen die Telekommunikationsüberwachung des § 100a StPO (TKÜ)[8] und zum anderen die Online-Durchsuchung des § 100b StPO[9]. Ihrem Wesen nach unterscheiden sich die beiden Maßnahmen ganz grundlegend darin, dass die TKÜ sich mit dem Auslesen bzw. Ausleiten der Inhalte aktuellen Kommunikationsgeschehens beschäftigt,[10] die Online-Durchsuchung hingegen Zugriff zu nehmen gestattet auf die gesamten im betreffenden Informationsverarbeitungssystem anzutreffenden Inhalte, gleichgültig, ob diese sich schon lange auf den Speichermedien des Systems befinden oder gerade „frisch hereingekommen" sind.[11]

---

[1] Näher hierzu *Heinrich*, in: Krey/Heinrich, Deutsches Strafverfahrensrecht, 2. Aufl. 2019, Rn. 718 ff., 773 ff.

[2] Eingehend auch zu diesen *Heinrich* (Fn. 1), Rn. 798 ff.

[3] Vgl. *Heinrich* (Fn. 1), Rn. 856 ff. mit Überblick in Rn. 857 f.

[4] Für eine Anwendbarkeit des § 100a StPO bspw. *Bruns*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl. 2019, § 100a Rn. 4; dagegen u.a. *Wolter/Greco*, in: Wolter (Hrsg.), Systematischer Kommentar zur Strafprozessordnung, Bd. 2, 5. Aufl. 2016, § 100a Rn. 31a m.w.N.; für eine Anwendbarkeit des § 100b StPO etwa *Eschelbach*, in: Satzger/Schluckebier/Widmaier (Hrsg.), Strafprozessordnung, 3. Aufl. 2018, § 100a Rn. 5.

[5] Wie Fn. 4; siehe auch *Hauck*, in: Becker/Erb/Esser/Graalmann-Scheerer/Hilger/Ignor, Löwe-Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Großkommentar, Bd. 3/1, 27. Aufl. 2019, § 100a Rn. 85.

[6] Ausführlich zum Begriff „Cloud Computing" *Hiéramente/Fenina*, StraFo 2015, 365 (366 f.); näher noch unten, IV. 1.

[7] Vgl. speziell zum Cloud Computing *Gähler*, HRRS 2016, 340 (341): „Ein Zugriff auf all diese Daten ist aus Perspektive der Ermittlungsbehörden selbstredend von großem Interesse."; siehe auch *Hiéramente/Fenina*, StraFo 2015, 365 (367): „Grundsätzlich haben die Ermittlungsbehörden aus ermittlungstaktischen Gründen ein Interesse, weitgehenden und zeitnahen Zugriff auf die Daten zu erlangen."

[8] Ausführlich hierzu *Heinrich* (Fn. 1), Rn. 871 ff.

[9] Ausführlich hierzu *Heinrich* (Fn. 1), Rn. 914 ff.

[10] Vgl. nur *Bruns* (Fn. 4), § 100a Rn. 5: „regelt § 100a nur den Eingriff in den technischen Vorgang der Nachrichtenübermittlung, also vom Absenden der Signale bis zu deren Empfang beim Adressaten"; siehe auch *Eschelbach* (Fn. 4), § 100a Rn. 2: „Überwachung und Aufzeichnung von laufender Kommunikation".

[11] Vgl. wiederum *Bruns* (Fn. 4), § 100a Rn. 6, insoweit klar von laufenden Übertragungsvorgängen abgrenzend: Es seien „die auf der Festplatte […] gespeicherten empfangenen Daten […] nicht von § 100a erfasst", der Zugriff auf die „angekommenen" Daten erfolge vielmehr „unter den besonderen Voraussetzungen der Online-Durchsuchung nach § 100b"; in diesem Sinne auch *Knierim/Oehmichen*, in: Knierim/Oehmichen/Beck/Geisler, Gesamtes Strafrecht aktuell, 2018, Kap. 20 Rn. 27; siehe auch *Eschelbach* (Fn. 4), § 100b Rn. 1: Auslesen von „Informationen, die auf dem informationstechnischen System *gespeichert* sind" (*Hervorhebung* auch im Original).

II. Beginnen wir mit der TKÜ: Diese in § 100a StPO sehr detailliert geregelte Maßnahme[12] erlaubt unter vergleichsweise strengen Voraussetzungen[13] die Überwachung und Aufzeichnung von „Telekommunikation". Und damit stellt sich bereits die erste in unserem Zusammenhang kernrelevante Frage: Erfasst der in § 100a StPO zugrunde zu legende „Telekommunikations"-Begriff überhaupt auch den *einseitigen Datenabruf*, wie er namentlich beim bloßen Surfen im Internet, im Falle der Internetrecherche oder auch beim Cloud Computing zu verzeichnen ist? Hier scheiden sich die Geister, sind doch mindestens drei verschiedene Ausdehnungen für diesen Begriff (und damit den Anwendungsbereich der TKÜ) im Gespräch:

Der weiteste Begriff von Telekommunikation ist derjenige des § 3 Nr. 22 Telekommunikationsgesetz (TKG), in welchem er definiert wird als „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen".[14] Danach wären auch die Übertragungsvorgänge beim Internetsurfen und dem Cloud Computing ohne Weiteres „Telekommunikation".[15]

Nun besteht aber weitestgehend Einigkeit darüber, dass diese einzig am technischen Aspekt des Telekommunikationsgeschehens ausgerichtete Sicht dem Schutzzweck des § 100a StPO nicht gerecht wird,[16] nachdem dieser doch die Grenzen zulässigen Eingriffs in das Fernmeldegeheimnis des Art. 10 GG festlegen will.[17] Mit der seinerzeit[18] erfolgten Umformulierung der ehemaligen „Überwachung des Fernmeldeverkehrs" in die heutige „Telekommunikationsüberwachung" sollte zwar der technischen Entwicklung Rechnung getragen werden.[19] Nicht aber ging es darum, den an Art. 10 GG ausgerichteten Schutzbereich der Eingriffsnorm zu verändern:[20] Nach wie vor sollteEreignisraum der ggf. über. § 100a StPO zu rechtfertigenden Eingriffe der Bereich menschlichen Kommunizierens sein,[21] nicht aber auch den – vom technikorientierten § 3 Nr. 22 TKG ebenfalls erfassten – „‚blinden' Austausch von Informationen zwischen Maschinen"[22] umgreifen.[23] Nach allgemeiner Auffassung fallen daher aufgrund ihrer automatischen Generierung – und als damit von vornherein außerhalb des Schutzbereichs des Art. 10 GG stehend – weder die Positionsmeldungen eines Mobilfunkendgerätes unter „Telekommunikation" i.S.d. § 100a StPO,[24] noch die im Zuge der Mauterfassung auf deutschen Autobahnen erhobenen und weitergeleiteten Daten.[25]

Angesichts dessen stellt sich nun die Frage, ob denn nicht auch die hier zu behandelnden Formen des einseitigen Datenabrufs diesem Verdikt unterfallen. Dies wird im Schrifttum vielfach angenommen,[26] weil es sich bei der im Internetsur-

[12] Ausführlich zu ihr *Heinrich* (Fn. 1), Rn. 871 ff.

[13] Vgl. im Einzelnen *Heinrich* (Fn. 1), Rn. 880 ff.

[14] Wobei gemäß § 3 Nr. 23 TKG unter „Telekommunikationsanlagen" zu verstehen sind: „Technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können".

[15] So denn etwa auch *Bruns* (Fn. 4), § 100a Rn. 4; siehe auch *Hauck* (Fn. 5), § 100a Rn. 31.

[16] Vgl. nur *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung, 63. Aufl. 2020, § 100a Rn. 6, sowie BVerfG NJW 2016, 3508 (3509), Rn. 32: „Die nähere Auslegung des Begriffs ‚Telekommunikation' im Rahmen des § 100a StPO muss sich […] insbesondere auch an dem grundrechtlichen Schutz des Betroffenen durch Art. 10 GG orientieren […]. Dabei ist […] zu berücksichtigen, dass Art. 10 I GG nicht dem rein technischen Telekommunikationsbegriff des Telekommunikationsgesetzes folgt."; siehe auch *Wolter/Greco* (Fn. 4), § 100a Rn. 31a: „Der Telekommunikationsbegriff von Art. 10 GG deckt sich nicht mit dem entsprechenden Begriff aus dem Telekommunikationsgesetz."

[17] BVerfG NJW 2016, 3508 (3509), Rn. 32: „denn das Fernmeldegeheimnis ist der verfassungsrechtliche Maßstab für die heimliche Überwachung flüchtiger Daten".

[18] Durch Art. 2 Abs. 9 Nr. 2 des Gesetzes v. 17.12.1997, BGBl. I 1997, S. 3108.

[19] So ist es denn dank ebendieser technischen Entwicklungsoffenheit des § 100a StPO mittlerweile auch „selbstverständlich und weitestgehend unstreitig, dass SMS, E-Mails, Chatnachrichten, Internettelefonie mittels einer Telekommunikationsüberwachung überwacht werden dürfen." (*Hiéramente/Fenina*, StraFo 2015, 365 [370]).

[20] *Hiéramente/Fenina*, StraFo 2015, 365 (370): „Der Wechsel des Kommunikationsmediums führt zwar zu technischem Anpassungsbedarf, ändert aber die Zielrichtung des § 100a StPO nicht wesentlich."

[21] In diesem Sinne zu Recht auch BGH NStZ 2018, 611 (612); siehe auch *Köhler* (Fn. 16), § 100a Rn. 6: „geht es bei § 100a um die Erfassung kommunikativen Sozialverhaltens"; *Roxin/Schünemann*, Strafverfahrensrecht, 29. Aufl. 2017, § 36 Rn. 4: „Telekommunikation setzt das Vorhandensein eines menschlichen Kommunikationspartners voraus."

[22] So die Formulierung bei *Wolter/Greco* (Fn. 4), § 100a Rn. 14; siehe auch BGH NStZ 2018, 611 (612): „lediglich ein Datenaustausch zwischen technischen Geräten".

[23] BVerfG NJW 2007, 351 (353 f.); BGH NStZ 2018, 611 (612); *Wolter/Greco* (Fn. 4), § 100a Rn. 14; *Köhler* (Fn. 16), § 100a Rn. 6; siehe auch *Roxin/Schünemann* (Fn. 21), § 36 Rn. 4: „Werden Informationen von Anlage zu Anlage automatisch übermittelt, geht es noch nicht um Kommunikation."; *Hauck* (Fn. 5), § 100a Rn. 29 verlangt, „dass eine Person mittels dieser Technik Kommunikation betreibt".

[24] Vgl. BVerfG NJW 2007, 351 (353 f., zum Einsatz eines „IMSI-Catchers"), sowie BGH NStZ 2018, 611 (612, zum Versenden sog. „stiller SMS"); ebenso *Roxin/Schünemann* (Fn. 21), § 36 Rn. 4; *Wolter/Greco* (Fn. 4), § 100a Rn. 21; *Köhler* (Fn. 16), § 100a Rn. 6a; *Hauck* (Fn. 5), § 100a Rn. 68 (näher zur Technik a.a.O., Rn. 65).

[25] *Niehaus*, NZV 2004, 502 f.; *Köhler* (Fn. 16), § 100g Rn. 10; siehe auch *Knierim/Oehmichen* (Rn. 11), Kap. 20 Rn. 22; a.A. LG Magdeburg NJW 2006, 1073 (1074).

[26] Vgl. nur *Eschelbach* (Fn. 4), § 100a Rn. 5; *Köhler* (Fn. 16), § 100a Rn. 6, 14f.; *Roxin/Schünemann* (Fn. 21), § 36 Rn. 5; *Wolter/Greco* (Fn. 4), § 100a Rn. 31a m.w.N;

fen und beim Cloud Computing vonstattengehenden „einseitigen Nutzung informationstechnischer Systeme ohne sozialen Informationsaustausch“ um „keine vertrauliche ‚Kommunikation‘“ im Sinne des § 100a StPO handele.[27] Dem möchte ich hier gerne beipflichten.

Was gerade das Surfen im Internet anlangt, ist es doch tatsächlich so, dass im Internet Informationen lediglich für eine unbestimmte Zahl noch unbekannter Empfänger bereitgestellt werden, welche von diesen dann aus eigener Initiative heraus abgerufen werden können;[28] *wer* das dann aber im Zuge seiner Internetnutzung *wann* und *wo* und *in welchem Umfang* tut, ist nicht vorauszusehen.[29] Dieses letztlich *ungezielte* Ineinandergreifen von Informationsangebot und Informationsinanspruchnahme durch zwei in keiner Weise miteinander auch nur im Entferntesten verbundene Personen als individualisierte Kommunikation in einem sich in § 100a StPO widerspiegelnden materiellen Sinne aufzufassen,[30] will mir nicht so recht gelingen.[31]

Dies gilt insbesondere auch mit Blick darauf, dass bei der ehemaligen Überwachung des Fernmeldeverkehrs (landläufig: der früheren *Telefon*überwachung) angesichts damals noch begrenzter technischer Möglichkeiten gerade und nur an den kommunikativen Austausch zwischen zwei Personen gedacht worden war (eben den Beteiligten an einem Telefonat) und die Ausgestaltung des § 100a StPO sich an gerade dieser Grundkonstellation orientierte[32] – unter Abwägung der aus ihr erwachsenden gegenläufigen Interessen zwischen Persönlichkeitsschutz und Strafverfolgungsinteressen.[33] Gerade darauf hin, jene klassische zweiseitige Kommunikation angemessen zu erfassen, war § 100a StPO a.F. bei seiner Schaffung ausgelegt worden.[34]

Und auch beim Umbau der Vorschrift anlässlich des Wechsels von der Telefon- hin zur Telekommunikationsüberwachung[35] sollte an dieser Grundjustierung nicht gerüttelt werden,[36] wurden jedenfalls keine gesetzgeberischen Gedanken darauf verwendet, neben der altbekannten zweiseitigen Kommunikation nunmehr auch etwaige Formen einseitiger Kommunikation mit ins Boot zu nehmen, sprich: einen in diesem Sinne erweiterten Anwendungsbereich in die Neugestaltung des § 100a StPO mit einfließen zu lassen.[37] Anders gesagt: Es haben sich zwar neue Formen im weiteren Sinne kommunikativen Geschehens entwickelt, § 100a StPO ist aber bis heute (mangels entsprechend ausgerichteter Umgestaltung) von seinem Regelungspotential noch immer allein auf die herkömmliche zweiseitige Kommunikation hin ausgerichtet.[38] Angesichts des niemals vorgenommenen entsprechenden Umbaus ist er auch gar nicht in der Lage, in einer den Besonderheiten einseitiger Kommunikation gerecht werdenden Weise über den tradierten Anwendungsbereich hinaus sachgerechte Ergebnisse zu liefern.[39]

Dem hält das BVerfG allerdings entgegen:[40] „Bei der Nutzung des Internets durch eine natürliche Person kommunizieren […] nicht ausschließlich technische Geräte miteinander […]. Vielmehr ist das für die Auslösung des Art. 10 GG notwendige spezifische Gefährdungspotenzial für die

siehe auch *Hiéramente/Fenina*, StraFo 2015, 365 (370): „Der Telekommunikationsbegriff der StPO setzt eine soziale Dimension voraus.“ – Dagegen jedoch *Bär*, in: v. Heintschel-Heinegg/Stöckel (Hrsg.), KMR, Kommentar zur Strafprozeßordnung, 70. Lfg., Stand: November 2013, § 100a Rn. 11a: „Der Telekommunikationsbegriff ist nicht auf eine Kommunikation zwischen Personen begrenzt.“; in diesem Sinne auch *Bruns* (Fn. 4), § 100a Rn. 4; *Hauck* (Fn. 5), § 100a Rn. 31.

[27] So speziell zum Internetsurfen *Wolter/Greco* (Fn. 4), § 100a Rn. 31a m.w.N.: „Bei § 100a müssen Sender und Empfänger natürliche Personen sein.“; entsprechend *Hiéramente/Fenina*, StraFo 2015, 365 (372) zum Cloud Computing: „Wer eine virtuelle Festplatte nutzt, Rechenleistung in der Cloud abruft oder dort Programme/Apps zur Datenverarbeitung verwendet, kommuniziert nicht im Sinne des § 100a StPO.“; siehe auch *Köhler* (Fn. 16), § 100a Rn. 6: Es gehe „bei § 100a um die Erfassung kommunikativen Sozialverhaltens“.

[28] So ganz richtig *Eidam*, NJW 2016, 3511 (3512).

[29] *Eidam*, NJW 2016, 3511 (3512).

[30] Explizit dagegen zu Recht *Eidam*, NJW 2016, 3511 (3512).

[31] In diesem Sinne auch *Wolter/Greco* (Fn. 4), § 100a Rn. 31a m.w.N.: „Bei der Lektüre einer Online-Zeitung oder dem Betrachten eines Livestreams oder gar von Internetfernsehen kann schwerlich von Telekommunikation die Rede sein“.

[32] Ganz richtig *Hiéramente/Fenina*, StraFo 2015, 365 (370): „Hinsichtlich der Intention des Gesetzgebers der Ursprungsfassung des § 100a StPO kann aufgrund der limitierten Fähigkeiten des analogen Telefonanschlusses […] mit hinreichender Wahrscheinlichkeit angenommen werden, dass ein sozialer Kommunikationsbegriff zugrunde gelegt wurde. Das heutige Multifunktionsgerät war schließlich nicht einmal in Sichtweite.“

[33] Näher und treffend hierzu *Hiéramente/Fenina*, StraFo 2015, 365 (369 f.).

[34] Vgl. *Hiéramente/Fenina*, StraFo 2015, 365 (369): „Einleuchten dürfte, dass die ursprüngliche Intention des § 100a StPO das Abhören von ‚Ganovengesprächen‘ gewesen ist.“

[35] Vgl. bereits oben bei und in Fn. 18.

[36] So denn auch BVerfG NJW 2016, 3508 (3509): „Der Begriff ‚Telekommunikation‘ […] setzt das ‚Fernmeldewesen‘ fort und wird nach wie vor in Anlehnung an die Definition dieses verfassungsterminologischen Vorläufers bestimmt“.

[37] Vgl. nur die einschlägige Gesetzesbegründung in BR-Drucksache 369/97, S. 27 ff., 45 f.

[38] So entspricht es denn auch durchaus der immer wieder erwähnten „technischen Entwicklungsoffenheit“ des § 100a StPO und ist es von daher „selbstverständlich und weitgehend unstreitig, dass SMS, E-Mails, Chatnachrichten, Internettelefonie mittels einer Telekommunikationsüberwachung überwacht werden dürfen“ (*Hiéramente/Fenina*, StraFo 2015, 365 [370]).

[39] Nach (zutreffender) Auffassung von *Hiéramente*, HRRS 2016, 448 (452), ist „die Überwachung der Internetnutzung […] ein Grundrechtseingriff eigener Art“, der „aufgrund der gesteigerten Eingriffsintensität eine eigenständige strafprozessuale Grundlage“ erfordert.

[40] BVerfG NJW 2016, 3508 (3510); explizit dagegen *Eschelbach* (Fn. 4), § 100a Rn. 5 m.w.N.

Privatheit der Kommunikation vorhanden, da […] willensgesteuert auf konkrete Kommunikationsinhalte zugegriffen wird. Auch das ‚Surfen' im Internet ist unter das Fernmeldegeheimnis zu subsumieren."

Nun ist dies freilich nur auf den ersten Blick ein Plädoyer für einen entsprechend weiten Anwendungsbereich des § 100a StPO.[41] Denn es mag ja sein und es soll hier auch gar nicht bestritten werden,[42] dass auch die „einseitige Nutzung informationstechnischer Systeme ohne sozialen Informationsaustausch"[43] in den Schutzbereich des Art. 10 GG fällt[44] – doch mehr hat das BVerfG auch gar nicht gesagt.[45] Insbesondere hat es aus seiner Aussage *nicht* den Schluss gezogen, aufgrund der Subsumierbarkeit unter das Fernmeldegeheimnis sei auch bereits per se und ohne Weiteres der Anwendungsbereich des – wie ich meine: dazu weder gedachten, noch geeigneten – § 100a StPO eröffnet.[46] Letztlich ging es dem Gericht vielmehr darum herauszuarbeiten, dass ein extensives Verständnis des § 100a StPO immerhin insofern verfassungskonform sei, als es mit dem in Art. 10 GG ausgelobten Schutz des Fernmeldegeheimnisses im Einklang stehe.[47] Wo also das Auslesen der Positionsmeldungen eines Mobiltelefons schon mangels überhaupt eines Bezugs zum Fernmeldegeheimnis aus der Anwendbarkeit des § 100a StPO herausfalle,[48] lasse sich dies im Hinblick auf Vorgänge des einseitigen Datenabrufs aufgrund ihrer Grundrechtsrelevanz nicht behaupten.[49]

Das war es dann aber auch, mehr Bindendes zur Anwendbarkeit des § 100a StPO ist aus den Ausführungen des BVerfG nicht herauszulesen.[50] So hebt denn auch das Gericht selbst ausdrücklich noch einmal den eingeschränkten verfassungsrechtlichen Prüfungsmaßstab hervor:[51] „Ein etwaiger Fehler der Fachgerichte muss gerade in der Nichtbeachtung von Grundrechten liegen. […] Nach diesem Maßstab ist die angegriffene Entscheidung des Landgerichts Ellwangen von Verfassungs wegen nicht zu beanstanden."[52] Nicht mehr und nicht weniger ist also mit der Feststellung des BVerfG im Hinblick auf die vom Landgericht Ellwangen befürwortete Erstreckung des § 100a StPO auch auf bloßes Surfen im Internet zum Ausdruck gebracht.[53] Ob nun aber § 100a StPO in eben dieser weiten Form nicht nur – aus verfassungsrechtlicher Sicht – angewendet werden dürfe, sondern vielleicht ja (aus welchen Gründen auch immer) sogar müsse, sei – so zu Recht das BVerfG[54] – eine Frage, die allein die Fachgerichte zu entscheiden hätten.

III. Somit ist die Frage der Erstreckbarkeit des § 100a StPO auch auf Internetsurfen und Cloud Computing letztlich aus einer wertenden Betrachtung des dem § 100a StPO einfachgesetzlich innewohnenden Regelungszwecks heraus zu beantworten – im Bewusstsein dessen, dass zwar die Eingriffsregelung des § 100a StPO sich im Rahmen des durch Art. 10 GG eröffneten Schutzbereichs bewegen muss, nicht aber angesichts jenes Schutzbereichs jede innerhalb seiner Umgrenzung stattfindende Ermittlungsmaßnahme auch von der Ermächtigungsnorm des § 100a StPO erfasst zu sein braucht.[55] Vielleicht, so der Gedanke, handelt es sich ja bei der strafverfolgerischen Überwachung des Internetsurfens oder Cloud Computings um Maßnahmen, die zwar in das

[41] In jenem (missverstandenen) Sinne etwa *Beulke/Swoboda*, Strafprozessrecht, 14. Aufl. 2018, Rn. 253a: „Auch das Surfverhalten […] unterfällt bei einer weiten Auslegung des Begriffs der Telekommunikation, wie sie vom BVerfG bestätigt wurde, dem Anwendungsbereich des § 100a StPO."

[42] Anders jedoch *Eschelbach* (Fn. 4), § 100a Rn. 5.

[43] So die Formulierung bei *Eschelbach* (Fn. 4), § 100a Rn. 5.

[44] Insofern durchaus überzeugend *Gähler*, HRRS 2016, 340 (343), speziell zum Cloud Computing.

[45] In diesem Sinne auch *Hiéramente*, HRRS 2016, 448 (449): „Eine umfassende Antwort haben die Karlsruher Richter vermieden."

[46] So aber (freilich noch vor der Entscheidung des BVerfG) *Bär* (Fn. 26), § 100a Rn. 11a; dies kritisierend sprechen *Hiéramente/Fenina*, StraFo 2015, 365 (371), ganz richtig von dem „fragwürdige[n] Umkehrschluss von der Interpretation des Art. 10 GG auf die Interpretation des § 100a StPO"; und auch *Wolter/Greco* (Fn. 4), § 100a Rn. 13, betonen, dass „der häufig anzutreffende Schluss von der Betroffenheit des Schutzbereichs von Art. 10 I GG auf die Anwendung von § 100a nicht richtig ist."; siehe auch unten, Fn. 55.

[47] In diesem Sinne auch *Hiéramente*, HRRS 2016, 448 (449).

[48] Hierzu BVerfG NJW 2007, 351 (353 f.), zum Einsatz eines „IMSI-Catchers".

[49] Vgl. BVerfG NJW 2016, 3508 (3510): „Bei der Nutzung des Internets durch eine natürliche Person kommunizieren […] nicht ausschließlich technische Geräte miteinander".

[50] Ganz richtig *Hiéramente*, HRRS 2016, 448 (449): „Auch wenn eine gewisse Tendenz für eine extensive Interpretation der staatsanwaltschaftlichen Ermittlungsbefugnisse zu erkennen ist, zieht sich der 2. Senat des Gerichts auf die grundlegende Feststellung zurück, dass die Entscheidung des Landgerichts Ellwangen aus verfassungsrechtlichen Gründen nicht in Zweifel zu ziehen sei."

[51] So auch der Hinweis bei *Hiéramente*, HRRS 2016, 448 (449).

[52] BVerfG NJW 2016, 3508.

[53] BVerfG NJW 2016, 3508 (3510): „Somit steht auch der Bedeutungsgehalt des Art. 10 I GG der vom LG vorgenommenen Auslegung des § 100a StPO nicht entgegen".

[54] Vgl. BVerfG NJW 2016, 3508: Es sei zu beachten, „dass die Auslegung und Anwendung von Strafprozessrecht Sache der dafür allgemein zuständigen Gerichte und einer Nachprüfung durch das BVerfG grundsätzlich entzogen ist, soweit bei der zu treffenden Entscheidung nicht Willkür vorliegt oder spezifisches Verfassungsrecht verletzt wird".

[55] So konstatiert denn auch *Gähler*, HRRS 2016, 340 (343), zu Recht, es sei „anerkannt, dass allein von der Eröffnung des Schutzbereichs des Art. 10 Abs. 1 Var. 3 GG nicht auf Vorliegen einer ‚Telekommunikation' i.S.d. §§ 100a ff. StPO geschlossen werden kann."; vgl. nur *Wolter/Greco* (Fn. 4), § 100a Rn. 13 m.w.N; siehe auch BVerfG NJW 2009, 2431 (2433), sowie bereits oben, Fn. 46.

Grundrecht aus Art. 10 GG eingreifen, nicht aber durch § 100a StPO legitimiert sind.[56]

Dass diese Möglichkeit besteht,[57] wird gerade auch in den literarischen Stellungnahmen zur Problematik zumeist nicht beachtet. Stattdessen wird zum Ausdruck gebracht, dass doch auch die einseitige Datennutzung im Internet dem Schutzbereich des Art. 10 GG unterfalle (was ja durchaus zutreffen mag) und deswegen gerade aus Schutzzwecküberlegungen heraus § 100a StPO anwendbar sein müsse,[58] um derartige Ermittlungsmaßnahmen den (wie schon erwähnt) doch vergleichsweise strengen Voraussetzungen dieser Eingriffsnorm zu unterwerfen.[59]

Was dabei freilich übersehen wird, ist, dass mit einer dergestalt motivierten – vermeintlichen – Ausweitung des grundrechtlichen Schutzes man eben diesem einen Bärendienst erweist:[60] Erfasst man nämlich die einseitige Internetnutzung über § 100a StPO, ist damit nicht nur eine Anbindung an die (nochmals: vergleichsweise strengen) Eingriffsvoraussetzungen der TKÜ verbunden,[61] sondern wird damit eine legale Zugriffsmöglichkeit überhaupt erst geschaffen:[62] Denn wie jeder andere Grundrechtseingriff auch, bedarf auch der Zugriff auf die Formen einseitiger Internetnutzung einer gesetzlichen Eingriffsgrundlage, die erst über die Anwendung des § 100a StPO auf diese Fälle verfügbar wird, die hingegen bei Ablehnung einer solchen Anwendbarkeit schlicht nicht vorhanden wäre: Eine analoge Anwendung des § 100a StPO stünde, da mittels Analogie begründete Eingriffsermächtigungen im Strafverfahrensrecht per se nicht zulässig sind,[63] ebenso wenig zur Debatte, wie die Möglichkeit, entsprechende Zugriffe auf die Ermittlungsgeneralklauseln der § 161 Abs. 1 S. 1 StPO und § 163 Abs. 1 S. 2 StPO zu stützen.[64] Denn diese können nach allgemeiner – und richtiger – Auffassung nur herangezogen werden für Ermittlungsmaßnahmen, die entweder *nicht* in Grundrechte eingreifen oder bei denen allenfalls von einem geringfügigen, weniger intensiven Eingriff gesprochen werden kann[65] – wovon bei der Überwachung von Internetsurfen und Cloud Computing bei Weitem nicht die Rede sein kann.[66] Zurückzuweisen ist dabei der Gedanke, es könne „die offene Informationspreisgabe im Internet eine Einwilligung darstellen, sodass der polizeiliche Zugriff auf solche Informationen schon keinen Eingriff in das Fernmeldegeheimnis darstellt“[67] und deswegen „der polizeiliche Ermittlungszugriff schon über die Generalklausel des § 161 Abs. 1 S. 1, § 163 Abs. 1 S. 2 StPO gedeckt“ wäre.[68] Denn ebenso gut könnte man sonst die (ob ihrer Eingriffsintensität zu Recht) in §§ 100f, 100h und 163f StPO eigens geregelten Ermittlungsmaßnahmen schlicht auf die polizeiliche Eingriffsgeneralklausel stützen mit der Begründung, wer

[56] Ganz in diesem Sinne *Hiéramente/Fenina*, StraFo 2015, 365 (371): „Nur weil das Verhalten des Bürgers im Internet im Lichte des Art. 10 GG besonders schutzwürdig ist, muss es noch nicht § 100a StPO unterfallen.“; siehe auch *Hiéramente*, HRRS 2016, 448 (450): „Aus der grundgesetzlichen Schutzbedürftigkeit folgt nicht die Notwendigkeit der extensiven Interpretation der Eingriffsmaßnahme.“

[57] Ganz richtig heißt es bei *Hiéramente/Fenina*, StraFo 2015, 365 (371): „Ein Gleichlauf der Definitionen ist keineswegs zwingend.“, und, mit Blick auf u.a. BVerfG NJW 2009, 2431 (2433), es habe das BVerfG „bereits betont, dass der Rückschluss vom Grundrecht auf die Ermächtigungsgrundlage nicht zwangsläufig ist.“; siehe auch *Wolter/Greco* (Fn. 4), § 100a Rn. 13: „Der Befugnisbereich von § 100a ist […] *nicht* mit dem Schutzzweck des Telekommunikationsgeheimnisses deckungsgleich.“ (*Hervorhebung* auch im Original).

[58] Vgl. *Gähler*, HRRS 2016, 340 (344): „Eine Zuordnung [zu § 100a StPO] muss auch unter Berücksichtigung des Aspektes erfolgen, ob der Betroffene aufgrund der Verdecktheit des Eingriffs in erhöhtem Maße schutzbedürftig ist.“

[59] So denn auf „die hohe Schutzbedürftigkeit des Cloud-Nutzers“ verweisend *Gähler*, HRRS 2016, 340 (344): „Durch die Subsumtion als Telekommunikation wird der Cloud-Nutzer […] privilegiert.“

[60] Ganz zu Recht spricht *Roggan*, StV 2017, 821 (823), hier von „*vermeintlich* grundrechtsfreundlicher Interpretation“ (*Hervorhebung* von *mir*).

[61] So aber *Hauck* (Fn. 5), § 100a Rn. 31, 81; siehe auch *Gähler*, HRRS 2016, 340 (344): „Der Eingriff darf erst unter den vergleichsweise strengen Voraussetzungen des § 100a StPO erfolgen und nicht schon nach den weiter gefassten Eingriffsvoraussetzungen anderer strafprozessualer Ermittlungsmaßnahmen.“; welche anderen (legalen) Maßnahmen dies sein sollen, lässt *Gähler* freilich offen.

[62] Ganz richtig *Hiéramente/Fenina*, StraFo 2015, 365 (371): „Schließt man Verhalten, wie etwa die Internetrecherche, aus dem Anwendungsbereich des § 100a StPO aus, ist […] die Überwachung […] dann mangels Eingriffsgrundlage in der StPO schlichtweg untersagt.“; ebenso die Einschätzung bei *Roggan*, StV 2017, 821 (823): Mittels Einbeziehung des Cloud-Computing in den Bereich der Telekommunikation „könnte […] die Zulässigkeit der Überwachung des Cloud-Computing auf Grundlage des § 100a Abs. 1 S. 2 StPO gefolgert werden“.

[63] Vgl. nur BVerfGE 29, 183 (195–197, für Eingriffe mit Freiheitsentzug), wo vom „Analogieverbot aus Art. 104 I GG, vergleichbar dem strafrechtlichen Analogieverbot aus Art. 103 II GG“ die Rede ist; siehe auch BVerfG NStZ 1996, 615; *Amelung*, NStZ 1982, 38 (40, zu § 136a StPO); *Konzak*, NVwZ 1997, 872 f.; *Krey*, ZStW 101 (1989), 838 (854 ff.); näher *Heinrich* (Fn. 1), Rn. 7 f., 701 m.w.N.

[64] So explizit *Wolter/Greco* (Fn. 4), § 100a Rn. 31a; ebenso hält LG Ellwangen ZD 2014, 33 (36), das Bemessen an dieser Vorschrift für „eher fatal“; anders jedoch *Hauck* (Fn. 5), § 100a Rn. 31, 81.

[65] Vgl. BGHSt 51, 211 (218, „lediglich geringfügig“); siehe auch *Köhler* (Fn. 16), § 161 Rn. 1 („weniger intensiv“); i.d.S. auch *Hilger*, NStZ 2000, 561 (564); *Griesbaum*, in: Hannich (Fn. 4), § 161 Rn. 1; näher *Heinrich* (Fn. 1), Rn. 703 ff. m.w.N.

[66] So betonen auch *Wolter/Greco* (Fn. 4), § 100a Rn. 31a, dass „die Ermittlungsgeneralklausel […] der Schwere des Eingriffs nicht gerecht zu werden vermag“.

[67] So aber *Hauck* (Fn. 5), § 100a Rn. 81.

[68] *Hauck* (Fn. 5), § 100a Rn. 81.

sich frei in der Öffentlichkeit bewege, willige damit konkludent in seine akustische bzw. visuelle Überwachung ein.

Kurzum: „Schließt man Verhalten, wie etwa die Internetrecherche, aus dem Anwendungsbereich des § 100a StPO aus, ist solch ein Verhalten nicht schutzlos gestellt. Im Gegenteil: Die Überwachung ist dann mangels Eingriffsgrundlage schlichtweg untersagt."[69]

IV. Lehnt man mithin, wie hier vertreten, da es sich bei der einseitigen Internetnutzung um keinen „sozialen Informationsaustausch", um „keine vertrauliche ‚Kommunikation' zwischen zwei Personen" und damit nicht um „Telekommunikation" i.S.d. § 100a StPO handelt, die Tauglichkeit eben dieser Vorschrift als Eingriffsnorm ab,[70] fragt sich, worauf sich Maßnahmen der Überwachung und Aufzeichnung von Internetsurfen, Internetrecherche, Cloud Computing etc. denn sonst stützen lassen – auf eine analoge Anwendung des § 100a StPO und eine Anwendbarkeit der Ermittlungsgeneralklauseln der § 161 Abs. 1 S. 1 StPO und § 163 Abs. 1 S. 2 StPO, wie schon erwähnt, jedenfalls nicht. Was bleibt, wäre noch die neuerdings vom Gesetzgeber in § 100b StPO zur Verfügung gestellte Online-Durchsuchung.[71]

Tatsächlich wird denn auch im Schrifttum nicht selten davon gesprochen, der hoheitliche Zugriff auf Internetsurfen, Cloud Computing etc. ähnele „ebenso im Erscheinungsbild wie beim Belastungsgewicht einer Online-Durchsuchung"[72] und sei daher „nunmehr nach § 100b StPO zu beurteilen".[73] An dieser Stelle ist es nun Zeit, zwischen Internetsurfen und Cloud Computing zu unterscheiden.

1. Wenden wir uns zunächst dem Letzteren zu. Worum also geht es der Sache nach beim sog. Cloud Computing und seiner Überwachung? „Wer eine virtuelle Festplatte nutzt, Rechenleistung in der Cloud abruft oder dort Programme/Apps zur Datenverarbeitung verwendet, kommuniziert nicht im Sinne des § 100a StPO."[74] So weit, so gut. Was aber geschieht denn eigentlich beim Cloud Computing? Um es noch einmal auf den Punkt zu bringen: Cloud Computing ist letztlich zu verstehen als „ein IT-Bereitstellungsmodell […], bei dem der Cloud-Nutzer auf die Beschaffung eigener Hard- und/oder Software verzichtet und stattdessen auf die ständig zu diesem Zweck bereitgestellten Ressourcen des Cloud-Anbieters zurückgreift".[75] „Das Spektrum dieser Dienste reicht von der Bereitstellung ‚einfacher' Datenspeicherplätze wie etwa Dropbox, Skydrive, Googledrive und der iCloud bis zur Auslagerung ganzer Benutzeroberflächen und gar Firmensystemen in die ‚Cloud'."[76]

Häufig geht es dabei im Wesentlichen oder gar ausschließlich um die Nutzung externer Speichermöglichkeiten, insbesondere um von verschiedenen Endgeräten aus oder von mehreren Personen unabhängig voneinander auf die in die Cloud gestellten Daten zugreifen zu können. Ständig wachsend ist jedoch auch die Nutzung vom Cloud-Anbieter zur Verfügung gestellter Möglichkeiten zur externen Datenverarbeitung.[77] Kurz und gut: Letztlich bedeutet mehr oder minder exzessiv praktiziertes Cloud Computing nichts anderes, als eine Verlagerung der sonst im Inneren des heimischen Computers vonstattengehenden Datenspeicherungs- bzw. Datenverarbeitungsvorgänge nach außen, im Ergebnis also eine virtuelle Erweiterung des eigenen PCs in die Cloud hinein.[78] In letzter Konsequenz „verbleibt am eigentlichen Arbeitsplatz nur noch ein Monitor und ein rudimentärer Rechner, der mehr oder weniger nur noch den Zugang zur Cloud ermöglicht."[79]

Will nun die Strafverfolgungsbehörde heimlichen Zugriff nehmen auf das in die Cloud hinein outgesourcte Datenverarbeitungsgeschehen,[80] insbesondere auf die in der Cloud auf fremden Speichermedien angelegten Datenbestände, stellt sich das im Grunde kaum anders dar, als würde sie auf das Datenverarbeitungsgeschehen am heimischen PC des Beschuldigten bzw. auf die auf dessen Festplatte abgespeicherten Daten zugreifen.[81] Dieses Bild einfach eines in die Cloud

[69] So ganz richtig *Hiéramente/Fenina*, StraFo 2015, 365 (371).

[70] Vgl. soeben Abschnitt III.

[71] Eingefügt durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens v. 17.8.2017, BGBl. 2017 I, S. 3202, in Kraft seit 24.8.2017; zur Gesetzgebungsgeschichte *Knierim*, in: Knierim/Oehmichen/Beck/Geisler (Fn. 11), Kap. 18 Rn. 1.

[72] *Eschelbach* (Fn. 4), § 100a Rn. 5 a.E.; speziell zur Überwachung des Cloud Computing siehe auch *Köhler* (Fn. 16), § 100a Rn. 14f.: Sie stehe „einer Online-Durchsuchung […] näher als einer TKÜ-Maßnahme"; *Roggan*, StV 2017, 821 (823): Sie komme „in qualitativer Hinsicht einem heimlichen Ausleiten von Datenbeständen mittels Online-Durchsuchung wesentlich näher als der Überwachung einer (Tele-)Kommunikation"; *Hiéramente/Fenina*, StraFo 2015, 365 (373): „(mindestens) dieselbe Eingriffsintensität".

[73] *Eschelbach* (Fn. 4), § 100a Rn. 5 a.E.; ebenso *Roggan*, StV 2017, 821 (825).

[74] *Hiéramente/Fenina*, StraFo 2015, 365 (372); vgl. schon oben, Abschnitt III.

[75] So zusammenfassend *Mavany*, ZIS 2018, 86, in seiner Rezension von *Wicker*, Cloud Computing und staatlicher Strafanspruch, 2016; siehe auch *Hiéramente/Fenina*, StraFo 2015, 365 (366): „ein Dienstleistungskonzept […], welches dem Nutzer Zugriff auf Soft- und/oder Hardware ermöglicht".

[76] *Gähler*, HRRS 2016, 340.

[77] Näher zu diesen *Hiéramente/Fenina*, StraFo 2015, 365 (367).

[78] Vgl. *Hiéramente/Fenina*, StraFo 2015, 365 (367): „stellt die Cloud eine externe Fortsetzung des Geräts des Cloudnutzers dar", und a.a.O., 372: „Die lokale Festplatte wird schrittweise durch die Speicherung in der Cloud ersetzt."

[79] *Gähler*, HRRS 2016, 340; siehe auch *Hiéramente/Fenina*, StraFo 2015, 365 (366): „Mehr und mehr werden Computer […] zum reinen Zugangsinstrument für den Abruf dezentral gelagerter Daten."

[80] Zur Möglichkeit des *offenen, nicht verdeckten* Zugriffs auf die in der Cloud gespeicherten Datenbestände über §§ 94 ff. StPO bzw. §§ 102, 110 Abs. 3 StPO vgl. nachfolgend Fn. 81.

[81] Was es, wie *Hiéramente/Fenina*, StraFo 2015, 367, ganz richtig dartun, den Strafverfolgungsbehörden denn auch ermöglicht, im Rahmen einer gem. § 102 StPO erfolgenden *offenen* Durchsuchung beim Verdächtigen über § 110 Abs. 3

hinein erweiterten, aber funktionell in sich geschlossenen „informationstechnischen Systems“ des Beschuldigten i.S.d. § 100b Abs. 1 StPO macht unschwer vorstellbar, dass zumindest diejenigen Autoren, die eine Anwendbarkeit des § 100a StPO ablehnen und von daher vor Einfügung des § 100b in die StPO davon überzeugt waren, es gebe somit de lege lata keine legale Möglichkeit der heimlichen Überwachung des Cloud Computing,[82] nunmehr geradezu aufatmend davon ausgehen mögen, dass jetzt in der Regelung der Online-Durchsuchung eine hinreichende Ermächtigungsgrundlage für entsprechende Eingriffe zu erblicken ist.

So nimmt man – zu Recht – an, dass § 100b StPO jetzt eben auch den heimlichen Zugriff nicht nur auf den heimischen PC des Beschuldigten ermögliche, sondern auch denjenigen auf den Server des Cloud-Anbieters, soweit es das Cloud Computing des Beschuldigten betrifft;[83] § 100b Abs. 3 S. 2 StPO stellt diese Möglichkeit des Eingriffs in informationstechnische Systeme anderer Personen (hier: des Cloud-Anbieters) ja auch ausdrücklich zur Verfügung.[84] Das mit dieser Lösung einhergehende Manko, dass damit freilich der Zugriff auf die (nicht als Telekommunikation im Sinne der TKÜ zu begreifenden) Übertragungsvorgänge in die Cloud hinein und aus der Cloud heraus mangels Anwendbarkeit des § 100a StPO noch immer nicht statthaft ist, verblasst angesichts der mit § 100b StPO eröffneten Möglichkeit, nunmehr auf die als Ergebnis der Übertragungsvorgänge in der Cloud gespeicherten Daten heimlichen Zugriff nehmen zu können.

2. Ist somit das Problem des Cloud Computing in der beschriebenen Weise mit Hilfe des § 100b StPO wohl hinreichend befriedigend in den Griff zu bekommen, lässt sich diese Lösung nicht einfach eins zu eins auch auf das Surfen im Internet übertragen. Denn so, wie sich die TKÜ und die Online-Durchsuchung ganz wesentlich dadurch voneinander unterscheiden, dass Erstere den Zugriff auf die laufende Kommunikation regelt, Letztere hingegen den Zugriff auf den vorhandenen Datenbestand,[85] unterscheiden sich auch die nach § 100b StPO zulässigen Überwachungsmaßnahmen beim Cloud Computing auf der einen und die beim Internetsurfen in den Blick zu nehmenden auf der anderen Seite: Gelangt man beim Überwachen des Cloud Computings mittels Online-Durchsuchungs-basiertem Auslesen des Cloud-Servers ans gewünschte Ermittlungsziel,[86] geht es beim Überwachen des Surfverhaltens gerade um den strafverfolgerischen Zugriff auf das laufende Internet-Geschehen, womit man sich im Grunde in der Domäne der Telekommunikationsüberwachung bewegt – wenn auch mit dem entscheidenden Schönheitsfehler, dass eben (wie in Abschnitt III. dargestellt) die Regelung des § 100a StPO zur TKÜ mangels zweiseitig erfolgender Kommunikation, nicht anwendbar ist. Was also tun?

Nun ist kaum bestreitbar, dass das Überwachen des Internetsurfens einen besonders schwerwiegenden Eingriff in die Persönlichkeitsrechte des Beschuldigten darstellt.[87] Immerhin geht es ja nicht um das eher punktuelle Abhören bzw. Mitverfolgen einzelner Surfvorgänge, sondern letztlich um eine flächendeckende Erfassung des gesamten Surfverhaltens.[88] Übertragen auf die analoge Welt wäre dies vergleichbar mit dem Einsatz einer Drohne, die tagein tagaus unsichtbar über dem zu Überwachenden schwebt und ihn ununterbrochen auf Schritt und Tritt begleitet. Dies ist ersichtlich um Einiges eingriffsintensiver als eine auf die Überwachung einzelner Telekommunikationsvorgänge beschränkte TKÜ. Wenn nun das BVerfG dem im Grunde auch durchaus zustimmt,[89] dann aber doch behauptet, durch die bei der Überwachung des Internetsurfens geschehende „Ausleitung der aufgerufenen HTML-Seiten“ ergebe sich zwar „ein quantitatives Mehr an überwachter Kommunikation als bei der Telefonüberwachung“, dieser Umstand rechtfertige aber „keine andere Bewertung“,[90] so vermag dies nicht zu überzeugen.

StPO vom durchsuchten Computer aus auch auf die Daten zuzugreifen, die in der (als bloße Erweiterung des sich körperlich beim Beschuldigten befindlichen PCs zu begreifenden) Cloud gespeichert sind. Nur wird die offene Durchsuchung vielfach nicht das Mittel der Wahl sein, wenn es (etwa im Zuge längerfristiger Ermittlungen) darum geht, den Verdächtigen auszuforschen, ohne ihn in u.U. ermittlungsgefährdender Weise in Kenntnis von den Ermittlungen zu setzen (auch hierzu a.a.O., 367 f.). Dazu, dass schließlich auch die (offene) Beschlagnahme gem. §§ 94 ff. StPO unmittelbar beim Cloudanbieter „nur bedingt für längerfristige Ermittlungen geeignet“ ist, ebenfalls a.a.O., 368). – Zum offenen Zugriff auf Cloud-Inhalte auch *Wolter/Greco* (Fn. 4), § 100a Rn. 41; *Wohlers/Greco*, in: Wolter (Fn. 4), § 94 Rn. 26.

[82] Vgl. nur (im Jahr 2016) *Wolter/Greco* (Fn. 4), § 100a Rn. 41: „Für den heimlichen Zugriff auf Cloud-Inhalte gibt es nach geltendem Recht keine Rechtsgrundlage.“; siehe *Hiéramente/Fenina*, StraFo 2015, 365 ff.: Es sei § 100a StPO „für die Überwachung des Internetdatenstroms […] schlichtweg ungeeignet“ (a.a.O., 373), bei Wegfall des § 100a StPO dann aber „die Überwachung […] mangels Eingriffsgrundlage in der StPO schlichtweg untersagt“ (a.a.O., 371).

[83] Vgl. nur *Köhler* (Fn. 16), § 100b Rn. 1, 10; insoweit ebenso *Roggan*, StV 2017, 821 (825); s.a. *Knierim/Oehmichen* (Fn. 11), Kap. 20 Rn. 32, 65.

[84] Explizit auf § 100b Abs. 3 StPO rekurrierend *Köhler* (Fn. 16), § 100b Rn. 10; *Roggan*, StV 2017, 821 (826); siehe auch *Bruns* (Fn. 4), § 100b Rn. 13.

[85] Vgl. hierzu bereits oben im Text bei Fn. 10 und 11.

[86] Vgl. oben Abschnitt 1., letzter Absatz.

[87] Näher und überzeugend hierzu *Hiéramente*, HRRS 2016, 448 (451 f.); siehe auch *Wolter/Greco* (Fn. 4), § 100a Rn. 31a: „Die Maßnahme ist in ihrer Eingriffsintensität mit der Online-Durchsuchung vergleichbar, möglicherweise sogar mit dem Zugriff auf Selbstgespräche.“

[88] Vgl. *Hiéramente*, HRRS 2016, 448 (451): „Bei der […] Internetüberwachung werden massenhaft Daten generiert, die bei einer längeren Überwachung die Erstellung eines umfassenden Persönlichkeitsprofils erlauben“.

[89] BVerfG NJW 2016, 3508 (3511) konzediert (immerhin) „ein quantitatives Mehr an überwachter Kommunikation als bei der Telefonüberwachung“.

[90] BVerfG NJW 2016, 3508 (3511).

Nicht schlagend ist gerade das Hauptargument des BVerfG, das da lautet:[91] „Denn der Masse an aufgerufenen Webseiten und eingegebenen Suchbegriffen steht ein fragmentarischer Inhalt des einzelnen Abrufs bzw. der einzelnen Informationsrecherche gegenüber. Es werden lediglich Einzelakte einer häufig nur sehr kurzen bzw. wie gerade beim ‚Surfen' lediglich oberflächlichen Kommunikation zur Kenntnis genommen."

Dem ist entschieden zu widersprechen: „Der Betroffene offenbart im Rahmen eines Telefonats, einer Email oder im Chat bewusst und freiwillig Wissen gegenüber einem Dritten. Er begibt sich damit freiwillig, wenn auch graduell des Schutzes der Privatsphäre."[92] Demgegenüber erfordert „die Nutzung des Internets zum Zwecke der reinen Informationsgewinnung (‚Googlen', ‚Surfen', Nutzung von Navigationssystemen, etc.) beziehungsweise Unterhaltung (Fernsehen, Spiele, Apps) […] keine Interaktion mit Dritten",[93] kein diesen gegenüber bewusstes Freigeben von Informationen und ist damit „seiner Natur nach […] privater",[94] weniger nach außen gerichtet. Sie ist damit „dem Selbstgespräch und Tagebucheintrag näher als der sozialen Interaktion mit Freunden und Bekannten".[95] Demgemäß ist – gerade im Hinblick auf ihr Gefährdungspotential – „die Überwachung des Surfverhaltens […] von der ‚klassischen' Telekommunikation wesensverschieden".[96] Nicht also geht es um ein bloßes quantitatives Mehr gegenüber der TKÜ, die Überwachung des Surfverhaltens stellt vielmehr ein dieser gegenüber deutliches qualitatives Plus dar.[97] Letztlich handelt es sich bei der Überwachung des Internetverkehrs um eine Form digitaler Totalüberwachung.[98]

Insoweit erscheint es – von den geschilderten Wertungsgesichtspunkten aus – durchaus naheliegend, dann eben die gegenüber den Anwendungsvoraussetzungen des § 100a StPO noch ein gutes Stück strenger ausgestaltete Online-Durchsuchung nach § 100b StPO als sedes materiae zu betrachten und demgemäß für deren Anwendbarkeit zu plädieren.[99]

Nun ist jedoch leider zu konstatieren, dass es beim Überwachen des Surf-Verhaltens um einen Eingriff in das aktuelle Nutzerverhalten geht, die Online-Durchsuchung aber den Zugriff auf den im Informationsverarbeitungssystem vorhandenen Datenbestand im Auge hat. Das passt nicht zusammen.

Möglich mag es ja sein, dass die Ermittlungsbehörden mit Hilfe der Online-Durchsuchung nach auf der Festplatte des Nutzers ggf. perpetuierten Restspuren vorherigen Surfens suchen, nur wird das bloße Surfen im Internet in aller Regel keine solchen bleibenden, mittels der Online-Durchsuchung abgreifbaren Surfspuren hinterlassen, so dass den Ermittlern bestenfalls unzusammenhängende Schnipsel des betreffenden Surfgeschehens sichtbar werden, was vermutlich nicht allzu viel Nutzen bringt.

Eine der TKÜ ähnliche *durchgehende* Überwachung des Surfverhaltens aber ist mittels § 100b StPO nicht zu rechtfertigen.[100] Und eine – ob der ja vielleicht vergleichbaren Eingriffsschwere angemessen erscheinende – analoge Heranziehung des § 100b StPO ist aufgrund des bereits erwähnten Analogieverbots bei Eingriffsnormen keine legitime Möglichkeit der Problembewältigung.[101]

V. So ist denn am Ende dieser Überlegungen zu konstatieren, dass zwar die strafverfolgerische Auswertung des Cloud Computing (im Hinblick auf die in der Cloud gespeicherten Daten) de lege lata über § 100b StPO legitimierbar ist,[102] nicht aber die Überwachung des bloßen Internetsurfens: Weder die Ermächtigungsnormen zur Telekommunikationsüberwachung noch diejenigen zur Online-Durchsuchung und schon gar nicht die allgemeinen Eingriffsgeneralklauseln der §§ 161 und 163 StPO vermögen eine solche Maßnahme zu gestatten.[103] Im Ergebnis ist also festzuhalten, dass die unmittelbare Überwachung und Auswertung des aktuellen Surfverhaltens nach unserer heutigen Gesetzeslage schlicht unzulässig ist und somit im Kanon der polizeilichen Ermittlungsmöglichkeiten jedenfalls derzeit keinen Platz findet.

De lege ferenda freilich ist durchaus die Schaffung einer eigenen Eingriffsnorm vorstellbar[104] und ein entsprechendes Tätigwerden des Gesetzgebers höchst wünschenswert, denn es lässt sich ja schwerlich bestreiten, dass in vielen Fällen ein legitimes Interesse der Strafverfolgungsbehörden daran besteht, eine Überwachung des Surfverhaltens eines Beschuldigten vorzunehmen, um auf diese Weise anders nicht zu

[91] BVerfG NJW 2016, 3508 (3511).
[92] *Hiéramente*, HRRS 2016, 448 (451).
[93] *Hiéramente*, HRRS 2016, 448 (451).
[94] *Hiéramente*, HRRS 2016, 448 (451).
[95] *Hiéramente*, HRRS 2016, 448 (451); auch *Roxin/Schünemann* (Fn. 21), § 36 Rn. 5 betonen „die Nähe zum Selbstgespräch".
[96] *Hiéramente*, HRRS 2016, 448 (451).
[97] Ausführlich und überzeugend hierzu *Hiéramente*, HRRS 2016, 448 (450 ff.).
[98] Ganz richtig *Hiéramente*, HRRS 2016, 448 (452): „[…] eignet sich die Überwachung des Internets besonders zur Erstellung umfassender Persönlichkeitsprofile".
[99] So denn auch *Eschelbach* (Fn. 4), § 100a Rn. 5: „Der hoheitliche Zugriff auf die Informationsbeschaffung der Zielperson im Internet […] ist nunmehr nach § 100b zu beurteilen."
[100] Insoweit zumindest missverständlich aber *Roggan*, StV 2017, 821 ff., wenn er zwar (ganz richtig) die „Beschränkung auf eine passive Kenntnisnahme von Datenbeständen, die sich bereits in dem System befinden", konstatiert (a.a.O., 826), dann aber (insoweit wertungswidersprüchlich) behauptet, es sei „möglich […] auch ein ‚Live-Zugriff', also der ‚heimliche Blick über die Schulter' des Betroffenen" (a.a.O., 825).
[101] Vgl. bereits im Text oben bei Fn. 63 mit Nachweisen in Fn. 63.
[102] Vgl. oben, Abschnitt IV. 1.
[103] Vgl. oben, Abschnitt IV. 2.
[104] In diesem Sinne offenbar auch *Hiéramente*, HRRS 2016, 448 (452): „Die Überwachung der Internetnutzung ist ein Grundrechtseingriff eigener Art und erfordert insbesondere aufgrund der gesteigerten Eingriffsintensität eine eigenständige strafprozessuale Grundlage."

erlangende Erkenntnisse zu gewinnen.[105] Dabei wäre aber unter Überwindung überkommener Regelungskonzepte zu berücksichtigen, dass die einseitige Internetnutzung „dem Selbstgespräch und Tagebucheintrag näher [ist] als der sozialen Interaktion mit Freunden und Bekannten“,[106] mithin „die Nutzung des Internet zu nicht sozial-kommunikativen Zwecken […] ein, von Art. 10 GG geschütztes, menschliches Verhalten eigener Art“ darstellt[107] und man deswegen „die Erhebung von Daten, die nicht sozial-kommunikativer Natur sind, als eigenständigen, typusprägenden Grundrechtseingriff anzusehen“ hat.[108] Nicht von ungefähr spiegelt sich dieser qualitative Unterschied denn auch in der Zielrichtung der Behörden wider, die eine entsprechende Maßnahme ergreifen: „Während das Abhören des Telefons und der Email-kommunikation primär dem Einblick in den Meinungs- und Wissensaustausch zwischen Beschuldigten dient, dient eine Internetüberwachung regelmäßig der Ermittlung der persönlichen Hintergründe und Vorlieben des Beschuldigten.“[109] Dem müsste in einer sachgerechten Neuregelung Rechnung getragen werden.

Auf dieser Grundlage wäre dann schließlich noch eine weitere, letztlich entscheidende Frage zu beantworten: Wie streng müsste eine solche surfspezifische Regelung ausgestaltet sein? So streng wie die ja schon eingangs als „vergleichsweise streng“ bezeichnete Regelung der TKÜ? Noch ein wenig strenger, nämlich so streng, wie die tatsächlich nur unter *noch* engeren Voraussetzungen anwendbare Online-Durchsuchung? Ohne dies hier nun aus Umfangsgründen in extenso ausbreiten zu können: Weder das eine, noch das andere.

Eine etwa zu schaffende Neuregelung müsste vielmehr in ihren Anwendungsvoraussetzungen jedenfalls strenger sein als die TKÜ,[110] aber sogar strenger auch als die Online-Durchsuchung.[111] Sie müsste (zumindest!) den gegenüber §§ 100a und 100b StPO noch einmal enger gehaltenen Anwendungsbedingungen der akustischen Wohnraumüberwachung des § 100c StPO unterworfen werden. Man denke insoweit nicht nur an den bei § 100b i.V.m. § 100d Abs. 3 StPO gegenüber § 100c i.V.m. § 100d Abs. 4 StPO weniger stark ausgeprägten Kernbereichsschutz,[112] sondern auch an das in § 100b Abs. 1 StPO fehlende Äquivalent zu der bei Lauschangriffen in § 100c Abs. 1 Nr. 3 verlangten „auf Grund tatsächlicher Anhaltspunkte“ – und nicht bloß auf Grund kriminalistischer Erfahrungswerte[113] – *konkret* bestehenden Erwartbarkeit, ermittlungsrelevante Beschuldigtenäußerungen zu erfassen:[114] „Eine solche ‚Erfolgsprognose‘ im Sinne einer Wahrscheinlichkeit des Ausleitens verfahrensrelevanter Informationen haben die Ermittler bei Online-Durchsuchungen […] nicht zu erstellen.“[115]

Denn nur so ist dem Umstand hinreichend Rechnung zu tragen, dass der beim Surfen lückenlos Überwachte mehr noch als der von einer Online-Durchsuchung[116] Betroffene für die Ermittlungsbehörden quasi zum „gläsernen Menschen“ wird, in völliger Transparenz im Hinblick auf seine Vorlieben, Neigungen und Interessen. Gerade das vermeintlich unbeobachtete Herumstöbern auf mitunter auch eher fragwürdigen Internetseiten vermag in der Summe so viel über den Einzelnen zu verraten, wie es vielleicht noch nicht einmal ein Blick in sein Tagebuch zu offenbaren vermöchte.[117]

Dem Rechnung zu tragen, wäre zwar eine klare Absage an die vom BVerfG geäußerte Auffassung, das Surfen im Internet sei nur ein quantitatives Mehr gegenüber der zweiseitigen Kommunikation via Telefonat, SMS oder E-Mail.[118] In der Sache aber wäre damit im Gesamtsystem der digitalen

---

[105] Deutlich strenger insofern *Roxin/Schünemann* (Fn. 21), § 36 Rn. 5: „legt die Nähe zum Selbstgespräch und sogar zum Denken selbst eher nahe, dass man auf ‚solipsistische‘ Inhalte keinen Zugriff erlaubt“.

[106] So ganz richtig *Hiéramente*, HRRS 2016, 448 (451), dies wie folgt erläuternd: „Die Nutzung des Internets zum Zwecke der reinen Informationsgewinnung (‚Googlen‘, ‚Surfen‘, Nutzung von Navigationssystemen, etc.) beziehungsweise Unterhaltung (Fernsehen, Spiele, Apps) erfordert […] keine Interaktion mit Dritten und ist [gegenüber der ‚klassischen‘ Telekommunikation] seiner Natur nach […] privater“.

[107] *Hiéramente*, HRRS 2016, 448 (451); sie stelle „eine logisch abgrenzbare und verfassungsrechtlich besonders schützenswerte Persönlichkeitsentfaltung dar“.

[108] *Hiéramente*, HRRS 2016, 448 (451).

[109] *Hiéramente*, HRRS 2016, 448 (451); ebenso *Roggan*, StV 2017, 821 (823).

[110] Vgl. *Roggan*, StV 2017, 821 (823): Es hätten „für entsprechende Maßnahmen angesichts ihrer evident erheblich gesteigerten Eingriffsintensität (zumindest!) die tatbestandlichen Schwellen von § 100b StPO zu gelten“, kämen sie doch „in qualitativer Hinsicht einem heimlichen Ausleiten von Datenbeständen mittels Online-Durchsuchung wesentlich näher als der Überwachung einer (Tele-)Kommunikation“.

[111] Siehe auch *Wolter/Greco* (Fn. 4), § 100a Rn. 31a: Die Überwachung des Surfverhaltens sei in ihrer Eingriffsintensität (nicht nur) „mit der Online-Durchsuchung vergleichbar“, (sondern) „möglicherweise sogar mit dem Zugriff auf Selbstgespräche“.

[112] Näher hierzu *Roggan*, StV 2017, 821 (828).

[113] Diese dezidiert nicht ausreichen lassend *Wolter*, in: Wolter (Fn. 4), § 100c Rn. 46.

[114] So der mehrfache Hinweis bei *Roggan*, StV 2017, 821 (825 und 827).

[115] *Roggan*, StV 2017, 821 (825); siehe auch a.a.O. 827: Es enthalte „§ 100b Abs. 1 StPO nicht einmal einen Ansatz eines Äquivalents zur (selbst dort schwachen) ‚Lauscherfolgs-Wahrscheinlichkeit‘ in § 100c Abs. 1 Nr. 3 StPO“.

[116] Wobei bereits bei dieser Maßnahme zu Recht zu monieren ist, dass sie „potenziell die heimliche Erstellung umfassender Persönlichkeitsprofile […] ermöglicht“ (so *Singelnstein/Derin*, NJW 2017, 2646 [2647]).

[117] Ganz richtig *Hiéramente*, HRRS 2016, 448 (452): „Selbst aus für sich genommen fragmentarischen Informationen kann ein Mosaik konstruiert werden, das Aufschluss über Gewohnheiten und Vorlieben aus allen Lebenslagen zu geben vermag.“

[118] BVerfG NJW 2016, 3508 (3511); vgl. bereits oben, Abschnitt IV. 2., bei Fn. 90.

Ermittlungsmöglichkeiten der dem Wesen und dem Gefährdungspotential einschlägiger Überwachung entsprechende, zutreffende Platz zugewiesen.