Alfred Huber

Oberstaatsanwalt als ständiger Vertreter des Leitenden Oberstaatsanwalts
Leiter der Abteilung für Betäubungsmittelsachen und Organisierte Kriminalität

Staatsanwaltschaft Nürnberg – Fürth

Stellungnahme zur Sachverständigenanhörung am 31.05.2017 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (Ausschussdrucksache 18 (6) 334)

1. Erforderlichkeit der Quellen-TKÜ aus Sicht der staatsanwaltschaftlichen Praxis

Die Telekommunikationsüberwachung ist seit vielen Jahren ein unverzichtbares Ermittlungsinstrument bei der Bekämpfung schwerer Straftaten. Sie ermöglicht den Strafverfolgungsbehörden durch das Abhören und Aufzeichnen der Gespräche insbesondere

- Beweismittel für bereits begangene Straftaten zu erlangen (z.B. Gespräche über die Tat)

- Hinweise auf weitere bevorstehende Straftaten zu erhalten (z.B. Gespräche über Planung weiterer Verbrechen).

Die Telekommunikationsüberwachung kann darüber hinaus aber auch zahlreiche wertvolle Indizien (z.B. auf die Organisationsstruktur innerhalb einer Bande, zu Beschaffungs- und Absatzwegen, etc.) liefern, die Ansätze für weitere Ermittlungen geben.

Gerade im Bereich der Bekämpfung der Organisierten Kriminalität sowie der schweren Betäubungsmittelkriminalität ist eine nachhaltige und effektive Verbrechensbekämpfung ohne die Telekommunikationsüberwachung nicht vorstellbar.

In den letzten Jahren fällt immer wieder auf, dass über die derzeit technisch mögliche Telekommunikationsüberwachung in manchen Fällen keine für die Strafverfolgung brauchbaren Erkenntnisse gewonnen werden können. Über die überwachbaren Anschlüsse werden in zunehmenden Maß nur Gespräche geführt, die nicht deliktsbezogen sind. Gleichzeitig ist erkennbar, dass ein verschlüsselter Datenverkehr stattfindet. Bei einer späteren Beschlagnahme der informationstechnischen Systeme kann nicht selten festgestellt werden, dass die deliktsbezogene Kommunikation verschlüsselt geführt wurde.

Da immer mehr Dienste, die verschlüsselten Datenverkehr anbieten, auf den Markt drängen und die Benutzung immer bedienerfreundlicher wird, ist mittelfristig damit zu rechnen, dass die Telekommunikationsüberwachung im herkömmlichen Sinn nur noch unzureichende Ergebnisse bringen wird („Going Dark“).

Dem kann wirksam nur dadurch begegnet werden, dass die Inhalte der verschlüsselten Kommunikation für die Ermittlungsbehörden zugänglich werden.

Hinsichtlich der in Rechtsprechung und Literatur umstrittenen Frage, ob die Quellen – TKÜ bereits nach derzeitiger Rechtslage zulässig ist, wird auf die Ausführungen in der Ausschussdrucksache 18(6)334 unter „B. Besonderer Teil; Zu Nummer 2“ verwiesen.

In der Entscheidung vom 20.04.2016 zum Bundeskriminalamtgesetz (BKAG) hat sich das Bundesverfassungsgericht mit der Zulässigkeit der Quellen-TKÜ befasst.[1] Das Gericht hält diese – für den Fall, dass eine eindeutige Befugnisnorm (dort: § 20l Abs.2 BKAG) gegeben ist - für zulässig. Dabei spielt für das Gericht der Umstand, dass der Gesetzgeber die technische Umsetzung der Quellen-TKÜ in § 20l Abs.2 Nr.1 und 2 BKAG ausdrücklich geregelt hat, offenbar eine wichtige Rolle. Es darf daher bezweifelt werden, ob sich die Auffassung, dass eine gesetzliche Regelung der Quellen-TKÜ nicht erforderlich ist, noch aufrechterhalten lässt.

Aus Sicht der staatsanwaltschaftlichen Praxis ist daher eine eindeutige Reglung durch den Gesetzgeber, die dem derzeitigen Meinungsstreit die Grundlage entzieht, dringend erforderlich.

Die Arbeit der Strafverfolgungsbehörden wird erheblich erschwert, wenn in jedem Fall mit dem zuständigen Gericht erst eine juristische Auseinandersetzung über die streitige Frage geführt werden muss, ob die Quellen-TKÜ nach derzeitiger Rechtslage zulässig ist. Muss z.B. gegen eine ablehnende Entscheidung des Ermittlungsrichters erst Beschwerde eingelegt werden, so entsteht ein Zeitverlust, der das Ergebnis der Ermittlungen unter Umständen gefährden kann. Auch können in einer Hauptverhandlung zeitintensive Auseinandersetzungen über die Frage der Verwertbarkeit von Erkenntnissen aus einer Quellen-TKÜ vermieden werden, wenn eine klare gesetzliche Regelung vorliegt.

---

[1] **BVerfG, Urteil vom 20.04.2016, 1 BvR 966/06, 1 BvR 1140/09:**

Rn 228: „a) § 20 l BKAG regelt die Telekommunikationsüberwachung und begründet damit Eingriffe in Art. 10 I GG. An Art. 10 I GG ist dabei nicht nur § 20 l I BKAG zu messen, der die herkömmliche Telekommunikationsüberwachung regelt, sondern auch § 20 l II BKAG, der die Quellen-Telekommunikationsüberwachung erlaubt, sofern durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation erfasst wird. Zwar setzt diese technisch einen Zugriff auf das entsprechende informationstechnische System voraus. Jedoch erlaubt § 20 l II BKAG ausschließlich Überwachungen, die sich auf den laufenden Telekommunikationsvorgang beschränken. Die Vorschrift hat damit lediglich die Aufgabe, den technischen Entwicklungen der Informationstechnik zu folgen und – ohne Zugriff auf weitere inhaltliche Informationen des informationstechnischen Systems – eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich ist. Von daher ist sie nicht am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, sondern an Art. 10 I GG zu messen (vgl. *BVerfGE* 120, 274 [309] = NJW 2008, 822).“

Selbstverständlich muss die erforderliche Software so konzipiert werden, dass nur Kommunikationsinhalte erfasst werden, die auch auf herkömmlichem Wege ausgeleitet werden können. Dies ist im Gesetzesentwurf festgeschrieben (§ 100a Abs.5 StPO-E)

2. Die Online-Durchsuchung aus Sicht der staatsanwaltschaftlichen Praxis

Die Online-Durchsuchung ist eine Ermittlungsmaßnahme, die nach hiesiger Einschätzung in der Praxis nur selten und ausschließlich im Bereich der Schwerkriminalität zum Tragen kommen wird. In diesen Fällen kann sie aber ein äußerst effektives Mittel der Strafverfolgung darstellen. Nach der derzeitigen Rechtslage (§ 161 Abs.2 StPO) dürfen in einem Strafverfahren nicht einmal die Erkenntnisse verwertet werden, die die Behörden im Rahmen der Gefahrenabwehr in zulässiger Weise erlangt haben (vgl. § 20k BKAG, Art.34d BayPAG, Art.10 BayVSG). Dass dieser Umstand im Sinne einer nachhaltigen Strafverfolgung völlig unbefriedigend ist, bedarf keiner näheren Darlegung.[2]

Die Darstellung in den Medien, dass die Online-Durchsuchung auch „für die Verfolgung leichterer Delikte wie Hehlerei oder Drogenbesitz“ (SZ vom 18.05.2017) möglich sei bzw. „flächendeckend bei ganz normaler Alltagskriminalität“ (Netzpolitik.org) eingesetzt werden soll, ist irreführend und geht sowohl in rechtlicher als auch in tatsächlicher Hinsicht an der Realität vorbei.

a) Rechtliche Voraussetzungen

aa) Straftatenkatalog

Eine Online-Durchsuchung ist nach dem Gesetzesentwurf nur bei besonders schweren Straftaten zulässig, der Katalog des § 100b StPO-E ist dem des § 100c StPO nachgebildet. Bei den in diesem Katalog genannten Straftaten hat das Bundesverfassungsgericht die akustische Wohnraumüberwachung für zulässig erklärt.[3] Da das Bundesverfassungsgericht den Grundrechtseingriff bei einer Online-Durchsuchung mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleicht[4], ist

---

[2] Die in § 161 Abs.2 StPO vorgesehene Ausnahme - die Einwilligung der von der Maßnahme betroffenen Person - spielt in der Praxis keine Rolle.

[3] **BVerfGE 109,279**; auch in seiner Entscheidung vom 27.02.2008 (**BVerfGE 120,274 ff.**) stellt das BVerfG klar, dass das Grundrecht auf Gewährung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht schrankenlos gewährleistet wird. Den dort aufgezeigten verfassungsrechtlichen Anforderungen wird durch den Straftatenkatalog des §100b StPO-E und der erforderlichen Einzelfallprüfung hinreichend Rechnung getragen.

[4] **BVerfG, Urteil vom 20.04.2016, 1 BvR 966/06, 1 BvR 1140/09,** Rn.210: „Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt dementsprechend vor einem geheimen Zugriff auf diese Daten und damit insbesondere vor Online-Durchsuchungen, mit denen private Computer wie sonstige informationstechnische Systeme manipuliert und ausgelesen, sowie persönliche Daten, die auf externen Servern in einem berechtigten Vertrauen auf Vertraulichkeit ausgelagert sind, erfasst und Bewegungen der Betroffenen im Netz verfolgt werden. Wegen der oft höchstpersönlichen Natur dieser Daten, die sich insbesondere auch aus deren Verknüpfung ergibt, ist ein Eingriff in dieses Grundrecht von besonderer Intensität. Er ist seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar.“

es nur folgerichtig, wenn der Gesetzesentwurf davon ausgeht, dass der Eingriff bei denselben Delikten zulässig ist.

Die Argumentation der Gegner des Entwurfs, das Bundesverfassungsgericht erlaube die Online-Durchsuchung nur bei „Gefährdung von Menschenleben, ihrer Gesundheit und elementarsten Lebensgrundlagen“ (vgl. netzpolitik.org.) ignoriert vollständig, dass das Bundesverfassungsgericht in seiner Entscheidung vom 20.04.2016 zum BKAG eine Entscheidung zur Frage der Zulässigkeit einer Online-Durchsuchung zur Gefahrenabwehr getroffen hat. In Randnummer 107 der genannten Entscheidung stellt das Gericht dabei sogar ausdrücklich klar, dass sich für den Bereich der Strafverfolgung andere Maßstäbe gelten.[5]

bb) Einzelfallprüfung

Von den Kritikern des Gesetzesentwurfes wird verschwiegen, dass der Gesetzesentwurf die Online-Durchsuchung nur gestattet, wenn die Tat auch im Einzelfall besonders schwer wiegt (§ 100b Abs.1 Nr.2 StPO-E). Damit wird klargestellt, dass der Gesetzgeber bei Katalogtaten, die sich – anders als z.B. Mord oder schwerer Raub mit Todesfolge - nicht in jedem Einzelfall den besonders schweren Straftaten zuordnen lassen (z.B. § 100b Abs.2 Nr.1 StPO-E „gewerbsmäßige Hehlerei“ oder § 100b Abs.2 Nr.2a StPO-E „Verleiten zur missbräuchlichen Asylantragstellung nach § 84 Abs.3 Asylgesetz“), eine weitere Einschränkung fordert, um einen ausufernden Einsatz der Online-Durchsuchung zu verhindern.

In der Praxis prüfen die Gericht gerade diesen Punkt sehr genau, so dass die Befürchtung, auch bei Delikten aus dem Bereich der mittleren Kriminalität müsse mit Online-Durchsuchungen gerechnet werden, unbegründet sind. Da das zuständige Gericht verpflichtet ist, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme einzelfallbezogen in der Begründung der

---

[5] **BVerfG Urteil vom 20.04.2016, 1 BvR 966/06, 1 BvR 1140/09:**

Rn. 107: „Für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, kommt es auf das Gewicht der verfolgten Straftaten an, die der Gesetzgeber insoweit in – jeweils näher bestimmte – erhebliche, schwere und besonders schwere Straftaten eingeteilt hat. So bedarf die Durchführung einer Wohnraumüberwachung des Verdachts einer besonders schweren Straftat (vgl. *BVerfGE* 109, Seite 279, 343 ff. = NJW 2004,Seite 999), die Durchführung einer Telekommunikationsüberwachung oder die Nutzung von vorsorglich erhobenen Telekommunikationsverkehrsdaten des Verdachts einer schweren Straftat (vgl. *BVerfGE* 125,Seite 260, 328 f. = NJW 2010,Seite 833, *BVerfGE* 129, Seite 208, 243 = NJW 2012, 833) und die Durchführung einer anlassbezogenen Telekommunikationsverkehrsdatenerhebung oder einer Observation etwa durch einen GPS-Sender einer – im ersten Fall durch Regelbeispiele konkretisierten – Straftat von erheblicher Bedeutung (vgl. *BVerfGE* 107,Seite 299, 321f. = NJW 2003, 1787; *BVerfGE* 112,Seite 304, 315 f. = NJW 2005, 1338; zu letzterer Entscheidung vgl. auch *EGMR*, NJW 2011, 1333, 1337 § 70 – Uzun/Deutschland zu Art.8 EMRK). “

Anordnung darzulegen (§ 100e Abs.4 Ziffer 2 StPO-E), ist eine weitere verfahrenstechnische Sicherung gegen eine ausufernde Anordnung der Online-Durchsuchung getroffen.

Da § 100b StPO-E dem § 100c StPO (Wohnraumüberwachung) nachgebildet ist, ist für eine Prognose, wie häufig künftig eine Online–Durchsuchung angeordnet werden wird, ein Vergleich mit § 100c StPO zulässig. Die hierzu erhobenen Statistiken belegen eindrucksvoll, dass die Strafverfolgungsbehörden die Vorgaben des Bundesverfassungsgerichts verantwortungsvoll umsetzen und nur in absoluten Ausnahmefällen auf die Wohnraumüberwachung zurückgreifen.

cc) Verfahrensrechtliche Absicherung

Aus hiesiger Sicht darf bezweifelt werden, ob die Verfassungsmäßigkeit der Online–Durchsuchung davon abhängt, dass anstelle des Ermittlungsrichters beim Amtsgericht gemäß § 100e Abs.2 StPO-E eine Kammer des Landgericht über die Anordnung entscheidet. Vergleichbares gilt für die in § 100e Abs.2 S.4 StPO-E angeordnete Monatsfrist.

Das Bundesverfassungsgericht hält in der zitierten Entscheidung vom 20.04.2016 zum BKAG eine Entscheidung durch das Amtsgericht (vgl. § 20v BKAG) sowie eine Befristung der Online-Durchsuchung auf drei Monate für verfassungsrechtlich unbedenklich.[6] Es ist nicht ersichtlich, weshalb die Online-Durchsuchung in der StPO nur unter strengeren Voraussetzungen zulässig sein soll.

Aus Sicht der staatsanwaltschaftlichen Praxis ist aber festzustellen, dass die Antragstellung bei einer Kammer des Landgerichts für die Staatsanwaltschaft ebenso problemlos möglich ist wie eine Antragstellung beim Ermittlungsrichter.

Die Möglichkeit, die Dauer der Online–Durchsuchung von vorherein auf drei Monate zu befristen, wenn bereits zum Zeitpunkt der Anordnung sicher zu erwarten ist, dass länger andauernde Ermittlungen, z.B. zur Struktur einer kriminellen Organisation erforderlich sind, wäre demgegenüber für die Strafverfolgungsbehörden eine deutliche Entlastung. Da § 100e Abs.5 StPO-E vorsieht, dass die Maßnahme unverzüglich zu beenden ist, wenn die Voraussetzungen der Anordnung nicht mehr vorliegen, werden die Rechte des Betroffenen gewahrt.

---

[6] **BVerfG, aaO.** Rn.216 „c) Keine Bedenken bestehen weiter gegen die verfahrensrechtliche Ausgestaltung der Vorschrift (vgl. § 20k V, VI BKAG). Die Anordnung einer Maßnahme ist nur durch den Richter möglich und dabei sachhaltig zu begründen (vgl. *BVerfGE* 120, 274 [331ff.] = NJW 2008, 822; s. oben C IV 2). Die mögliche lange Dauer von drei Monaten, für die die Maßnahme angeordnet werden kann, ist verfassungsrechtlich allerdings nur mit der Maßgabe tragfähig, dass es sich hierbei für die jeweilige Anordnung um eine Obergrenze handelt und sich die tatsächliche Dauer der Anordnung nach einer Verhältnismäßigkeitsprüfung im Einzelfall richtet."

b) Prognose über die Umsetzung in der Praxis

Zunächst muss klargestellt werden, dass die Strafverfolgungsbehörden in der großen Masse der Fälle eine wesentlich einfachere Möglichkeit haben, um auf Daten eines informationstechnischen Systems zuzugreifen. Durch eine richterliche Durchsuchungs- und Beschlagnahmeanordnung können sie unter den Voraussetzungen der §§ 94 ff. StPO auf die Daten eines Mobilfunkgerätes bzw. Computers zugreifen. Diese Art der Ermittlung wird in der staatsanwaltschaftlichen Praxis auch künftig der Regelfall bleiben. Sie ist erforderlich und – im Sinne des Übermaßverbotes – auch ausreichend, wenn es sich um die Ermittlung eines abgeschlossenen Sachverhalts handelt und Anhaltspunkte dafür bestehen, dass auf den informationstechnischen Systemen des Beschuldigten (ggfls. eines Dritten) Beweise gespeichert sind, die für einen Tatnachweis benötigt werden (z.B. Speicherung von kinderpornographischen Bildern, volksverhetzenden Äußerungen etc.).

Der Nachteil dieser Art des Zugriffs ist der Umstand, dass der Beschuldigte ab dem Moment der Beschlagnahme Kenntnis von den gegen ihn geführten Ermittlungen hat. Gerade bei der Bekämpfung der Organisierten Kriminalität ist eine nachhaltige Strafverfolgung jedoch nur möglich, wenn die Ermittlungen – gegebenenfalls auch über einen längeren Zeitraum – verdeckt geführt werden, z.B. um Erkenntnisse über die Strukturen innerhalb einer Organisation zu gewinnen. Werden die Ermittlungen zu früh offen gelegt, so ist es regelmäßig nicht möglich, gegen die Beschuldigten auf der Führungsebene einer Organisation einen Tatnachweis zu führen. Die Handlanger, die häufig bei der Ausführung der Taten verhaftet werden können, sind nur in den seltensten Fällen bereit, gegen ihre Auftraggeber auszusagen. Häufig besteht dann zwar der Verdacht, dass eine bestimmte Person innerhalb einer Organisation die Aufträge für die Straftaten gibt und den Großteil der dadurch erzielten Gewinne einstreicht. Ebenso häufig fehlen allerdings gerichtsverwertbare Beweise. In derartigen Fällen gibt die Online-Durchsuchung die Möglichkeit, die Mitglieder einer Organisationen über einen gewissen Zeitraum zu überwachen, um festzustellen, wer die Entscheidungen trifft und wer die Befehle lediglich ausführt.

3. Zusammenfassung

Sowohl die Quellen–TKÜ als auch die Online-Durchsuchung sind strafprozessuale Ermittlungsmaßnahmen, die für eine zeitgemäße Strafverfolgung unabdingbar sind. Durch den Gesetzesentwurf ist sichergestellt, dass sie nur bei schweren (Quellen-TKÜ) bzw. besonders schweren (Online-Durchsuchung) Straftaten zum Einsatz kommen dürfen.