ALLGEMEINE BEITRÄGE

Onlinedurchsuchung und Quellen-TKÜ in der Strafprozessordnung – Neuordnung der tiefen technischen Eingriffsmaßnahmen in der StPO seit dem 24.8.2017

von OStA Dieter Kochheim[*]

Abstract
Am 24. August 2017 sind eine Reihe von Änderungen im Straf- und -verfahrensrecht in Kraft getreten, darunter besonders auch die Quellen-TKÜ in § 100a Abs. 1 StPO n.F. und die Onlinedurchsuchung in § 100b StPO n.F.

Der Beitrag beschreibt zunächst die zügige Verabschiedung im parlamentarischen Verfahren (I, I.1) und gibt einen Überblick über die maßgeblichen Änderungen (I.2) sowie über das jetzt geltende System der technischen Eingriffsmaßnahmen in den §§ 100a bis 101b StPO (I.3).

Unter Teil II werden die abschließenden Straftatenkataloge in den §§ 100a, 100b und 100g StPO im Hinblick auf die üblichen Erscheinungsformen des Cybercrime mit dem Ergebnis betrachtet, dass dem IuK-Strafrecht im Wesentlichen die Instrumente der Überwachung der Telekommunikation und der Quellen-TKÜ zur Verfügung stehen. Dabei ergibt sich auch, dass die Straftatenkataloge im Detail Wertungswidersprüche enthalten und besonders der des § 100g Abs. 2 StPO für wichtige Kriminalitätsfelder keine „Tür" öffnet, die dennoch der Besonders schweren Kriminalität angehören.

Der Autor ist der Auffassung, dass jedenfalls die Onlinedurchsuchung für die Strafverfolgung keine nachhaltige Bedeutung haben wird. Deshalb ist es nötig, die Frage nach der wirksamen Verwertung polizeirechtlich erlangter Erkenntnisse im Strafverfahren zu stellen. Dem widmet sich der Teil III.

Teil III behandelt die strafverfahrensrechtlichen Verwertungsschranken und den hypothetischen Ersatzeingriff.

Ausgehend von dem Doppeltürmodell des BVerfG werden die gesetzlich geregelten Verwertungsschranken und ihre Öffnungen dargestellt. Eine besondere Betrachtung verdienen die §§ 100e Abs. 6 und 101a Abs. 5 StPO, die verbindliche Verwertungsverbote einrichten und auch den von der Rechtsprechung entwickelten Spurenansatz ausschließen. Sie führen dazu, dass der Spurenansatz greift, solange personenbezogene Daten unter den Voraussetzungen des Straftatenkatalogs des § 100a Abs. 2 StPO erhoben wurden. Wegen der Onlinedurchsuchung und dem Zugriff auf Vorratsdaten ist hingegen der Spurenansatz von der Rechtsprechung des BVerfG ausgeschlossen worden.

I. Umfassende Reform der StPO, des StGB und anderer Gesetze

Am 22.2.2017 startete die Bundesregierung zwei strafrechtliche Reformvorhaben, einerseits mit dem *Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze*[1] und andererseits mit dem *Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*.[2] Darin vorgesehen sind etliche vernünftige Neuregelungen gewesen. Das gilt etwa für die Anordnung der Blutprobe in Straßenverkehrssachen ohne Richtervorbehalt (§ 81a StPO),[3] die Verwertbarkeit von Beinahetreffern[4] (§§ 81e, 81h StPO) und ganz besonders die mit Ordnungsgeld bewehrte Erscheinenspflicht von Zeugen bei der Polizei (§ 163 StPO),[5] wenn ihre Vernehmung von der Staatsanwaltschaft angeordnet worden ist. Daneben werden die Erleichterung des Verfahrens bei der

---

* Der Verfasser ist Oberstaatsanwalt bei der Staatsanwaltschaft Hannover. Der Beitrag beruht auf dem Vortrag, den der Verfasser am 1.12.2017 anlässlich der KriPoZ-Tagung an der Deutschen Hochschule der Polizei in Münster hielt.

1 BT-Drs. v. 22.2.2017 – 18/11272.

2 BT-Drs. v. 22.2.2017 – 18/11277.

3 Die Anordnung der Entnahme einer – oder mehrerer (Nachtrunkeinrede) – Blutprobe nach altem Recht ist zeitkritisch und vergleichbar der stillen Post: Der Streifenpolizist ruft (zu welcher Tageszeit auch immer und gerne auch nächtens) den eildiensthabenden Staatsanwalt an, trägt einen Sachverhalt vor, der Staatsanwalt stellt noch ein paar schlaue Fragen und ruft dann den Ermittlungsrichter an, der vielleicht noch erreichbar ist. Die von ihm gefilterten Informationen übermittelt er dem diensthabenden Ermittlungsrichter und der ordnet dann die Blutprobe an, weil ihm gar nichts anderes übrig bleibt. Die einzige sachliche Kontrolle obliegt dem diensthabenden Staatsanwalt und dessen Entscheidungsspielraum bei Straßenverkehrssachen gründelt auf tiefem Niveau. Das muss die Polizei jetzt selber verantworten.

4 Die Beinahetreffer wurden bislang von der Rechtsprechung akzeptiert: *BVerfG,* Beschl. v. 13.5.2015 - 2 BvR 616/13; *BGH,* Urt. v. 20.12.2012 – 3 StR 117/12; jetzt § 81h Abs. 1 nach Nr. 3 StPO.

5 Die Erscheinens- und Aussagepflicht von Zeugen bei der Polizei wird seit gefühlten Ewigkeiten von der Ermittlungspraxis und verschiedenen Regierungsverantwortlichen gefordert, kam aber vorher nicht zustande. Auch schriftliche Auskunftsersuchen der Polizei sind jetzt ordnungsgeldbewehrt, wenn die Staatsanwaltschaft diese Auskunftserhebung angeordnet.

Richterablehnung (§§ 26 ff. StPO), wegen der Fristsetzung und der inhaltlichen Gestalt von Beweisanträgen (§ 244 StPO) sowie wegen der Videovernehmung des Beschuldigten erstrebt (§ 136 StPO). Über den Sinn anderer Reformprojekte lässt sich streiten. Das gilt für die sowieso schon gängige Abstimmung über die Verhandlungstermine mit der Verteidigung und der Staatsanwaltschaft in Umfangsverfahren (§ 213 StPO) und ganz besonders für die Eröffnungsrede der Verteidigung nach § 243 StPO, gegen die der Staatsanwaltschaft keine Erwiderung zusteht. Welche Bedeutung das Fahrverbot bei Nicht-Verkehrsstraftaten erlangen wird (§ 44 StGB), muss sich zeigen. Sinnvoll ist jedenfalls die Ausgestaltung der Nötigung als Privatklagedelikt (§ 374 StPO) und sinnlos sind die weiteren Tatbestände zum besonders schweren Fall des Vorenthaltens von Sozialversicherungsbeiträgen (§ 266a StGB), die zwar auf die Verwendung von Abdeckrechnungen[6] ansprechen, aber die Erstellung solcher Scheinrechnungen keiner eigenen Strafdrohung unterwerfen.[7] Soweit der Überblick über die ursprünglichen Reformbemühungen.

1. Parlamentarische Beratungen

Am 9.3.2017 verhandelte der Bundestag in erster Beratung über beide Gesetzesentwürfe und verwies sie in die Ausschüsse.[8]

Maßgeblich ist der Rechtsausschuss (Ausschuss für Recht und Verbraucherschutz), der am 15.5.2017 tagte. Genau unter diesem Datum erschien auch die *Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD* ...[9] und die hat es in sich: Einfügung der Quellen-TKÜ in den § 100a Abs. 1 S. 2 StPO nebst ergänzenden Regeln für diese Eingriffsmaßnahme (§ 100a Abs. 4 bis 6 StPO), Einführung der Onlinedurchsuchung durch einen völlig neu gestalteten § 100b StPO einschließlich eines Straftatenkatalogs (Abs. 2), der nahtlos aus dem § 100c StPO überführt wird (Akustische Wohnraumüberwachung; großer Lauschangriff), und eine nachhaltige Umgestaltung des Rechts der Eingriffsmaßnahmen in den §§ 100a bis 101b StPO.

Der Rechtsausschuss hat beide Gesetzesentwürfe und die Formulierungshilfe zusammengefasst.[10] In zweiter Beratung vom 22.6.2017[11] und nach Gegenreden der beiden Abgeordneten *Wunderlich* und *Ströbele* hat der Bundestag einen Gegenantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN[12] abgelehnt und dem Entwurf des Rechtsausschusses mehrheitlich zugestimmt.[13] Nach einer Gegenrede der niedersächsischen Justizministerin *Niewisch-Lennartz*[14] hat der Bundesrat am 7.7.2017 seine Zustimmung erteilt.[15]

Das Gesetz wurde am 23.8.2017 im Bundesgesetzblatt veröffentlicht[16] und trat mit geringfügigen Ausnahmen am 24.8.2017 in Kraft.

Das ganze Gesetzgebungsverfahren hat 4 ½ Monate gedauert und am Ende befinden sich die Quellen-TKÜ und die Onlinedurchsuchung in der Strafprozessordnung, ohne dass die beiden Eingriffsmaßnahmen in der Öffentlichkeit diskutiert wurden. Das Verfahren scheint formell ordnungsgemäß gewesen zu sein und es bleibt nur der fahle Nachgeschmack, dass im Rechtsausschuss versteckt hinter wichtigen, im Ergebnis aber unscheinbaren Gesetzesänderungen zwei maßgebliche Eingriffsmaßnahmen zu Gesetz wurden, die in den ursprünglichen Gesetzesentwürfen nicht enthalten waren.[17]

2. Die Rechtslage seit dem 24.8.2017

Die wesentlichen Neuerungen sind:

§ 44 StGB	Fahrverbot bei Nicht-Verkehrsdelikten
§ 266a StGB	Vorenthalten von Sozialversicherungsbeiträgen
§ 81a StPO	Blutprobe ohne Richtervorbehalt
§§ 81e, 81h StPO	Verwertung von Beinahetreffern
§ 100a StPO	Quellen-TKÜ
§ 100b StPO	Onlinedurchsuchung
§ 136 StPO	Belehrung des Beschuldigten, Videoaufzeichnung
§ 163 StPO	Erscheinens- und Aussagepflicht des Zeugen bei der Polizei
§ 374 StPO	Nötigung als Privatklagedelikt

Im Folgenden interessiert mich die neue Gestalt des Rechts der Eingriffsmaßnahmen in den §§ 100a ff. StPO.

3. Änderungen im Recht der technischen Eingriffsmaßnahmen

§ 100a StPO betrifft jetzt nicht nur die Überwachung der Telekommunikation (TKÜ) – ursprünglich: Telefonüberwachung, sondern auch die Quellen-TKÜ einschließlich der Messengerdienste. Die traditionelle TKÜ folgt dem Bild vom heimlichen Horcher an der Leitung. Dem wiederum folgend begreift das *BVerfG* den Eingriff in den technischen Vorgang der Telekommunikation – also auf die Leitung; besser: auf ihre Schnittstellen im technischen TK-Prozess – als einen Eingriff im Sinne von Art. 10 GG.[18] Der kommunikative Zugriff auf Inhalte und Verkehrsdaten als Kommunikationspartner („Endgerät“

6 Scheinrechnungen von angeblichen Subunternehmern, die in die Buchhaltung eingestellt werden, um Schwarzlöhne und verdeckte Gewinnausschüttungen zu verschleiern.

7 Der Ersteller der Abdeckrechnungen bleibt somit Gehilfe beim Grunddelikt, so dass ihm nicht nur die Tatsache nachgewiesen werden muss, Abdeckrechnungen erstellt zu haben, sondern auch, dass diese kriminell genutzt wurden (Akzessorietät).

8 BT-Protokoll v. 9.3.2017, S. 22 142 und S. 22 183.

9 Ausschuss-Drs.18(6)334 v. 15.5.2017.

10 BT-Drs. 18/12785 v. 20.6.2017.

11 BT-Protokoll v. 22.6.2017, S. 24 585 ff.

12 BT-Drs. 18/12834 v. 21.6.2017.

13 BT-Protokoll v. 22.6.2017, S. 24 595.

14 BR-Protokoll v. 7.7.2017, S. 355.

15 BR-Protokoll v. 7.7.2017, S. 356.

16 BGBl. I v. 23.8.2017, S. 3202.

17 Auf die Formulierungshilfe wurde ich erst durch eine Meldung bei Heise online aufmerksam und dann neugierig: Stefan *Krempl*, Schwarz-Rot will Einsatz von Staatstrojanern massiv ausweiten, Heise online 17.5.2017.

18 *BVerfG,* Urt. v. 27.2.2008 – 1 BvR 370/07, 595/07, Rn. 182, 183, 184; *BVerfG,* Beschl. v. 13.11.2010 – 2 BvR 1124/10, Rn. 13 (verlängerter Schutz für Verkehrsdaten nach ihrer Speicherung beim Zugangsprovider).

oder „Anschluss“ im Sinne des TKG) folgt hingegen nur den Grundsätzen, die zur informationellen Selbstbestimmung entwickelt wurden,[19] und nicht auch denen zur technischen Integrität.[20] Eine Entschlüsselung auf dem Übermittlungsweg ist denklogisch nicht unmöglich,[21] faktisch aber wegen der erforderlichen Rechnerleistung ausgeschlossen. Ein „Horcher“ ist aber auch eine Malware, die dem Zielgerät untergeschoben wird, um die Kommunikation abzugreifen, bevor sie verschlüsselt (Versand) oder nachdem sie entschlüsselt wurde (Empfang). Aus technischer Sicht unterscheidet sich die forensische Malware nicht (Remote Forensic Software), wenn es darum geht, nur die Telekommunikation (Quellen-TKÜ; § 100a StPO[22]) oder auch alle weiteren gespeicherten Daten und Datenverarbeitungsprozesse abzugreifen (Onlinedurchsuchung; § 100b StPO). Sie nistet sich in den Datenverarbeitungsprozessen im Prozessor (CPU) und im Arbeitsspeicher (Hauptspeicher) ein und kann je nach dem, welche Instrumente zur Detektion sie mitführt, alle Datenverarbeitungsprozesse und die in den angeschlossenen Massenspeichern (Festplatten, andere Speichermedien, Cloud) abgelegten Daten durchsuchen.

Die systematische Struktur der technischen Eingriffsmaßnahmen in der Strafprozessordnung hat durch die Änderungen eine neue und im Ergebnis klarere Gestalt bekommen. Das zeigt sich besonders daran, dass die Vorschriften über das Verfahren und die Förmlichkeiten der TKÜ (§ 100b StPO a.F.) und des Großen Lauschangriffs (§ 100c StPO a.F.) jetzt in den neuen Fassungen der §§ 100d (Kernbereichsschutz) und 100e StPO (Verfahrensregeln) zusammengefasst wurden. Der § 100b StPO a.F. wurde dabei völlig aufgelöst und widmet sich jetzt der Onlinedurchsuchung. Beide Maßnahmen, die Onlinedurchsuchung und der Große Lauschangriff, behandelt das *BVerfG* als schwerste Eingriffsmaßnahmen, die miteinander vergleichbar sind.[23] Dem folgt die jetzige Gesetzesfassung und sie hat dadurch folgende Struktur bekommen:

§ 100a StPO

Abs. 1	Voraussetzungen der Überwachung der Telekommunikation.
Abs. 1 S. 2, S. 3	Quellen-TKÜ sowie Inhalts- und Verkehrsdaten gespeicherter, vormals verschlüsselt übermittelter Nachrichten
Abs. 2	Straftatenkatalog in Bezug auf die „Schwere Kriminalität“.
Abs. 3	Ausweitung beider Eingriffsmaßnahmen auf die Nachrichtenmittler
Abs. 4	Mitwirkungspflicht der Zugangsprovider.
Abs. 5	Beschränkung der Quellen-TKÜ auf die Inhalts- und Verkehrsdaten der Telekommunikation.
Abs. 6	Protokollierung der Quellen-TKÜ einschließlich der Angaben zum angegriffenen itS,[24] der Entscheidungsgrundlage für die Anordnung und der Eingriffsbehörde.

§ 100b StPO

Abs. 1	Voraussetzungen der Onlinedurchsuchung.
Abs. 2	Straftatenkatalog in Bezug auf die „Besonders schwere Kriminalität“; vormals § 100c Abs. 2 StPO (Großer Lauschangriff, jetzt weggefallen).
Abs. 3	Ausweitung der Eingriffsmaßnahme auf die Nachrichtenmittler.
Abs. 4	Verweise auf § 100a Abs. 5 und Abs. 6 mit Ausnahme auf die Beschränkung der Quellen-TKÜ auf reine Kommunikationsdaten.

§ 100c StPO

Abs. 1	Voraussetzungen der Akustischen Wohnraumüberwachung unter Verweis auf die Besonders schweren Straftaten aus dem Katalog des § 100b Abs. 2 StPO.
Abs. 2	Ausweitung der Maßnahme auf Drittbetroffene und Nachrichtenmittler.

§ 100d StPO

Abs. 1	Kernbereichsschutz für alle Maßnahmen nach den §§ 100a bis 100c StPO.
Abs. 2	Verwertungsverbot und Löschpflicht.
Abs. 3	Technische Anforderungen an die Onlinedurchsuchung, um kernbereichsbezogene Erkenntnisse zu verhindern; verbindliche gerichtliche Entscheidung in Zweifelsfällen.[25]
Abs. 4 S. 1	Verbot der Onlinedurchsuchung und des Großen Lauschangriffs bei allen Berufshelfern im Sinne von § 53 StPO.
Abs. 4 S. 2	Grundsätzliches Verwertungsverbot für Zufallsfunde, die von Angehörigen (§ 52 StPO) oder Berufshelfern herrühren (§ 53 StPO), nach Maßgabe des § 160a StPO.

§ 100e StPO

Abs. 1	Anordnungskompetenz des Ermittlungsgerichts in den Fällen des § 100a StPO; Gefahr im Verzug: Anordnung der StA mit gerichtlicher Bestätigung.

[19] *BVerfG,* Urt. v. 15.12.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 (Volkszählungsurteil).

[20] *BVerfG,* Urt. v. 27.2.2008 – 1 BvR 370/07, 595/07 (Onlinedurchsuchung).

[21] Auch die *Enigma* wurde von genialen britischen Mathematikern geknackt.

[22] § 100a Abs. 1 S. 3 StPO lässt auch die Durchsicht und Speicherung schon gespeicherter Kommunikationsdaten zu, wenn sie auf dem Übertragungsweg verschlüsselt waren und entschlüsselt gespeichert werden (Messenger ua).

[23] *BVerfG,* Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 115, 210.

[24] itS: informationstechnisches System im Anschluss an *BVerfG,* Urt. v. 27.2.2008 – 1 BvR 370/07, 595/07 (Onlinedurchsuchung).

[25] Die Kommunikation über stattgefundene oder geplante Straftaten unterliegen keinem Kernbereichsschutz, auch wenn sie mit Elementen des Kernbereichs verknüpft sind: *BVerfG,* Urt. v. 27.2.2008 – 1 BvR 370, 595/07, Rn. 281; *BVerfG,* Beschl. v. 26.6.2008 – 2 BvR 219/08, Rn. 19 (Tagebuch). Das sind im Wesentlichen die Anwendungsfälle, in denen eine gerichtliche Entscheidung in Betracht kommt.

Abs. 2	Anordnungskompetenz der Staatsschutzkammer in den Fällen der §§ 100b und 100c StPO; Gefahr im Verzug: Anordnung des Vorsitzenden der Staatsschutzkammer; Verlängerung der Maßnahme nach 6 Monaten: Entscheidung des *OLG*.
Abs. 3	Formelle Anforderungen an dem Eingriffsbeschluss.
Abs. 4	Formelle Anforderungen an dem Fortsetzungsbeschluss.
Abs. 5	Beendigungsgebot und Anordnungsbefugnisse.
Abs. 6	Verwertungsbeschränkungen für und aus schwellengleichen Eingriffsmaßnahmen in anderen Verfahren und Verfahrensordnungen (hypothetischer Ersatzeingriff).

Während der § 100g StPO (Verkehrsdaten, Vorratsdaten) und ihm folgend § 101a StPO (Verfahrensregeln) zuletzt 2015 nachhaltig geändert wurden,[26] sind durch die Reform von 2017 die §§ 100f bis 101b StPO nur redaktionell angepasst worden.

4. Bedeutung der neuen Eingriffsinstrumente

Nach den Unterrichtungen der Bundesregierung über die Eingriffsmaßnahmen mit strenger Katalogbindung[27] stiegen die Anordnungen nach § 100g StPO von 9.901 (2012) über 13.979 (2014) auf 16.363 (2016), wobei nach dem Ablauf der Übergangsregelung am 29.7.2017 (§ 12 Abs. 1 EGStPO) mit einem jähen Absinken der Zugriffszahlen zu rechnen ist. Die Anordnungen nach § 100a StPO schwankten zwischen 2012 und 2016 zwischen 5.625 (2014) und 5.945 (2015). Dagegen wurden von der Strafverfolgung zwischen 2012 und 2015 jährlich zwischen 6 (2014) und 8 (2012) Akustische Wohnraumüberwachungen gemäß § 100c StPO durchgeführt.

Sowohl die Quellen-TKÜ als auch die Onlinedurchsuchung sind technisch aufwendige Eingriffsmaßnahmen, die einer soliden Vorbereitung und Erkundung der technischen Umgebung des Zielsystems bedürfen. Wegen dieser Schwierigkeiten und der hohen Eingriffsschwellen, die § 100b StPO setzt, vermute ich, dass künftig sehr wenige – also vergleichbar dem Großen Lauschangriff – Onlinedurchsuchungen in strafrechtlichen Ermittlungsverfahren durchgeführt werden. Mit den Eingriffsschwellen anhand der einschlägigen Straftatenkataloge befasst sich unten Nr. 2.

Eher erwarte ich die Fälle, in denen eine Quellen-TKÜ oder eine Onlinedurchsuchung in anderen Verfahrensordnungen – zum Beispiel nach dem Polizeirecht – durchgeführt werden und sich die Frage stellt, unter welchen Voraussetzungen und mit welcher Beweisqualität die dort gewonnenen Erkenntnisse in das Strafverfahren als Vollbeweis oder als Spur übernommen werden dürfen. Dementsprechend widmet sich unten die Nr. 3 den gesetzlichen Verwertungsregeln, dem hypothetischen Ersatzeingriff und schließlich dem von der Rechtsprechung entwickelten Spurenansatz. Besondere Verwertungsregeln und -verbote in Bezug auf die Angehörigen (§ 52 StPO) und besonders die Berufshelfer (§ 53 StPO) werden hier nicht vertieft betrachtet.

II. Straftatenkataloge betreffend die Schwere und Besonders schwere Kriminalität

Nach der Definition des *BVerfG* betrifft ein Gesetz[28] die besonders schwere Kriminalität, wenn es mit einer Höchstfreiheitsstrafe von mehr als 5 Jahren droht.[29] Der Straftatenkatalog des § 100a Abs. 2 StPO befasst sich ausdrücklich mit der Schweren Kriminalität und ist für seine Anwendungsfälle abschließend, auch wenn etliche Katalogstraftaten mit einer Höchstfreiheitsstrafe von nur 5 Jahren drohen und viele Gesetze nicht in ihm enthalten sind (zum Beispiel der besonders schwere Fall der schweren Computersabotage; § 303b Abs. 4 StGB). Die Akustische Wohnraumüberwachung und die Onlinedurchsuchung beziehen sich jetzt einheitlich auf den deutlich engeren Straftatenkatalog in § 100b Abs. 2 StPO, der deckungsgleich aus dem § 100c Abs. 2 StPO a.F. übernommen wurde und sich der Besonders schweren Kriminalität widmet. § 100g StPO knüpft die laufende Protokollierung von Verkehrs- und Standortdaten an den Katalog in § 100a Abs. 2 StPO an und unterwirft den Zugriff auf zu diesem Anlass gespeicherten Vorrats- und Funkzellendaten (retrograde Verkehrsdaten; § 113b TKG; Einschränkung in § 100g Abs. 3 S. 2 StPO) seinem eigenen, streckenweise noch strengeren Straftatenkatalog in § 100g Abs. 2 StPO. Damit reagiert dieses Gesetz auf den streubreiten Eingriff, der mit der anlasslosen Vorratsdatenspeicherung verbunden ist. Die Straftatenkataloge sind in sich nicht stimmig und wirken wie Flickwerk. Besonders deutlich wird das daran, dass der Wohnungseinbruchsdiebstahl in eine dauerhaft genutzte Privatwohnung (§ 244 Abs. 4 StGB n.F.) zwar die Erhebung von Vorratsdaten erlaubt (§ 100g Abs. 2 S. 2 Nr. 1 lit. b StPO), nicht aber die deutlich niederschwelligere TKÜ.

Zunächst referiere ich die Eingriffsmaßnahmen im Hinblick auf ihre Katalogbindung (Nr. 1) und betrachte anschließend verschiedene Kriminalitätsfelder, ob sie von den drei einschlägigen Katalogen erfasst werden (Nr. 2). Das Ergebnis ist ernüchternd: Dem IuK-Strafrecht im engeren Sinne, dem mein besonderes Interesse gilt,[30] stehen allenfalls die Maßnahmen aus § 100a StPO zur Verfügung und nicht auch die Onlinedurchsuchung und der Zugriff auf Vorratsdaten. In Einzelfällen, in denen sich das IuK-mit dem klassischen Strafrecht verschränkt, kann das anders sein (BtM-Handel, sexuelle Ausbeutung u.a.).

---

[26] Zuletzt geändert durch das *Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten* vom 18.12.2015 auf der Grundlage der BT-Drs. v. 9.6.2015 – 18/5080.

[27] Im Internet veröffentlicht vom Bundesamt für Justiz unter Justizstatistiken – Telekommunikationsüberwachung.

[28] *Gesetz* ist in meinen Worten jede Rechtsnorm, die aus einem Tatbestand eine Rechtsfolge ableitet (in Anlehnung an § 7 EGStPO).

[29] *BVerfG,* Urt. v. 03.03.2004 – 1 BvR 2378/97, 1084/99, Rn. 235, 238, 241; das Gericht unterscheidet nicht danach, ob die Strafdrohung aus dem Grunddelikt oder einem besonders schweren Fall entstammt.

[30] *Kochheim*, Cybercrime und IuK-Strafrecht, 2015.

1. Katalogbindungen bei den technischen Eingriffsmaßnahmen

Die materiellen Voraussetzungen für die technischen Eingriffsmaßnahmen orientieren sich an der grundrechtsbeeinträchtigenden Schwere der Maßnahme und zeigen eine stringente Schlüssigkeit.

§ 100j Abs. 1 StPO	*Auskunft über Bestandsdaten* unter Zugriff auf die Auskunftsdaten (§§ 95, 111 TKG); keine Katalogbindung.
§ 100j Abs. 2 StPO	*Auskunft über Bestandsdaten* unter zusätzlichem Zugriff auf die *Vorratsdaten* (dynamische IP-Adressen; §§ 96, 113 TKG); keine Katalogbindung, aber Mitteilungspflichten.[31]
§ 100g Abs. 1 S. 1 Nr. 1 StPO	Protokollierung von Verkehrsdaten wegen *Straftaten*, die *nicht* die *Telekommunikation* betreffen; Bindung an den Katalog in § 100a StPO.
§ 100g Abs. 1 S. 1 Nr. 2 StPO	Rückgriff auf Vorratsdaten und Protokollierung von Verkehrsdaten wegen *Straftaten* im Zusammenhang mit der *Telekommunikation*; keine Katalogbindung, aber Ausschluss von Funkzellendaten (§ 100g Abs. 3 S. 2 StPO; sonst Bindung an den Katalog in § 100g Abs. 2 StPO).
§ 100g Abs. 1 S. 1 Nr. 1, S. 2 StPO	Rückgriff auf *Vorrats-* und *Funkzellendaten* wegen Straftaten, die *nicht* die *Telekommunikation* betreffen; Bindung an den Katalog in § 100g Abs. 2 StPO.
§ 100i StPO	IMSI-Catcher; nicht zwingende Bindung an den Katalog in § 100a Abs. 2 StPO.
§ 100a Abs. 1 S. 1 StPO	Überwachung der Telekommunikation einschließlich der Standortdaten;[32] Bindung an den Katalog in § 100a Abs. 2 StPO.
§ 100b StPO	Onlinedurchsuchung;[33] Bindung an den Katalog in § 100b Abs. 2 StPO.
§ 100c StPO	Akustische Wohnraumüberwachung; Bindung an den Katalog in § 100b Abs. 2 StPO.

2. Einzelne Kriminalitätsfelder im Spiegel der Straftatenkataloge

a) Betrugs- und Fälschungsdelikte

Seit der Reform aus 2007[34] sind die besonders schweren Formen der Betrugs- (§§ 263, 263a StGB; § 100a Abs. 2 Nr. 1n StPO) und der Fälschungsdelikte (§§ 267 bis 269 StGB; § 100a Abs. 2 Nr. 1q StPO) im Katalog des § 100a Abs. 2 StPO enthalten. Aus dem Cybercrime betrifft das besonders die Erscheinungsformen des Cardings, des Eingehungsbetruges in Bezug auf Handelsplattformen und des Phishings (Onlinebanking); in Randbereichen auch die Zahlungskartenkriminalität (Skimming).[35] Diese Deliktsformen tauchen weder in § 100b Abs. 2 noch in § 100g Abs. 2 StPO auf. Das Skimming im engeren Sinne, also das Ausspähen von Kontozugangsdaten, das noch im (strafbaren; § 149 StGB) Vorbereitungsstadium angesiedelt ist, wird vom Rückgriff auf Vorratsdaten ausgeschlossen und das schließt eine Strafverfolgung weitgehend aus. Geschädigt im strafrechtlichen Sinne werden aber nicht die Kontoinhaber, sondern die kontoführenden Banken, weil sie unautorisierte Zahlungen aus den Zahlungsdiensterahmenverträgen mit ihren Kunden aus eigenem Vermögen leisten, die nur zu einredebehafteten Erstattungsansprüchen wegen der Zahlungen und den damit verbundenen Gebühren führen (entgeltliche Geschäftsbesorgung; §§ 675f BGB ff.).

b) Erpressung

Die Drohungen mit DDoS-Angriffen und der Einsatz von Ransomware sind grundsätzlich Formen der Computersabotage im Sinne von § 303b StGB, die in Tateinheit mit Erpressung begangen werden. Das Grunddelikt nach § 253 Abs. 1 StGB ist im Katalog des § 100a Abs. 2 StPO enthalten (Nr. 1.k), nicht aber in den anderen Katalogen, was angesichts der vorgesehenen Höchstfreiheitsstrafe von 5 Jahren nicht überrascht. Die qualifizierten Formen der Erpressung im besonders schweren Fall und der räuberischen Erpressung werden hingegen in allen drei Katalogen genannt. Wenn es sich um keine Einzelfälle des Cybercrime handelt ist die Schwelle zum gewerbsmäßigen Handeln schnell erreicht (§ 253 Abs. 4 StGB), so dass bei diesen beiden Formen des Cybercrime grundsätzlich auch eine Onlinedurchsuchung und ein Zugriff auf Vorratsdaten in Betracht kommen.

c) Absatzkriminalität

Als Formen der Absatzkriminalität begreife ich besonders die Handelsplattformen in geschlossenen Boards und im Darknet, die sich dem Handel mit Betäubungsmitteln, Falschgeld, gefälschten Zahlungskarten (Carding, Skimming) und pornografischen Abbildungen widmen. Insoweit ergibt sich bei der Betrachtung der Straftatenkataloge ein uneinheitliches Bild.

Die qualifizierten Formen des BtM-Handels (§§ 29 Abs. 3 S. 2 Nr. 1, 29a, 30, 30a BtMG) drohen mit einer Höchstfreiheitsstrafe von 15 Jahren und werden in allen drei Straftatenkatalogen genannt. Der besonders schwere Fall eines Vergehens nach dem Grundstoffüberwachungsgesetz (§ 19 Abs. 3 GÜG) droht mit derselben Höchststrafe, ist aber nur im Katalog des § 100a Abs. 2 StPO enthalten, obwohl es mit den BtMG-Verbrechen kriminalistisch vergleichbar ist.

---

31 § 100j Abs. 4 StPO.

32 Die Standortdaten sind die Geodaten, die anlässlich einer laufenden Telekommunikation im Einzelfall entstehen. Dagegen sind die Funkzellendaten alle stationären Geodaten, die in einer Funkzelle während eines bestimmten Zeitrahmens entstanden sind.

33 Die *Onlinedurchsuchung light* anlässlich einer offenen Durchsuchung (§ 110 Abs. 3 StPO) kennt keine Katalogbindung.

34 Fußend auf BT-Drs. 16/5846 v. 27.6.2007.

35 Wegen der Einzelheiten: *Kochheim*, Cybercrime und IuK-Strafrecht, 2015.

Der Falschgeldhandel (§ 146 Abs. 1, Abs. 2 StGB), der Handel mit Zahlungskarten im besonders schweren Fall (§ 152a Abs. 3 StGB) und der Umgang[36] mit Zahlungskarten mit Garantiefunktion (§ 152b Abs. 1, Abs. 2 StGB) werden in den Katalogen von § 100a Abs. 2 und § 100b Abs. 2 StGB genannt, nicht aber in dem des § 100g StPO. Der Umgang mit kinderpornografischen Schriften (§ 184b Abs. 1 StGB) droht im Grunddelikt mit einer Höchstfreiheitsstrafe von 5 Jahren und wird deshalb nur in § 100a Abs. 2 StPO genannt. Der besonders schwere Fall (§ 184b Abs. 2 StGB) ist in allen drei Katalogen enthalten. Ungewöhnlich ist die Behandlung des Umgangs mit jugendpornografischen Schriften, dessen besonders schwerer Fall mit einer Höchstfreiheitsstrafe von 5 Jahren droht. Dieses qualifizierte Delikt ist im Katalog des § 100a Abs. 2 StPO enthalten und richtigerweise nicht in dem des § 100b StPO. Dessen ungeachtet wird es im Katalog des § 100g Abs. 2 StPO genannt.

d) Hehlerei und Geldwäsche

Die gewerbsmäßige und die Bandenhehlerei (§ 260 Abs. 1 Nr. 1, Nr. 2 StGB) drohen mit einer Höchstfreiheitsstrafe von 10 Jahren und sind nicht nur im Katalog des § 100a Abs. 2 StPO erfasst, sondern auch in dem des § 100b Abs. 2 StPO, nicht aber in dem des § 100g StPO. Das Verbrechen der gewerbsmäßigen Bandenhehlerei (§ 260a Abs. 1 StGB) ist in allen drei Katalogen vorgesehen. Das Grunddelikt der Geldwäsche (§ 261 Abs. 1, Abs. 2 StGB) droht im Höchstmaß mit 5 Jahren Freiheitsstrafe und wird – zutreffend – nur von § 100a Abs. 2 StPO genannt. Dagegen ist die Geldwäsche im besonders schweren Fall in allen drei Katalogen enthalten (§ 261 Abs. 1, Abs. 2, Abs. 4 StGB).

Die Hehlerei betrifft im Zusammenhang mit dem Cybercrime besonders die Carding-Foren, in denen betrügerisch erlangte Waren verbreitet werden und auch das Auftrags-Carding angeboten wird. Dabei handelt es sich um eine besondere Spielart des Betruges, bei dem der Carder (der „etwas mit Karten macht“) eine Bestellung von Waren, Eintrittskarten, Fahrkarten und anderen online angebotenen Diensten entgegennimmt, sie mit ausgespähten Kartendaten ausführt und sich dafür vom Besteller bezahlen lässt, nachdem er die Ware in einer Packstation, einem Hausdrop[37] oder einem anderen Übermittlungsweg empfangen hat. Die Geldwäsche hat im Cybercrime einen festen Platz. Ihre Zwischenstationen reichen von Online-Casinos über Verrechnungssysteme wie E-Gold, Webmoney und Wechselstuben (Currencies) sowie Kryptowährungen wie Bitcoin bis hin zu Bankdrops,[38] zu denen nicht nur unter falschen oder ausgespähten Personalien eingerichtete Bankkonten und der Bargeldtransfer, sondern auch die ohne Identitätsprüfung gewährten Kreditkarten auf Guthabenbasis gehören.

Die unterschiedliche Behandlung der besonders schweren Kriminalitätsformen in den einschlägigen Straftatenkatalogen zeigt sich am Beispiel der Hehlerei besonders deutlich. Die Onlinedurchsuchung als eine der beiden tiefsten Grundrechtseingriffe des Strafverfahrensrechts ist zugelassen, der Zugriff auf Vorratsdaten als dagegen geringerer persönlicher Eingriff hingegen nicht. Das passt nicht zusammen.

e) Kriminelle Vereinigung und Volksverhetzung

Die Gründung einer kriminellen Vereinigung und die Mitgliedschaft in ihr gehören zur schweren Kriminalität und sind bei einer Höchstfreiheitsstrafe von 5 Jahren (§ 129 Abs. 1 S. 1 StGB) im Katalog des § 100a StPO enthalten. Dagegen ist die Unterstützung einer kriminellen Vereinigung, für die das Gesetz mit 3 Jahren Höchstfreiheitsstrafe droht (§ 129 Abs. 1 S. 2 StGB), allenfalls der erheblichen Kriminalität zuzurechnen und dennoch im Straftatenkatalog des § 100a Abs. 2 StPO enthalten. Der Widerspruch setzt sich fort: Die kriminelle Vereinigung in Bezug auf eine Katalogtat des § 100b Abs. 2 StPO mit einer Höchstfreiheitsstrafe von 5 Jahren befindet sich in allen drei Katalogen. Dasselbe gilt für die Volksverhetzung (§ 130 StGB[39]), die mit einer Höchstfreiheitsstrafe von 5 Jahren droht und nur in dem Katalog des § 100a Abs. 2 StPO aufgeführt wird.

f) Kritische Infrastrukturen

Ganz kritisch wird es bei dem Thema Kritische Infrastrukturen. Dazu gehören durchweg Verbrechen mit einer Mindestfreiheitsstrafe von 1 Jahr und zweistelligen Höchststrafen, beginnend bei der Brandstiftung (§ 306 StGB) und der Herbeiführung einer Kernenergieexplosion (§ 307 StGB) über den Missbrauch ionisierender Strahlen (§ 309 StGB) und der vorsätzlichen Herbeiführung einer Sprengstoffexplosion (§ 308 StGB) bis hin zur Vorbereitung eines Explosions- oder Strahlungsverbrechens (§ 310 Abs. 1 StGB) und der Herbeiführung einer gemeingefährlichen Vergiftung (§ 314 StGB). Alle sechs Beispiele lassen eine TKÜ und den Zugriff auf Vorratsdaten zu, aber keine Onlinedurchsuchung.

Dabei sind alle sechs Deliktsformen typische Beispiele für ein besonders gefährliches Hacking gegen industrielle Anlagensteuerungen, das im Profitinteresse, aus kriegerischen Motivationen oder schlicht aus Wettbewerbsgründen ausgeführt wird. Das hat der Gesetzgeber übersehen

---

36 Ich spreche im Anschluss an § 1 Abs. 3 WaffG vom *Umgang*, wenn das Gesetz mehrere Begehensformen wie Besitz, Verschaffen usw. kennt und es auf die einzelne Begehensform bei der Diskussion nicht ankommt.

37 Der *Hausdrop* ist eine Zustelladresse für Post- und Paketsendungen eines Warenagenten, der sich dazu zur Verfügung stellt, oder ein ungenutzter Briefkasten in einem Mehrfamilienhaus (der sich für Warensendungen nur eingeschränkt nutzen lässt). Besser geeignet sind Paketstationen – auch fremde, die gehackt wurden – oder vorübergehend angemietete Wohnungen.

38 Die frühe Form davon war der *Mule Account*, also das „Eselskonto“ eines Finanzagenten, der im Endeffekt auf dem Schaden sitzenblieb und bestraft wurde. *Bankdrops* werden hingegen von Tätern mit falschen oder ausgespähten Personalien eingerichtet und dann genutzt oder verkauft. Geläufig ist auch die Methode, dass arbeitssuchende Ausländer mehrere Bankkonten einrichten und dem Vermittler in der Erwartung einer baldigen Arbeitsstelle zur Nutzung überlassen, der sie seinerseits verkaufen kann. Vor einigen Jahren brachte das bis zu 1.500 € pro Bankdrop.

39 Zuletzt maßgeblich geändert durch das 49. StrÄndG v. 21.1.2015.

und einen vielleicht drohenden Cyberwar unbeachtet gelassen.

3. Fazit

Die Betrachtung der Straftatenkataloge unter dem Gesichtspunkt des Cybercrime zeigt bereits Lücken im weitreichenden Katalog des § 100a StPO, mit denen die Strafverfolgung leben kann. Dass der Große Lauschangriff und die Onlinedurchsuchung gleichbehandelt werden und ihr Katalog in § 100b StPO nicht immer stringent ist, sei dahingestellt. Ärgerlich sind hingegen die klaffenden Lücken im Katalog des § 100g Abs. 2 StPO. Die anlasslose Speicherung von Verkehrsdaten ist ein streubreiter Eingriff in Grundrechte, daran besteht kein Zweifel. Der Zugriff auf Vorratsdaten ist jedoch unterhalb der Schwelle zum Großen Lauschangriff und der Onlinedurchsuchung angesiedelt, weil die Vorratsdaten keine Inhaltsdaten sind (die schon im Wege der TKÜ abgegriffen werden dürfen) und auch die Geodaten (Funkzellendaten) nur einen begrenzten Eingriff gegen die persönliche Lebensführung darstellen, weil sie Bewegungsprofile ermöglichen, ohne jedoch die Tiefe von Inhaltsdaten zu erreichen. Dadurch entsteht eine Unwucht, die wegen der Vorratsdaten wie eine rechtsstaatswidrige Einschränkung der verfassungsrechtlich gebotenen Strafverfolgung wirken kann.[40]

Welchen Bestand die Vorratsdatenspeicherung haben wird, ist unklar. Am 1.7.2017 hätten die Zugangsprovider in den Echtbetrieb übergehen müssen (§ 150 Abs. 13 S. 1 TKG). Die zur Überwachung der Umsetzung zuständige Bundesnetzagentur hat aber Ende Juni 2017 alle Maßnahmen zur Durchsetzung der Speicherpflicht ausgesetzt[41] und damit auf die Entscheidung des *OVG Münster* vom 22.6.2017 reagiert,[42] wonach die gesetzliche Verpflichtung unionsrechtswidrig sei. Das *OVG* folgt damit einer Entscheidung des *EuGH*,[43] wonach die europarechtliche Datenschutzrichtlinie einer anlasslosen Vorratsdatenspeicherung entgegen stehe. Der *EuGH* und ihm folgend das *OVG Münster* verlangen von der Speicherpflicht besonders auch, dass sie von vornherein auf bestimmte Personengruppen oder Regionen beschränkt wird und jedenfalls nicht flächendeckend sein darf. Die Forderungen des *EuGH* sind unter verfassungsrechtlicher Betrachtung nicht unproblematisch. Bereits die Speicherpflicht stellt einen äußerst streubreiten Grundrechtseingriff dar, der nur durch strenge Zugriffsregeln gerechtfertigt werden kann.[44] Mit der inhaltlichen Bewertung der Vorratsdaten bei ihrer Auswahl würde ein weiterer, vergleichbarer streubreiter Eingriff eingerichtet, der nach der Spruchlinie des *BVerfG* nicht zulässig wäre. Das *BVerfG* hat sich unlängst zu der Frage geäußert, ob die Speicherpflichten gegen die Berufsfreiheit nach Art. 12 GG verstoßen und die entsprechenden Verfassungsbeschwerden nicht zur Entscheidung angenommen,[45] weil die Speicherpflichten nicht dem Zugang zum Beruf, sondern der Berufsausübung dienen. Das signalisiert, dass das nationale Verfassungsrecht der aktuellen Gesetzesfassung nicht entgegensteht. Die europarechtliche Betrachtung bleibt offen und ich kann mir gut vorstellen, dass an dieser Stelle noch ein interessanter Konflikt ansteht.

III. Verwertungsbeschränkungen und -verbote

Erhebungsverbote und Verwertungsbeschränkungen folgen aus den einschlägigen Gesetzen oder nach übergeordneten verfassungsrechtlichen Maßgaben. Nr. 1 befasst sich deshalb mit den verfassungsrechtlichen Verwertungsverboten, die zunächst von der Staatsanwaltschaft[46] und abschließend vom Gericht zu beachten sind. Nr. 2 betrachtet sodann die Erhebungs- und Verwertungsverbote in der Strafprozessordnung. Jedenfalls wegen der „Zweitverwertung“ in anderen strafrechtlichen Verfahren oder anderen Verfahrensordnungen gelten die Grundsätze des hypothetischen Ersatzeingriffs (Nr. 3), der seine besonderen Ausformungen an verschiedenen Stellen der Strafprozessordnung gefunden hat. Unter Nr. 4 wird schließlich der von der Rechtsprechung entwickelte Spurenansatz behandelt, der jedenfalls dem Freibeweis im Zusammenhang mit Daten aus Ermittlungsmaßnahmen unter den Schranken des § 100a Abs. 2 StPO zugänglich ist.

1. Verwertungsverbote mit übergeordneter Bedeutung

Die Frage nach den Beweisverwertungsverboten folgt im Wesentlichen der Generalklausel in § 261 StPO für die richterliche Überzeugungsbildung nach Abschluss der Beweisaufnahme im Urteil.[47] Durchgreifende Verwertungsverbote folgen aus der Missachtung des Richtervorbehalts,[48] aus nachhaltig willkürlichen Verfahrenshandlungen[49] oder solchen, die schwerwiegend gegen das Gebot der Fairness verstoßen.[50] Schlichte Fehler in der Rechtsanwendung oder eine unzureichend begründete Eingriffsentscheidung reichen dazu nicht aus.[51] Somit gilt laut *BGH*: [52] „Ein Verwertungsverbot kann … nur verfassungsrechtlicher Natur sein und kommt nur bei ausdrücklicher gesetzlicher Anordnung oder aus übergeordneten wichtigen Gründen im Einzelfall in Betracht.“
Dem folgt auch das *BVerfG*:[53] „Die Annahme eines Verwertungsverbots schränkt … eines der wesentlichen Prinzipien des Strafverfahrensrechts ein, nämlich den Grundsatz, dass das Gericht die Wahrheit zu erforschen und dazu die Beweisaufnahme von Amts wegen auf alle hierfür bedeutsamen Tatsachen und Beweismittel zu erstrecken hat. Daran gemessen bedeutet ein Beweisverwertungsverbot eine Ausnahme, die nur nach ausdrücklicher

40 *BVerfG,* Urt. v. 2.3.2006 – 2 BvR 2099/04, Rn. 98; *BVerfG,* Beschl. v. 18.3.2009 – 2 BvR 2025/07, Rn. 16.
41 Bundesnetzagentur, Verkehrsdatenspeicherung, Stand 28.6.2017.
42 *OVG Münster,* Beschl. v. 22.6.2017 – 13 B 238/17.
43 *EuGH,* Urt. v. 21.12.2016 – C-203/15 und C-698/15 – „Tele2 Sverige AB und Watson“.
44 *BVerfG,* Urt. v. 2.3.2010 – 1 BvR 256/08, 263/08, 586/08, Leitsätze 2 ff.
45 *BVerfG,* Beschl. v. 28.9.2017 – 1 BvR 847/16, 1 BvR 1560/16.
46 *BGH,* Beschl. v. 23.8.2011 – 1 StR 153/11, Rn. 18; *BVerfG*, Urt. v. 19.3.2013 – 2 BvR 2628, 2883/10, 2155/11, Rn. 93.
47 Der Angeklagte hat keinen Anspruch auf einen Zwischenbescheid: *BVerfG,* Beschl. v. 18.3.2009 – 2 BvR 2025/07, Rn. 13 ff.
48 *BGH,* Beschl. v. 30.8.2011 – 3 StR 210/11, Rn. 8.
49 *BVerfG,* Beschl. v. 9.11.2010 – 2 BvR 2101/09, Rn. 50.
50 *BVerfG,* Beschl. v. 15.10.2009 – 2 BvR 2438/08, Rn. 7.
51 *BGH,* Beschl. v. 18.1.2011 – 1 StR 663/10, Rn. 22, 25.
52 *BGH,*Urt. v. 20.12.2012 – 3 StR 117/12, Rn. 33 m.w.N.
53 *BVerfG,* Beschl. v. 24.2.2011 – 2 BvR 1596, 2346/10, Rn. 10.

gesetzlicher Vorschrift oder aus übergeordneten wichtigen Gründen im Einzelfall anzuerkennen ist…“ In einer etwas jüngeren Entscheidung heißt es dann:[54] „Grundrechtsverletzungen, zu denen es außerhalb der Hauptverhandlung gekommen ist, führen daher nicht zwingend dazu, dass auch das auf dem Inbegriff der Hauptverhandlung beruhende Strafurteil gegen Verfassungsrecht verstößt. Aus verfassungsrechtlicher Sicht ist ein Beweisverwertungsverbot geboten, wenn die Auswirkungen des Rechtsverstoßes dazu führen, dass dem Angeklagten keine hinreichenden Möglichkeiten zur Einflussnahme auf Gang und Ergebnis des Verfahrens verbleiben, die Mindestanforderungen an eine zuverlässige Wahrheitserforschung nicht mehr gewahrt sind oder die Informationsverwertung zu einem unverhältnismäßigen Eingriff in das allgemeine Persönlichkeitsrecht führen würde. Zudem darf eine Verwertbarkeit von Informationen, die unter Verstoß gegen Rechtsvorschriften gewonnen würden, nicht bejaht werden, wo dies zu einer Begünstigung rechtswidriger Beweiserhebungen führen würde. Ein Beweisverwertungsverbot kann daher insbesondere nach schwerwiegenden, bewussten oder objektiv willkürlichen Rechtsverstößen, bei denen grundrechtliche Sicherungen planmäßig oder systematisch außer Acht gelassen worden sind, geboten sein.“

Demzufolge stellen sich drei Fragen:

1. Welche gesetzlichen Erhebungs- und Verwertungsverbote kennt die StPO? Sie schließen die aktuelle Verwertung der gewonnenen Erkenntnisse aus, die dann denklogisch auch nicht zu anderen Zwecken verwendet werden dürfen.[55]

2. Greift das Institut des hypothetischen Ersatzeingriffes zugunsten des Folgeverfahrens? Insoweit muss das Doppeltürmodell des *BVerfG* – jedenfalls für den Vollbeweis – sowohl den Export als auch den Import bei gleichzeitiger Schwellengleichheit zulassen.

3. Gibt es Anwendungsfälle, in denen auch eine nicht schwellengleiche Verwertung möglich ist?

3a. Nach der Änderung des rechtlichen Gesichtspunktes bleibt die gewonnene Erkenntnis weiterhin verwertbar. Das gilt etwa für die TKÜ, die zum Beispiel wegen des Verdachts eines besonders schweren Falles des Betruges zunächst zulässig war, der sich nach den weiteren Ermittlungen als „normaler“ Betrug darstellt, der keine TKÜ gerechtfertigt hätte.[56] Das gilt auch für weitergehende Ermittlungen in demselben Verfahrenskomplex, der demselben Lebenssachverhalten zugehört.

3b. Der Spurenansatz lässt zudem die Verwertung von Erkenntnissen auch in niedrigerschwelligen Folgeverfahren zu, solange sie nur im Freibeweis verwendet werden (lit. d).

2. Erhebungs- und Verwertungsgrenzen in der StPO

Dem Institut des hypothetischen Ersatzeingriffes folgend (unten lit. c) wurden 2007 mit dem § 161 Abs. 2 StPO (Import von personenbezogenen Daten nach Maßgabe der Schwellengleichheit) und dem § 477 Abs. 2 S. 2, S. 3 StPO (Export in andere Strafverfahren und andere Verfahrensordnungen) die beiden grundlegenden Verwertungsgrenzen in das Strafverfahren eingeführt. Für sie gilt – vereinfacht – der Grundsatz, dass Erkenntnisse aus dem einen Verfahrensrecht nur dann in dem anderen Verfahrensrecht verwertet werden dürfen, wenn ihre Erhebung dort ebenfalls zulässig gewesen wäre (Schwellengleichheit). Ausschlaggebend ist der Zeitpunkt des Eingriffs. Die Verwertung von Zufallsfunden stellt einen erneuten Eingriff dar, so dass wegen der Geltung des Verfahrensrechts auf den Zeitpunkt der „Zweitverwertung“ abzustellen ist.[57]

Das klassische Verwertungsverbot in der Strafprozessordnung bestimmt § 136a StPO: Die Aussage eines Beschuldigten – und das ist nicht schon jeder Verdächtige[58] – ist unter keinen Umständen verwertbar, wenn sie unter dem Einsatz verbotener Vernehmungsmethoden zustande gekommen ist. An die Zeugnisverweigerungsrechte (§§ 52 bis 53a StPO) der Angehörigen und der Berufshelfer knüpfen die Beschlagnahmeverbote in § 97 Abs. 1 StPO und das Verwertungsverbot in § 108 Abs. 2 StPO an (ärztliche Aufzeichnungen über einen Schwangerschaftsabbruch). Außerdem verbietet § 160a StPO grundsätzlich Ermittlungsmaßnahmen gegen Berufsgeheimnisträger, wenn sie nicht an der Straftat ihres Auftraggebers oder am Beuteabsatz beteiligt sind. Darüber hinaus bestimmen die §§ 100d Abs. 5 und 100g Abs. 4 StPO Erhebungsverbote in Bezug auf eine Onlinedurchsuchung, eine Akustischen Wohnraumüberwachung oder beim Zugriff auf Vorratsdaten, wenn die Erkenntnisse von einem Berufshelfer erlangt wurden (Löschpflicht), allerdings mit einer Öffnungsklausel in § 100d Abs. 5 S. 2 StPO nach einer eingegrenzten Verhältnismäßigkeitsprüfung.
§ 100e Abs. 6 StPO nimmt die §§ 100b und 100c StPO auf und lässt die Verwertung von personenbezogenen Daten in anderen Strafverfahren nur zu, wenn sie ebenfalls Straftaten aus dem Katalog des § 100b Abs. 2 StPO betreffen (Nr. 1). Dasselbe gilt für personenbezogene Daten, die aufgrund einer polizeirechtlichen Onlinedurchsuchung oder einer Akustischen Wohnraumüberwachung

---

54 *BVerfG,* Beschl. v. 7.12.2011 – 2 BvR 2500/09, 1857/10, Rn. 117.

55 Ein Sonderfall kann darin bestehen, dass die Verwertung im Ausgangsverfahren zwar unzulässig ist, im Folgeverfahren hingegen nicht. Nach der Spruchlinie des BVerfG ist die Verwertung im – sozusagen höherwertigem – Folgeverfahren zulässig: *BVerfG,* Beschl. v. 7.12.2011 – 2 BvR 2500/09, 1857/10. Soweit Löschpflichten bestehen ist noch offen, ob die Löschpflicht Vorrang vor der Weitergabe an das höherwertige Verfahren hat. In der Tradition der Verfassungsrechtsprechung werden im Einzelfall die verschiedenen Verfassungsziele gegeneinander abgewogen werden müssen.

56 *BGH,* Urt. v. 30.8.1978 – 3 StR 255/78, Leitsätze. Die gesetzliche Grundlage dafür liefert § 265 Abs. 2 StPO, wonach das Gericht bei geänderter Sachlage zwar einer Hinweispflicht unterliegt, nicht aber in der Beweisverwertung beschränkt wird.

57 *BGH,* Urt. v. 27.11.2008 – 3 StR 342/08, Rn. 13.

58 „Die Strafverfolgungsbehörden haben einen Zeugen erst dann als Beschuldigten zu behandeln, wenn sich der Verdacht gegen ihn so verdichtet hat, dass der Zeuge ernstlich als Täter der untersuchten Straftat in Betracht kommt“; *BGH,* Beschl. v. 7.9.2017 – 1 StR 186/17, S. 3.

erlangt wurden, für die Verwertung in einem Strafverfahren (Nr. 3). Sowohl § 161 Abs. 3 als auch § 100e Abs. 6 Nr. 2 StPO erlauben umgekehrt die polizeiliche Nutzung von im Strafverfahren erhobenen Daten, wenn die Gefahrenabwehr besonders hochrangige Schutzgüter betrifft. Das Gesetz folgt somit den Anforderungen des *BVerfG*, das im Hinblick auf die Verkehrsdaten verlangt hat, dass sie nicht schon für die Gefahrenvorsorge, sondern erst für die konkretisierte Gefahrenabwehr erhoben und eingesetzt werden dürfen.[59]

3. Hypothetischer Ersatzeingriff

Diese besonderen Regelungen entsprechen dem vom *BVerfG* entwickelten Doppeltürmodell:[60] „Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten."

Gedanklich fußt es im hypothetischen Ersatzeingriff, der aber nur nach der Schwellengleichheit der hypothetischen Eingriffsmaßnahme fragt, und nicht auch danach, ob der Export aus dem Verfahren (zum Beispiel § 477 Abs. 2 StPO) und der Import aus einem anderen Verfahren erlaubt sind (zum Beispiel § 161 Abs. 2 StPO). Damit greift das Doppeltürmodell die Zweckänderung der Datenerhebung auf, wenn es darum geht, ob Erkenntnisse vollbeweislich zur gerichtlichen Überzeugungsbildung oder in anderen Verfahren oder Verfahrensordnungen genutzt werden dürfen. Seine grundlegende Gestalt hat das *BVerfG* schon 2009 beschrieben: „Ist eine Maßnahme nach [der StPO] nur bei Verdacht bestimmter Straftaten zulässig, so dürfen die auf Grund einer solchen Maßnahme erlangten personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen zu Beweiszwecken in anderen Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz hätte angeordnet werden dürfen."[61]

Folgender Gedanke ist tragend: „Entscheidend ist, dass ein Ermittlungsrichter bei hypothetischer Betrachtung einen entsprechenden richterlichen Durchsuchungsbeschluss auf strafprozessualer Grundlage zweifelsfrei erlassen hätte."[62]

Bemerkenswert ist die Einschränkung, die das *BVerfG* vornimmt, wenn es von „zu Beweiszwecken" spricht. Im Strafverfahrensrecht erfolgt die Beweisaufnahme grundsätzlich in der Hauptverhandlung vor dem erkennenden Tatsachengericht (§ 244 Abs. 1 StPO). Hier gilt der Strengbeweis nach Maßgabe der Vorschriften über die Beweisaufnahme. Nach ihrem Abschluss entscheidet das Gericht abschließend nach dem Grundsatz der freien richterlichen Beweiswürdigung (§ 261 StPO). Verfahrensleitende Entscheidungen unterliegen hingegen dem Freibeweis, der keine strengen Förmlichkeiten kennt und nicht mit der Beschwerde angegriffen werden kann (§ 305 StPO). Darauf spricht auch das *BVerfG* an, wenn es dem Angeklagten das Recht auf einen Zwischenbescheid über ein Verwertungsverbot abspricht;[63] um sich eine Überzeugung bilden zu können, muss sich das Gericht alle erreichbaren, zulässigen und sinnvollen Beweise (Erkenntnisse) verschaffen, um schließlich in einer Gesamtschau die Beweise einzeln und in ihrem Zusammenwirken zu bewerten.

4. Spurenansatz

Verwertungsbeschränkte Beweise und Spuren können als Zufallsfunde (§ 108 Abs. 1 StPO) grundsätzlich bei der Freibeweisführung dazu herangezogen werden, um andere (zulässige) Beweiserhebungen zu begründen. Das hat der *BGH* wegen der TKÜ-Erkenntnisse zunächst mit einer Einschränkung ausgeführt: Die Nichtkatalogstraftat muss im Sinne derselben prozessualen Tat mit der Anlasstat für die Maßnahme verbunden sein.[64] Dem ist das *BVerfG* im Hinblick auf die TKÜ gefolgt.[65] Maßgeblich ist jedoch die – hier polizeirechtliche – Zweckbindung, die der rechtmäßigen Datenerhebung zugrunde gelegen hat.[66] Dem folgend hat der *BGH* die freibeweisliche Verwertung von Spuren auch nach der Maßgabe neuerer gesetzlichen Verwertungsschranken als zulässig angesehen[67] und der Gesetzgeber legt diesen Maßstab den allgemeinen Verwertungsregeln in den §§ 161 Abs. 2 und 477 Abs. 2 S. 2, S. 3 StPO zugrunde.[68] Das kann allerdings nicht wegen der personenbezogenen Daten aus einer Akustischen Wohnraumüberwachung oder einer Onlinedurchsuchung gelten, weil das *BVerfG* in diesen Fällen die Anwendung des Spurenansatzes im Zusammenhang mit Nichtkatalogtaten ausschließt.[69]

Zu unterscheiden ist danach zwischen den Eingriffsmaßnahmen, hier im Wesentlichen die TKÜ nach § 100a StPO, und den besonders tiefen Eingriffsmaßnahmen nach den §§ 100b und 100c StPO. Nach den verfassungsrechtlichen Grenzen, die das *BVerfG* gezogen hat, sind die Verwertungsregeln in § 100e Abs. 6 StPO entsprechend der Eingriffstiefe der Erstmaßnahme wegen des Spurenansatzes streng auszulegen: Der Spurenansatz gilt jedenfalls nicht, wenn die personenbezogenen Daten entweder aus einer Onlinedurchsuchung oder einer Akustischen Wohnraumüberwachung stammen und die weitere Strafverfolgung – im Sinne derselben prozessualen Tat – keinen Bezug zur Erstmaßnahme hat.

Die dogmatische Schranke, die das *BVerfG* 2009 einge-

59 *BVerfG,* Beschl. v. 24.1.2012 – 1 BvR 1299/05, Rn. 157.
60 *BVerfG,* Beschl. v. 24.1.2012 – 1 BvR 1299/05, Rn. 123.
61 *BVerfG,* Beschl. v. 18.3.2009 – 2 BvR 2025/07, Rn. 18.
62 *BGH,* Urt. v. 26.4.2017 – 2 StR 247/16, Rn. 40.
63 *BVerfG,* Beschl. v. 18.3.2009 – 2 BvR 2025/07, Rn. 13 ff.
64 *BGH,* Beschl. v. 18.3.1998 – 5 StR 693/97, Rn. 9.
65 *BVerfG,* Beschl. v. 29.6.2005 – 2 BvR 866/05, Rn. 4.
66 *BVerfG,* Urt. v. 20.4.2016 – 1 BvR 966/09, 1140/09, Rn. 281, 283.
67 *BGH,* Urt. v. 14.8.2009 – 3 StR 552/08, Leitsatz 2; so auch *OLG Hamm,* Urt. v. 8.8.2013 – 1 RVs 58/13, Rn. 20, 21.
68 BT-Drs. 16/5846 v. 27.6.2007 – 16/5846, S. 64, 66.
69 *BVerfG,* Urt. v. 20.4.2016 – 1 BvR 966/09, 1140/09, Rn. 301, 313, 316 (BKA-Gesetz). Diese Position hat das *BVerfG* auch schon ausdrücklich wegen der Akustischen Wohnraumüberwachung vertreten: *BVerfG,* Urt. v. 3.3.2004 – 1 BvR 2378/98, 1084/99, Rn. 339.

führt hat, indem es die Verwertungsgrenzen auf „zu Beweiszwecken" beschränkte, folgt den Wortlauten in den §§ 161 und 477 StPO (seit 2007). Mit der Rechtsprechungslinie, die anhand der Erkenntnisse aus einer TKÜ entwickelt wurde, kommt der Spurenansatz im Hinblick auf die personenbezogenen Daten aus einer TKÜ oder einer Quellen-TKÜ weiterhin zum Zuge, wenn es um die Verfolgung von Nichtkatalogtaten geht.

Eine besondere Rolle spielt die Verwertung von Verkehrsdaten nach § 100g StPO. Auf § 100g StPO geht § 101a Abs. 5 StPO näher ein und unterwirft jedenfalls die Vorratsdaten einer Verwertungsschranke mit Katalogbindung an § 100g Abs. 2 StPO. Wegen der Verkehrsdaten unterscheidet § 100g jedoch zwischen den technisch veranlassten Verkehrsdaten (§§ 96, 100 TKG), auf die nach Maßgabe des § 100a Abs. 2 StPO oder wegen Straftaten zugegriffen werden darf, die die Telekommunikation betreffen, und die Vorrats- sowie die Standortdaten (§ 113b TKG), die der Katalogbindung des § 100g Abs. 2 StPO unterliegen.

Danach ergibt sich ein für den Spurenansatz klares Bild, das nur von dem unzureichenden Straftatenkatalog des § 100g Abs. 2 StPO getrübt wird: Personenbezogene Erkenntnisse, die beim Erstzugriff unter den Schranken des § 100a Abs. 2 StPO erhoben wurden, können im Wege des Spurenansatzes auch für Beweiserhebungen zu Nichtkatalogtaten (freibeweislich) verwertet werden, wenn nicht nur ein innerer Tatbezug zum Ausgangsverdacht besteht (prozessuale Tat), sondern die Erkenntnisgewinnung als solche rechtmäßig war. Der Spurenansatz ist hingegen ausgeschlossen, wenn der Erstzugriff nur unter den strengeren Voraussetzungen der Kataloge in § 100b Abs. 2 oder § 100g Abs. 2 StPO zulässig war.