Verdeckte Ermittlungen im Internet

Dieter Kochheim

Strafverfahrensrechtliche Voraussetzungen und Grenzen
beim Einsatz von Überwachungstechnik und
bei verdeckten Ermittlungen
zur Bekämpfung der Cybercrime

Thema:	**Verdeckte Ermittlungen im Internet**
Autor:	Dieter Kochheim
Version:	1.20
Stand:	07.03.2012
Cover:	„Drei Damen“ (Vilnius, Litauen, 2003), D. Kochheim
Impressum:	**CF**, cyberfahnder.de

5 **Einleitung**

9 **1. Internet und Strafverfahrensrecht**

10 1.1 Gefahrenabwehr und Strafverfahren

11 1.2 Dokumentation und Auswertung

13 1.3 Geltung des Strafverfahrensrechts

14 **2. Grundrechte und Eingriffsmaßnahmen**

14 2.1 Telekommunikationsgeheimnis

15 2.2 informationelle Selbstbestimmung

16 2.3 Integrität informationstechnischer Systeme

17 2.4 Wohnung

17 2.5 Internetermittlungen und Grundrechte

20 **3. Ermittlungsmethoden**

20 3.0.1 tatsächlichen Anhaltspunkte (§ 152 Abs. 2 StPO) für eine Straftat

20 3.0.2 welche Straftat kommt in Betracht?

20 3.0.3 Wahl der Mittel

21 3.0.4 Eilbedürftigkeit

21 3.0.5 materielles Cybercrime-Strafrecht

22 Tatbestände der Cybercrime

23 Strafrahmenübersicht

25 **Eingriffsmaßnahmen**

26 **3.1 Auskünfte und Sachbeweise**

26 3.1.1 Auskünfte von Behörden und anderen Einrichtungen

27 3.1.2 Bestandsdaten

27 3.1.3 Verkehrsdaten und Dateien in Mobilgeräten

28 3.1.4 Verkehrsdaten und Funkzellendaten

29 3.1.5 Staatsanwaltschaftliches Auskunftsersuchen

30 3.1.6 Herausgabeersuchen

31 3.1.7 Beschlagnahme

31 3.1.8 Beschlagnahme von E-Mails

33 3.1.9 Beschlagnahme von Dateien beim Hostprovider

33 3.1.10 Ferndurchsuchung. Fernzugriff

35 **3.2 technische Mittel**

36 3.2.1 technische Observationshilfen

38 3.2.2 Überwachung der Telekommunikation

40 3.2.3 IMSI-Catcher

40 3.2.4 Serverüberwachung

40 3.2.5 Quellen-TKÜ

41 3.2.6 Onlinedurchsuchung

42 3.2.7 Quellen-Zugriff auf nicht kommunikative Aktivitäten

42 3.2.8 Spyware

43 **3.3 personale Ermittlungen**

44 3.3.1 verdeckte personale Ermittlungen

45 3.3.2 Grenzen zwischen VP und NoeP

48 3.3.3 Verdeckter Ermittler im gewalttätigen Umfeld

49 3.3.4 Beobachtungen und Kommunikation bei Internetermittlungen

51 3.3.5 Scheinkauf

51 3.3.6 Keuschheitsprobe

52 **Anhang**

53 **A.1 Staatsanwaltschaft und Strafverfolgung**

53 **A.2 Verhältnis zur Polizei**

54 **A.3 Verfahren der Strafrechtspflege**

54 A.3.1 Vorfeldermittlungen

54 A.3.2 Vorermittlungen

55 A.3.4 unbekannte Täter

55 A.3.5 bekannte Täter

56 **A.4 Eingriffsrechte während der Vorermittlungen**

57 A.4.1 Vorermittlungen nach der StPO

57 A.4.2 Prävention und Vorfeld

58 A.4.3 beobachtete Erscheinungsformen

58 A.4.4 Initiativermittlungen

58 A.4.5 Ermächtigung zu Vorermittlungen

60 A.4.6 Merkwürdigkeiten

60 A.4.7 Eingriffsrechte im Stadium der Vorermittlungen

61 A.4.8 Fazit

62 **A.5 Geltung von Beweisen und Erfahrungen**

63 A.5.1 Geltung

64 A.5.2 Geltung und Wechselwirkungen

65 A.5.3 Kategorisierung des Geltungsgrades

65 A.5.4 Bewertung von Beweisen und Erfahrungssätzen

67 **B. Hintergrund: Carding-Boards**

Einleitung [1]

Kriminalität als breite Erscheinung im Internet wird immer stärker wahrgenommen, wobei die Alltagsdelikte und ihre Erscheinungsformen auch die Öffentlichkeit bewegen. Das betrifft vor Allem die Sicherheit des Onlinebankings (Phishing) und den Missbrauch von ausgespähten Daten von Zahlungskarten (Skimming [2]). Beide Kriminalitätsformen haben verschiedene Gestaltungen und sind Teil eines Phänomens, das insgesamt als **Identitätsdiebstahl** diskutiert wird. Er richtet sich gegen die persönlichen Daten anderer, die mit technischen Mitteln (Malware, Hacking, Kameras, technische Eingabegeräte) oder sozialen Techniken (Social Engineering, Beobachtung, persönliches Aushorchen [3]) ausgespäht, kombiniert, verbreitet und schließlich betrügerisch missbraucht werden. Betroffen sind nicht nur Bankkonten [4], sondern jede Art von persönlichen Präsenzen im Internet, also Verkaufsplattformen (zum Beispiel eBay), Warenkonten (zum Beispiel bei Amazon und Kaufhäusern), Webauftritte [5], Netzdienste (Verwaltung von Paketstationen) und schließlich die persönlichen Präsentationen in sozialen Netzen.

Die Marktplätze dafür liefern vor Allem die seit rund zehn Jahren in Erscheinung getretenen Hackerboards, die sich meistens bereits durch ihren DNS-Namen [6] zu erkennen geben, weil er Abwandlungen des Wortes „Carding“ enthält (carders, cardersplanet) [7]. Carding steht für den kriminellen Umgang mit Kartendaten. In den einschlägigen Boards wurden zunächst nur ausgespähte Kartendaten zum Kauf oder zur Verwendung auf Kommission angeboten und erworben. Die Angebote erweiterten sich schnell und umfassen seither gefälschte Personalpapiere, Führerscheine, Hochschuldiplome, Fälschungswerkzeuge einschließlich WhitePlastics, Prägemaschinen, Drucker und Schreibgeräte für Zahlungskarten, Skimmer [8], Malware für jeden Zweck, Exploits [9], Rootkits [10] und schließlich funktionstüchtige Botnetze zur Miete [11].

Hackerboards dieser Art sind geschlossene Kom-

---

1 Die blau gefärbten Texte (mit Ausnahme der Überschriften) sind mit Links zu den Quellen im Internet unterlegt.

Wörtliche Zitate werden in Kursivschrift und ohne Anführungszeichen wiedergegeben.

2 Das Skimming zeigt Besonderheiten dadurch, dass die wichtigsten Tatteile in dem Fälschen und Gebrauchen von Zahlungskarten mit Garantiefunktion besteht (§§ 152a, 152b StGB). Alle Einzelheiten werden in meinem Arbeitspapier beschrieben: Dieter **Kochheim,** Skimming #3 (Stand: März 2012).

3 Einen Überblick auf dem Stand vom Sommer 2010 gibt mein Arbeitspapier: Dieter **Kochheim**, Cybercrime (24.05.2010)

4 Neben traditionellen Bankkonten auch modernere Transfersysteme wie PayPal uva.

5 Das betrifft nicht nur das Defacement, also die offensichtliche Verschandelung einer Webseite durch einen Eindringling, sondern vor allem auch die Einbindung von iFrames oder direkt von Schadcote, mit denen Malware auf den Geräten der Besucher installiert wird.

6 Domain Name System – DNS. Beschreibende Internetadressen, die unter verschiedenen Top Level Domains verwaltet werden (.com, .de uva).

7 Siehe auch Anhang: B. Hintergrund: Carding-Boards.

8 Getarnte Lesegeräte für Geldautomaten, POS- und anderen Terminals für die bargeldlose Bezahlung an Tankstellen, für Fahrkarten und andere Dienste und Leistungen.

9 Exploit: Schwachstelle in handelsüblichen Computerprogrammen einschließlich ihrer Beschreibung und den Routinen, mit denen sie missbraucht werden können.

10 Rootkit: Digitale Werkzeugsammlung zum Verstecken und Tarnen von Malware auf infizierten Rechnern. Sie sind an die aktuellen Antiviren-Programme angepasst und sollen die Entdeckung von Malware verhindern.

11 Botnetz: Netz aus ferngesteuerten PCs (Zombies), die vor Allem zum Versand von Spam und Malware sowie für verteilte Angriffe (DDoS) verwendet werden können. Verbunden ist damit in aller Regel, dass die Handlungen des Anwenders am infizierten Rechners überwacht und seine persönlichen Daten ausgespäht werden. Jeder Zombie lässt sich prinzipiell auch als Konsole (Eingabestelle) des Botnetz-Betreibers und seiner getarnten Aktivitäten missbrauchen, als Festspeicher für Dateien und als Steuereinheit im Botnetz selber (Flux-Server).

munikationsforen, in denen sich ein Neuling zunächst anmelden und durch passende Beiträge oder Dienste (Keuschheitsproben) Vertrauen erwerben muss, bevor er zu den engeren Zirkeln des Boards Zutritt erlangt. Dem gehen gelegentlich regelrechte Bewerbungsverfahren voraus, in denen der Kandidat um Fürsprache und Unterstützung bei den etablierten Mitgliedern werben muss. In den inneren Zirkeln, die ihrerseits weiter gestaffelt sein können, werden erfahrungsgemäß auch illegale Geschäfte mit Arzneien, Betäubungsmitteln und sogar Waffen abgesprochen und abgewickelt.

Die Betreiber der Boards tarnen sich dadurch, dass sie Bullet-Proof-Dienste nutzen. Das bekannteste Beispiel für einen solchen Schurkenprovider ist das Russian Business Network – RBN – mit Sitz in Petersburg gewesen, das 2007 seine provokante öffentliche Präsenz aufgab und seine Standorte und Dienste seither besser tarnt. Das RBN und seine Nachahmer müssen funktionstüchtige Autonome Systeme [12] mit stabilen Verbindungen zum Internet im Übrigen sein, wodurch ihr Standort gemessen und örtlich bestimmt werden kann. In ihrem inneren Netz betreiben sie Server, die sie beliebig konfigurieren und wegen ihrer Meldungen nach außen kontrollieren können. Das gilt besonders für ihre DNS-Server, mit denen sie die Identität ihrer Kunden verschleiern [13]. Die Tarnung mit technischen Mitteln wird begleitet von einer Mauer des Schweigens: Fragen von Verbraucherverbänden, Verwaltungsbehörden und der Strafverfolgung nach Kunden bleiben unbeantwortet [14],

Das Geschäftsmodell der Schurkenprovider ist einfach: Je mehr Anfragen von Geschädigten, Neugierigen und Strafverfolgern abgewimmelt werden müssen, desto teurer wird der Dienst.

CF, Kriminelle Unternehmer, 07.08.2008

Scheinfirmen verschleiern ihre Identitäten und Zusatzdienste beim Webauftritt und für das Inkasso werden gleich mit angeboten.

Von den kriminellen Geschäften der Board-Mitglieder profitieren die Board-Betreiber und Schurkenprovider durch Umsatzbeteiligungen und Gebühren. Sie sind Teil einer bereits etablierten Underground Economy, in der sich auch die Anbieter von Malware, Finanz- und Warenagenten, Paketstationen und Bezahl- und Abrechnungsdiensten tummeln.

Dieser kriminelle Teil des Internets bleibt der Öffentlichkeit weitgehend verborgen. Sie nimmt vor Allem betrügerische Webshops und sonstige Anbieter wahr, die versuchen, falsche Versprechungen gegen Vorkasse oder Nachnahme zu Beute zu machen, Malware, die ihre Daten ausspähen, Phishing-Trojaner und immer mehr Ransomware wahr, also erpresserische Malware, die den PC blockiert und zur Zahlung eines Lösegeldes auffordert.

Ein anderes Beispiel liefert die „Zauberwald"-Entscheidung des BGH [15]: In einer Internetplattform für „*pädophil orientierte Menschen*" malten sich gesprächsweise zwei Männer aus, dass sie einen „*idealerweise*" achtjährigen Jungen barbarisch sexuell missbrauchen und umbringen wollen. In diesem Zusammenhang hat das Gericht grundsätzlich anerkannt, dass auch einander unbekannte und unter Tarnnamen kommunizierende Mittäter (§ 25 Abs. 2 StGB [16]) eine strafbare Verbrechensabrede (§ 30 StGB) treffen können <Rn 17>. Im entscheidenden Fall, bei dem es nur zu einem einzigen Gesprächskontakt zwischen

[12] Autonome Systeme – AS – sind Subnetze, die mit mindestens zwei anderen AS verbunden sind und in ihrer Gesamtheit und Vernetzung das Internet bilden. Ihnen sind verbindliche AS-Nummern zugewiesen, die von der zentralen Internetverwaltung ICANN (siehe **CF**, Zentralismus und Regionalisierung, 18.07.2010) und ihren Zonenverwaltungen (zum Beispiel RIPE für Europa) vergeben und verwaltet werden.

[13] Siehe **CF**, Schurkenprovider, 11.04.2010 (Whois Protection, anonyme Server).

[14] Insoweit wird auch von „beschwerdeignoranten Providern" gesprochen; siehe **CF**, Rogue-Provider, 13.07.2008.

[15] **BGH**, Beschluss vom 16.03.2011 - 5 StR 581/10

[16] An der Verbrechensabrede können sich nur Täter und nicht auch Gehilfen (§ 27 Abs. 2 StGB) beteiligen: **CF**, Verbrecher muss Mittäter sein, 25.04.2009; **BGH**, Urteil vom 04.02.2009 - 2 StR 165/08.

den Männern gekommen war und keine Ausführungshandlungen erfolgten, bemängelt der BGH jedoch, das erkennende Gericht habe unzureichend die *Verbrechensfantasie von wirklichem verbrecherischen Willen und dessen Umsetzung* abgegrenzt <Rn 18> [17].

Die Entscheidung zeigt das Bemühen der Rechtsprechung, moderne Kommunikationsformen mit den klassischen Instrumenten des Rechts zu erfassen. Sie stellt jedenfalls klar, dass die Kommunikation per Internet zwar Besonderheiten aufweist, ungeachtet dessen aber wie andere Kommunikationsprozesse auch der Bewertung und Beweiswürdigung unterliegt.

Die Berichterstattung über die Kriminalität im Internet lässt den Eindruck entstehen, dass die Strafverfolgung wenn überhaupt, dann nur punktuell erfolgreich ist. Sie ist nicht untätig, hat aber mit mehreren Erschwernissen zu kämpfen.

- Internetkriminalität ist grenzüberschreitend und interlokal. Ihre Identifikation kann im Wesentlichen nur mit den Mitteln und der Technik des Internets selber erfolgen, die mit anderen intelligenten Ermittlungsmethoden verbunden werden müssen.
- Intelligente Täter versuchen sich zu tarnen und einem Zugriff zu entziehen. Auch sie machen gelegentlich Fehler und das vor Allem dann, wenn sie ihre Beute in der realen Welt sichern müssen.
- Die Verfolgung der Internetkriminalität stößt schnell an nationale Grenzen. Sie ist nicht nur wegen der notwendigen Methoden, sondern auch deshalb aufwändig und anspruchsvoll, weil sie auf die internationale Rechtshilfe und Zusammenarbeit angewiesen ist. Das gilt besonders für die staatlichen Eingriffsrechte, deren besonderen Voraussetzungen zwar vorliegen mögen, die aber nur innerhalb der nationalstaatlichen Grenzen angewendet werden können. Internationale Abkommen, vor Allem im europäischen Verbund, haben den Umgang erleichtert, gelten aber nicht lückenlos.

> *Der Rechtsstaat kann sich nur verwirklichen, wenn ausreichende Vorkehrungen dafür getroffen sind, dass Straftäter im Rahmen der geltenden Gesetze verfolgt, abgeurteilt und einer gerechten Bestrafung zugeführt werden.*
>
> BVerfG, Beschluss vom 18.03.2009 - 2 BvR 2025/07, Rn 16

- Internetbezogene Ermittlungen und der Umgang mit den Strukturen und Möglichkeiten des Internets bilden noch weitgehend Neuland, für das es noch wenige Erfahrungen und vor Allem keine standardisierte Ausbildung gibt. Es gibt auch in der Strafverfolgung geniale Spezialisten und engagierte Multiplikatoren, aber es fehlt ganz besonders an technischem und praktischem Allgemeinwissen, Ausstattung und politischem Willen. Er würde in klaren Bekenntnissen zur Strafverfolgung, in der Förderung der Fortbildung und in der Bereitstellung personeller Ressourcen zum Ausdruck kommen. Das geschieht jedoch erst vereinzelt und punktuell.
- Neben Unkenntnis und Unerfahrenheit wirkt sich bei den Ermittlungspersonen besonders fatal die Verunsicherung aus, die mit den Fragen nach den zulässigen Ermittlungsmethoden, ihren förmlichen Anforderungen und möglichen Verwertungsverboten verbunden ist. Die anhaltenden und vielfach irrational angeheizten Diskussionen um die Vorratsdatenspeicherung und die Onlinedurchsuchung tragen ein Übriges bei.

Sowohl die Vorratsdatenspeicherung wie auch die Onlinedurchsuchung sind wegen ihrer Ausgestaltungen vom BVerfG untersagt worden [18]. Das ändert nichts an der Tatsache, dass das Verfas-

[17] Tragend ist insoweit, dass die besondere Gefährlichkeit der Verbrechensabrede in dem sozialen Zwang besteht, aus dem heraus die anderen Beteiligten das zugesagte Handeln einfordern können. Je weitläufiger und anonymer die Beziehung zwischen den Beteiligten ist, desto stärker muss der Bindungswille des einzelnen Beteiligten betrachtet und hinterfragt werden.

[18] Jüngst auch die Abfrage von Bestandsdaten im Zusammenhang mit dynamischen IP-Adressen: **BVerfG**, Beschluss vom 24.01.2012 - 1 BvR 1299/05.

sungsgericht beide Ermittlungsmethoden grundsätzlich anerkennt, aber präzise Schranken wegen ihrer Anwendung, Absicherung gegen Missbrauch und klare Regeln wegen des nachträglichen Rechtsschutzes verlangt. Dagegen ist ernsthaft nichts einzuwenden.

Die öffentliche Diskussion, in der sich nicht zuletzt prominente Funktionsträger äußern, ist hingegen von einem Misstrauen geprägt, das ein Bild von der Strafverfolgung vermittelt, wonach sie ungehemmt und willkürlich schnüffelt und Bürgerrechte mit Füßen tritt. Augenmaß und Differenzierung sind nicht die Parameter, die für das politische Geschäft und öffentliche Meinungsstreite leitend sind.

Das vorliegende Arbeitspapier wendet sich gegen Unkenntnis und Verunsicherung. Es ist eine rechtliche Bestandsaufnahme, die sich den Möglichkeiten, förmlichen Anforderungen und Grenzen der Ermittlungen im Internet widmet. Wie bei diesem Themenbezug üblich, kann auf bewährte Quellen zurück gegriffen werden, die im Zusammenhang mit klassischen Sachverhalten stehen. Sie lassen sich häufig auf die Anforderungen der digitalen Welt übertragen. Gleichwohl betrete ich zum Beispiel wegen der längerfristigen Observation und dem Einsatz Verdeckter Ermittler Neuland.

Darin kommt der Anspruch auf eine Bestandsaufnahme zum Ausdruck. Im Neuland kann ich keine allgemein anerkannte herrschende Meinung beanspruchen, wohl aber eine ernst zu nehmende Position, die sich der Kritik und Anerkennung stellt. Mut macht mir dazu, dass ich wegen meiner schnell entwickelten und deutlichen Position zur Verwertbarkeit von zulässig erhobenen Vorratsdaten auch nach der Entscheidung des BVerfG [19] Recht behalten habe und von mehreren Senaten des BGH bestätigt worden bin [20].

Zu fragen ist zunächst nach den einschlägigen Ermächtigungsgrundlagen, die in einem ganz engen Zusammenhang mit den betroffenen Grundrechten, der Eingriffstiefe der Ermittlungsmethode und ihrer Ausgestaltung im Einzelfall stehen.

Die technischen Ermittlungsmethoden sind bereits breit diskutiert, so dass ich mich wegen der Quellen-TKÜ, dem Einsatz von Spionagetechnik (Onlinedurchsuchung) und der Bedeutung der Verkehrsdaten (Auskünfte über Bestands- und Vorratsdaten) auf die wesentlichen Argumente beschränken kann.

Wegen der Erörterung der Personenbeweise müssen jedoch zunächst die Grundlagen geschaffen und darauf aufbauend Aussagen über die Zulässigkeit, die förmlichen Anforderungen und die Grenzen getroffen werden. Dadurch komme ich zu dem Ergebnis, dass im Zusammenhang mit schweren Formen der Kriminalität im Internet geheime Methoden bis tief in Hackerboards hinein angewendet werden können. Die Informationsbeschaffung im Internet, die Verwendung von Falschnamen und die Teilnahme an Diskussionen sind ohne besondere Beschränkungen zulässig. Wegen längerfristiger Beobachtungen bedarf es gerichtlicher Zustimmungen wegen Observationen oder dem Einsatz Verdeckter Ermittler. Unüberschreitbare Grenzen sehe ich vor Allem bei Keuschheitsproben in Bezug auf ihrerseits strafbare Handlungen und beim Einsatz von Spionagetechnik.

---

[19] Dieter **Kochheim**, Zum Umgang mit Verkehrsdaten, 08.03.2010

[20] **CF**, Verwertungsgrenzen, 03.04.2011

1. Internet und Strafverfahrensrecht

§ 101 StPO benennt die verdeckten Ermittlungshandlungen, die die Strafprozessordnung wegen der Aktenführung und vor Allem wegen der nachträglichen Benachrichtigungspflichten hervorhebt. Sie reichen von der Rasterfahndung über die Überwachung der Telekommunikation und dem großen Lauschangriff bis hin zur längerfristigen Observation. Bei den Regelungen im Einzelfall handelt es sich um besondere Eingriffsermächtigungen, die an strenge Voraussetzungen geknüpft und vom Gebot des rechtlichen Gehörs ausgenommen sind (Art 103 Abs. 1 GG, § 33 Abs. 4 StPO). In Bezug auf die Ermittlungen wegen Straftaten im Internet haben nur wenige von ihnen eine besondere Bedeutung. Das gilt etwa für die technischen Ermittlungsmaßnahmen, für die die Überwachung der Telekommunikation (§ 100a StPO) und die Auskünfte über Verkehrsdaten stehen (§ 100g StPO), und dem Einsatz eines Verdeckten Ermittlers als besondere Form des Personenbeweises (§ 110a StPO).

Aufgrund der Urteile des BVerfG gegen die Ausgestaltung der Onlinedurchsuchung [21] sowie gegen die Verwendungsregeln und Sicherungsmaßnahmen wegen der Vorratsdaten [22] ist vielfach der Eindruck entstanden, Ermittlungen wegen Straftaten im Internet seien grundsätzlich stark behindert oder gar ausgeschlossen. Das stimmt nur bedingt wegen dieser beiden Eingriffsmaßnahmen und verdeckt den Blick darauf, dass die Strafprozessordnung viele Ermittlungshandlungen zulässt, die auch auf Erkundungen im Internet anwendbar sind und schnelles und effektives Handeln der Strafverfolgungsbehörden wegen Straftaten im Internet zulassen. Das gilt vor Allem für die Ermittlungsgeneralklausel des § 161 Abs. 1 StPO, die die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 Abs. 1 GVG) dazu ermächtigt, ***Ermittlungen jeder Art*** durchzuführen, soweit sie nicht durch besondere Vorschriften reguliert, begrenzt

> *§ 161 Abs. 1 StPO stellt als Ermittlungsgeneralklausel die Ermächtigungsgrundlage für Ermittlungen jeder Art dar, die nicht mit einem erheblichen Grundrechtseingriff verbunden sind und daher keiner speziellen Eingriffsermächtigung bedürfen. Sie ermächtigt die Staatsanwaltschaft zu den erforderlichen Ermittlungsmaßnahmen, die weniger intensiv in Grundrechte des Bürgers eingreifen (...). Die Staatsanwaltschaft kann auf dieser Grundlage in freier Gestaltung des Ermittlungsverfahrens die erforderlichen Maßnahmen zur Aufklärung von Straftaten ergreifen.*
>
> **BVerfG**, Beschluss vom 17.02.2009 - 2 BvR 1372/07, Rn 26

oder ausgestaltet sind.

Bereits die Generalklausel ermächtigt die Strafverfolgungsbehörden zu „wenig intensiven“ Grundrechtseingriffen [23], wenn sie unter den Gesichtspunkten der Erforderlichkeit und der Verhältnismäßigkeit geboten sind. Diese optimistische Einschätzung könnte sich jedoch durch die jüngste Entscheidung des ersten Senats des BVerfG zu den Auskünften über die Telekommunikation ändern [24].

Leitend dafür ist, dass das Grundgesetz einerseits die Grundrechte des Einzelnen gegen staatliche Eingriffe in ihrem Wesensgehalt schützt (Art 19 Abs. 2 GG) und andererseits auch die Rechte anderer betrachtet, die durch die Freiheitsgewähr ihrerseits in eigenen Grundrechten auf Würde, Ehre, Meinung, Eigentum und andere beeinträchtigt werden können. Das findet seinen Ausdruck besonders auch in der Rechtsschutzgarantie (Art 19 Abs. 4 GG), die ein Teil der Rechtsstaatsgarantie ist (Art 20 Abs. 3 GG). Zu ihr gehört die Gewährung des Rechtsfriedens und damit auch eine effektive Strafverfolgung [25].

Bei der Frage nach der Verhältnismäßigkeit von strafrechtlichen Eingriffsmaßnahmen kommen mehrere Aspekte ins Spiel. Das betrifft besonders

---

21 **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07

22 **BVerfG**, Urteil vom 02.03.2010 - 1 BvR 256, 263, 586/08

23 Siehe Kasten oben; **BVerfG**, Beschluss vom 17.02.2009 - 2 BvR 1372/07, Rn 26.

24 **CF**, Auskünfte über die Telekommunikation, 26.02.2012

25 **BVerfG**, Beschluss vom 18.03.2009 - 2 BvR 2025/07

Straftaten von erheblicher Bedeutung

sind keine Bagatelldelikte aus dem Bereich der ***einfachen Kriminalität***

- Freiheitsstrafe bis 3 Jahre

sind mindestens ***wiederholte*** Delikte aus dem Bereich der ***mittleren Kriminalität***

- Freiheitsstrafe bis 5 Jahre
- erhöhte Mindeststrafe und
- alle Verbrechen

der ***schweren Kriminalität***

- mehr als 5 Jahre Freiheitsstrafe
- Straftatenkatalog des § 100a Abs. 2 StPO

und der ***besonders schweren Kriminalität***

- Straftatenkatalog des § 100c Abs. 2 StPO

die Frage nach einer weniger einschneidenden Alternative, ihren Erfolgsaussichten und nach der Schwere der Kriminalität, gegen die die Maßnahme gerichtet ist.

Die Schwere der Kriminalität ist vor Allem in den Entscheidungen des BVerfG zum großen Lauschangriff behandelt worden [26], wobei das Gericht die besonders schwere Kriminalität auf einfache Art definiert hat: Besonders schwere Kriminalität ist die, die das Gesetz mit mehr als fünf Jahren Freiheitsstrafe im Höchstmaß bedroht und das unabhängig davon, ob es sich um einen selbständigen Straftatbestand oder um eine Qualifikation wegen eines besonders schweren Falles handelt [27]. Durchgängig akzeptiert das BVerfG jetzt den Straftatenkatalog des § 100a Abs. 2 StPO zur Überwachung der Telekommunikation als Richtlinie dafür, dass die aufgeführten Tatbestände jedenfalls der schweren Kriminalität angehören [28]. Die oben gezeigte Zuordnung (siehe Kasten) folgt den Bezeichnungen zu den Straftatenkatalogen in § 100a Abs. 2 StPO (schwere Straftaten, TKÜ) und § 100c Abs. 2 StPO (besonders schwere Straftaten, großer Lauschangriff) und der Zuordnung des BVerfG [29].

Verschiedene Eingriffsnormen aus der Strafprozessordnung sprechen von „Straftaten von erheblicher Bedeutung“ (§§ 110a, 163f StPO), ohne dass dieser Begriff genau definiert wird. Im Anschluss an die formalisierte Betrachtungsweise des BVerfG gehe ich deshalb von den Kriterien aus, die im Kasten oben aufgeführt sind. Danach sind die tiefsten Grundrechtseingriffe, die die StPO zulässt, der mindestens schweren Kriminalität vorbehalten, zum Beispiel der Überwachung der Telekommunikation (§ 100a StPO).

1.1 Gefahrenabwehr und Strafverfahren

Auch aus dem Arbeitsalltag von Polizei und Strafrechtspflege ist die Recherche im Internet nicht mehr wegzudenken. Gesucht wird nach Adressen, Fachinformationen, Rechtsprechung und anderen Auskünften, die frei oder in zugänglichen Datensammlungen zur Verfügung stehen. Im polizeilichen Bereich geht das bis hin zur gezielten anlassunabhängigen Internetrecherche. Ein Beispiel dafür ist die Ermächtigung des Bundeskriminalamtes zur Sammlung und Auswertung von Informationen zur Verhütung und Verfolgung von Straftaten (§ 2 Abs. 2 Nr. 1. BKAG). Entsprechende Vorschriften sehen die Ländergesetze zur Gefahrenabwehr vor [30].

Die strafrechtliche Untersuchung umfasst das Ermittlungs- und das gerichtliche Verfahren bis zum rechtskräftigen Urteil [31]. Ihr folgt die Strafvollstreckung, zu der die Staatsanwaltschaft gesondert als Vollstreckungsbehörde beauftragt ist (§ 451

---

[26] Besonders: **BVerfG**, Urteil vom 03.03.2004 - 1 BvR 2378/97, 1 BvR 1084/99.

[27] Ebenda, Rn 238, 241

[28] **BVerfG**, Beschluss vom 11.03.2008 - 1 BvR 256/08, Rn 167

[29] **BVerfG**, Beschluss vom 16.06.2009 - 2 BvR 902/06, Rn 69

[30] Zum Beispiel das Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung: § 31 Nds. SOG (Datenerhebung), § 38 Nds. SOG (Speicherung, Nutzung und Zweckbindung) und § 40 Nds. SOG (Datenübermittlung).

[31] Siehe Anhang:
A.1 Staatsanwaltschaft und Strafverfolgung
A.3 Verfahren der Strafrechtspflege

Abs. 1 StPO).

Die Gefahrenabwehr, also die unmittelbare Reaktion auf Gefahren und die Verhütung von Straftaten (Vorbeugung, Prävention), ist die Kernaufgabe der Polizei. Die Leitungsbefugnis der Staatsanwaltschaft [32] gilt nur in Bezug auf strafrechtliche Ermittlungen und nicht für die Gefahrenabwehr. Sie darf und muss zur Prävention allerdings im Rahmen ihrer zugewiesenen Aufgaben, dem Rechtsstaatsgebot (Art 20 Abs. 3 GG) und ihrer Verpflichtung zum Schutz der Grundrechte (Art 1 Abs. 3 GG) beitragen [33].

Die Vorfeldermittlungen [34] (Initiativermittlungen), die sich auf kriminelle Umfelder konzentrieren, nicht aber auf bestimmte Straftaten und Straftäter, sind präventiv und deshalb eine Obliegenheit der Polizei. Sobald dabei konkrete Hinweise auf Straftaten zu Tage treten (§ 152 Abs. 2 StPO), endet die Prävention und sind alle weiteren Erkundungen nach Maßgabe der Strafprozessordnung zu führen. Sie sind *selbst im Fall einer "Gemengelage" ... einheitlich an den Regelungen der StPO zu messen* [35].

Zwischen den Vorfeldermittlungen und dem förmlichen Ermittlungsverfahren sind die Vorermittlungen angesiedelt [36]. Sie dienen zur Aufklärung von besonderen Ereignissen, die für sich alleine keinen zwingenden Schluss auf eine Straftat zulassen (Merkwürdigkeiten [37]). Sie markieren einen fließenden Übergang vom Polizei- zum Strafverfahrensrecht und rechtfertigen zu bestimmten Eingriffsmaßnahmen, die die Strafprozessordnung ausdrücklich zulässt [38]. Spätestens bei ihrem Einsatz beginnt das Ermittlungsverfahren nach Maßgabe der StPO.

Nichts anderes gilt für die Ermittlungen im Internet. Die Beobachtung von möglicherweise betrügerischen Webshops und von sozialen Kommunikationsplattformen sind grundsätzlich von der Aufgabe der Gefahrenabwehr geprägt. Sobald jedoch Hinweise auf konkrete Straftaten bemerkt werden, „kippt“ sozusagen die Gefahrenabwehr zur Strafverfolgung um [39]. Das ist vor Allem bei der Beobachtung von Hackerboards aus der Carding-Szene sehr schnell zu erwarten.

Das stellt jedoch kein Hindernis dar, weil auch im Zusammenhang mit polizeilichen Ermittlungen im Strafverfahren zunächst die Ermittlungsgeneralklausel des § 161 Abs. 1 StPO greift und die Polizei zum ersten Zugriff berechtigt ist (§ 163 Abs. 1 StPO). Erst die jüngste Entscheidung des BVerfG [40] zu den Auskünften über die Telekommunikation verlangt ausdrücklich nach „normenklaren“ Auskunftspflichten der Provider und die Auswirkung davon auf die Ermittlungsgeneralklauseln für die Staatsanwaltschaft und ihre Ermittlungspersonen ist noch unklar [41].

1.2 Dokumentation und Auswertung

Als Folge des Grundrechts auf informationelle Selbstbestimmung [42] hat das BVerfG auch im Zusammenhang mit der Onlinedurchsuchung darauf hingewiesen, dass die gezielte Sammlung, Dokumentation und Auswertung von Daten nach einer besonderen Eingriffsermächtigung verlangen kann, wenn sich daraus *eine besondere Gefah-*

---

[32] A.2 Verhältnis zur Polizei

[33] Daraus folgt auch die Verpflichtung zur Amtshilfe (Art 35 Abs. 1 GG), die von Auskunftsrechten begleitet wird: zum Beispiel § 8 Abs. 2 BND-Gesetz, § 18 Abs. 1 BVerfSchG, § 30 Abs. 2 StVollstrO.

[34] A.3.1 Vorfeldermittlungen
A.4.2 Prävention und Vorfeld
A.4.4 Initiativermittlungen

[35] BGH zum Einsatz eines Lockspitzels: **BGH**, Urteil vom 18.11.1999 - 1 StR 221/99, Rn 52.

[36] A.3.2 Vorermittlungen

[37] A.4.6 Merkwürdigkeiten

[38] A.4.7 Eingriffsrechte im Stadium der Vorermittlungen

[39] **BGH**, Urteil vom 18.11.1999 - 1 StR 221/99, Rn 52 (Gemengelage beim Lockspitzel)

[40] **BVerfG**, Beschluss vom 24.01.2012 - 1 BvR 1299/05

[41] **CF**, Manuelles Auskunftsverfahren, 26.02.2012

[42] **BVerfG**, Urteil vom 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 (Volkszählungsurteil)

renlage für die Persönlichkeit des Betroffenen ergibt [43]. Solche Ermächtigungsgrundlagen sind in der Strafprozessordnung vorhanden und betreffen die Aktenführung, ihre Vollständigkeit und die Ermächtigung der Strafverfolgungsbehörden zum „Quervergleich“ ihrer Kenntnisse aus verschiedenen Verfahren.

Die Strafprozessordnung ermächtigt nicht nur, sondern verpflichtet die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 Abs. 1 GVG) in verschiedenen Zusammenhängen zur Dokumentation ihrer Ermittlungshandlungen und -ergebnisse. Das gilt zunächst für die Staatsanwaltschaft, die das Ergebnis ihrer Untersuchungen aktenkundig machen und über Vernehmungen Protokolle fertigen muss (§ 168b StPO). Nach dem Abschluss der Ermittlungen (§ 169a StPO) erlangt der Verteidiger ein unbeschränktes Akteneinsichtsrecht (§ 147 Abs. 1, 2 StPO). Bei der Anklageerhebung sind dem Gericht neben der Anklageschrift auch die vollständigen Akten vorzulegen (§ 199 Abs. 2 S. 2 StPO). Dazu gehört *das gesamte vom ersten Zugriff der Polizei ... an gesammelte Beweismaterial, einschließlich etwaiger Bild- und Tonaufnahmen nebst hiervon gefertigter Verschriftungen, zugänglich gemacht werden, das gerade in dem gegen den Angeklagten gerichteten Ermittlungsverfahren angefallen ist (...). Eine Ausnahme gilt nur für Unterlagen oder Daten, denen eine allein innerdienstliche Bedeutung zukommt. Dies können etwa polizeiliche Arbeitsvermerke im Fortgang der Ermittlungen unter Bewertung der bisherigen Ermittlungsergebnisse oder sonstige rein interne polizeilichen Hilfs- oder Arbeitsmittel nebst entsprechender Dateien sein (...). Im Bereich der Justizbehörden sind vom Akteneinsichtsrecht ausgenommen etwa entsprechende Bestandteile der staatsanwaltschaftlichen Handakten, Notizen von Mitgliedern des Gerichts während der Hauptverhandlung oder so genannte Senatshefte (...).* [44]

Die Dokumentationspflicht trifft die Polizei in gleichem Maße. Bereits nach dem ersten Zugriff muss sie ihre „Verhandlungen“ ohne Verzug der Staatsanwaltschaft übersenden (§ 163 Abs. 2 S. 1 StPO). Einzelheiten über die Form der Aktenführung ergeben sich zum Beispiel aus § 101 Abs. 2 StPO.

Die Berechtigung zum Vergleich und zur Auswertung von Daten folgt bereits aus der Ermittlungsgeneralklausel des § 161 Abs. 1 S. 1 StPO, die die Staatsanwaltschaft ausdrücklich dazu ermächtigt, Auskünfte von ***anderen*** Behörden einzuholen. Das untermauert § 98c StPO, der ohne formelle Hürden auch den ***maschinellen*** Abgleich zwischen den Daten aus anderen Verfahren zulässt. Die Verwertungsverbote, die sich aus § 161 Abs. 2 StPO ergeben, greifen nicht schon bei der Datenauswertung, sondern erst bei Übernahme in ein neues Verfahren, wobei die Schwellengleichheit der verfolgten Vorwürfe zu prüfen ist [45]. Insoweit ist von der Rechtsprechung anerkannt, dass bei der Freibeweisführung alle Erkenntnisse verwertet werden dürfen, auch wenn für sie Verwertungshindernisse bestehen (Spurenansatz [46]).

Die Ermächtigung zum Datenabgleich ist keine Rasterfahndung. § 98a StPO setzt nämlich voraus, dass ein Dritter, der keine Strafverfolgungsbehörde ist, die Daten zur Verfügung stellen muss [47].

---

[43] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 309

[44] **BGH**, Urteil vom 18.06.2009 - 3 StR 89/09, Rn 20

[45] **BGH**, Urteil vom 27.11.2008 - 3 StR 342/08, Rn 13. Siehe auch: **CF**, Schwellengleichheit, 21.12.2008

[46] **BVerfG**, Urteil vom 03.03.2004 - 1 BvR 2378/98, 1 BvR 1084/99, S. 64; **BVerfG**, Beschluss vom 25.04.2005 - 2 BvR 866/05. Siehe auch: **CF**, zulässige Verwertung verdeckter Zufallserkenntnisse, 28.02.2009.

[47] Abgrenzung zum staatsanwaltschaftlichen Auskunftsersuchen und zur Anwendung der Ermittlungsgeneralklausel: **BVerfG**, Beschluss vom 17.02.2009 - 2 BvR 1372/07, 2 BvR 1745/07 (Mikado).

1.3 Geltung des Strafverfahrensrechts

Das strafrechtliche Ermittlungsverfahren (Untersuchung) beginnt bereits bei den Vorermittlungen, die der Frage dienen, ob bestimmte Tatsachen aus einer Straftat herrühren oder eine harmlose Erklärung haben (zum Beispiel Leichenfund, Brand oder verendete Fische). Bereits in diesem Stadium ermächtigt die Ermittlungsgeneralklausel die Staatsanwaltschaft und ihre Ermittlungspersonen zu allgemein gehaltenen Ermittlungen und sind zum Beispiel Durchsuchungen und Beschlagnahmen von der Strafprozessordnung zugelassen.

Polizeiliche Ermittlungen im Vorfeld des Ermittlungsverfahrens dienen der Gefahrenabwehr und Kriminalprävention. Die Ermächtigungen dazu können sich nur aus dem Polizeirecht ergeben. Sobald jedoch von der Polizei Tatsachen erkannt werden, die eine Straftat möglich erscheinen lassen, greifen für die weiteren polizeilichen Maßnahmen die Vorschriften der StPO.

Im Stadium der Vorermittlungen kann dadurch eine Gemengelage zwischen polizei- und strafverfahrensrechtlichen Ermittlungszielen eintreten. Dafür stellt die Ermittlungsgeneralklausel eine allgemeine Ermächtigung zur Verfügung. Sie allein reicht aber nicht aus, um eingriffsschwere Maßnahmen zu begründen. Alle Eingriffe, die die StPO unter besondere Zulässigkeitsvoraussetzungen stellt, müssen deshalb bereits während der Vorermittlungen nach den Maßstäben der StPO angeordnet und durchgeführt werden.

Wenn die polizeirechtlichen Ermächtigungen weiter reichen als die der StPO, so sind die Ermittlungen nicht zwingend abzubrechen. Die Verwertung der Erkenntnisse richtet sich dann nach § 161 Abs. 2 StPO. Unter Umständen können die Erkenntnisse der Polizei dann nur nach Maßgabe des Spurenansatzes freibeweislich zur Begründung von strafverfahrensrechtlichen Eingriffsmaßnahmen herangezogen werden.

Diese Grundsätze gelten selbstverständlich auch für die polizeilichen Ermittlungen im Internet. Auch die anlassunabhängigen Recherchen müssen nach Maßgabe der StPO zulässig sein, sobald sie Tatsachen betreffen, die eine Straftat erwarten lassen. Die Polizei wird insoweit im ersten Zugriff tätig und unterliegt wegen ihren „Verhandlungen“ einer Dokumentationspflicht nach der StPO.

Die weiten Ermächtigungen, die die Strafprozessordnung auch für das Vorverfahren zur Verfügung stellt, lassen Kollisionen nur im Ausnahmefall erwarten.

2. Grundrechte und Eingriffsmaßnahmen

Die Frage nach der Tiefe, mit der bestimmte Ermittlungsmaßnahmen in grundrechtlich geschützte Rechtsgüter eindringen, ist in zweierlei Hinsicht bedeutsam:

1) Danach richtet sich, ob eine allgemeine Eingriffsbefugnis wie die Ermittlungsgeneralklausel in § 161 Abs. 1 StPO zur Begründung reicht oder eine besondere Eingriffsbefugnis mit einschränkenden Voraussetzungen zu fordern ist [48] und

2) ob eine fehlerhaft begründete oder durchgeführte Ermittlungsmaßnahme zu einem Verwertungsverbot führen kann [49].

Dem Einstieg dient ein knapper Überblick über die in Betracht kommenden Grundrechte. Für sie gilt, dass ihr Wesensbereich unangetastet bleiben muss (Art 19 Abs. 2 GG), im Interesse anderer, im Einzelfall stärkerer Rechte aber aufgrund eines Gesetzes in sie eingegriffen werden darf (Art 19 Abs. 1 GG). Von besonderer Bedeutung ist insoweit der vom BVerfG [50] hervorgehobene und vom Gesetzgeber in verschiedene Eingriffsnormen übernommene Schutz des Kernbereichs der privaten Lebensgestaltung. Dazu hat das Gericht bereits deutliche Worte gefunden: *Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten … gehören ... dem unantastbaren Bereich privater Lebensgestaltung nicht an* [51] und *wenn konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern* [52], dann bleibt die Überwachung zulässig.

2.1 Telekommunikationsgeheimnis

Das Telekommunikationsgeheimnis aus Art 10 Abs. 1 GG umfasst die Telekommunikation insgesamt, *einerlei, welche Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und welche Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) genutzt werden, und schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs unabhängig davon ..., ob die (Eingriffs-) Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation erfolgt. Neben den Inhalten schützt es auch die Umstände der Telekommunikation, also ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist* [53]. *Der Schutz des Fernmeldegeheimnisses endet in dem Moment, in dem die Nachricht bei dem Empfänger angekommen und der Übertragungsvorgang beendet ist* [54].

Von dieser strengen Betrachtung ist das BVerfG jetzt im Zusammenhang mit den Auskünften über dynamische IP-Adressen abgerückt [55]. Die „einfachen“ Bestandsdatenabfragen der Sicherheitsbehörden im Automatisierten Auskunftsverfahren nach § 112 TKG berühren „nur“ die Informationelle Selbstbestimmung <Rn 153>, so dass es überhaupt nur einer Eingriffsermächtigung bedarf. Dafür dürfte die Ermittlungsgeneralklausel weiterhin ausreichen.

Das TK-Geheimnis schützt *das Vertrauen des*

---

[48] Grundlegend: **BVerfG**, Beschluss vom 17.02.2009 - 2 BvR 1372/07, Rn 26

[49] Einschränkende Voraussetzungen für ein Verwertungsverbot (hier: Vorratsdaten): **BGH**, Beschluss vom 18.01.2011 – 1 StR 663/10, Rn 22, 25. Siehe auch: **CF**, Verwertungsverbot und Vorratsdaten, 10.03.2011.

[50] Seit **BVerfG**, Urteil vom 16.01.1957 - 1 BvR 253/56, Rn 14 – 16 (Elfes)

[51] **BVerfG**, Beschluss vom 26.06.2008 - 2 BvR 219/08

[52] **BVerfG**, Urteil des vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 281

[53] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 182, 183, 184 (Onlinedurchsuchung)

[54] **BVerfG**, Beschluss vom 13.11.2010 - 2 BvR 1124/10, Rn 13

[55] **BVerfG**, Beschluss vom 24.01.2012 - 1 BvR 1299/05

Einzelnen darin, dass eine Fernkommunikation, an der er beteiligt ist, nicht von Dritten zur Kenntnis genommen wird [56], also den technischen Vorgang als solchen, nicht aber die *Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartners* [57]. Nach Abschluss der Fernkommunikation gewährt das Grundrecht auf informationelle Selbstbestimmung den Schutz der Persönlichkeitsrechte in Bezug auf technische Einrichtungen.

Das Telekommunikationsgeheimnis ist deshalb einschlägig für die heimlichen technischen Überwachungsmaßnahmen, allen voran für die Überwachung der Telekommunikation als solche (§ 100a StPO), dem Einsatz eines IMSI-Catchers (§ 100i StPO) und Erhebung von Verbindungsdaten (§ 100g StPO). Auch nach Maßgabe des Urteils gegen die Ausgestaltung der Vorratsdatenspeicherung [58] können noch immer die nach § 96 TKG gespeicherten Verkehrsdaten und nach § 98 TKG verbliebenen Standortdaten im automatisierten und manuellen Auskunftsverfahren (§§ 112, 113 TKG) zum Ermittlungsverfahren beigezogen und die „laufenden" Daten protokolliert werden [59]. Dasselbe gilt für die Nutzungsdaten nach § 15 TMG [60].

Nach § 100g Abs. 3 StPO gelten die besonderen Formanforderungen nicht, sobald der Telekommunikationsvorgang abgeschlossen ist. Das gilt zum Beispiel für die in einem Mobiltelefon gespeicherten oder bei einer Durchsuchung gefundenen Verkehrsdaten auf den Speichermedien des Betroffenen.

Problematisch sind die Bestandsdatenauskünfte im Manuellen Auskunftsverfahren (§ 113 TKG). Hier richten die Sicherheitsbehörden ihre Anfragen direkt an die Zugangsprovider und andere Mediendienste um zu erfahren, wer wann über eine technische Adresse (Internetadresse; TCP/IP) agiert hat. Die Dienste können darauf nur antworten, wenn sie auf ihre gespeicherten Verkehrsdaten zugreifen. Deshalb sagt das BVerfG jetzt [61]: *Soweit der Gesetzgeber die Telekommunikationsunternehmen dazu verpflichtet, auf diese Daten zurückzugreifen und sie für die staatliche Aufgabenwahrnehmung auszuwerten, liegt darin ein Eingriff in Art 10 Abs. 1 GG. Dies ist nicht nur dann der Fall, wenn die Diensteanbieter die Verbindungsdaten selbst herausgeben müssen, sondern auch dann, wenn sie sie als Vorfrage für eine Auskunft nutzen müssen*. Die Folge davon ist, dass das BVerfG die Auskunftsvorschriften des TKG nur noch bis zum 30.06.2013 gelten lässt. Die amtierende Bundesjustizministerin lässt erwarten, dass danach keine dynamischen Bestandsdatenauskünfte mehr erteilt werden [62].

2.2 informationelle Selbstbestimmung

Die allgemeinen Persönlichkeitsrechte werden von Art 1 Abs. 1 GG (Würde des Menschen) und Art 2 GG (Freiheitsrechte) garantiert. Aus ihnen hat das BVerfG im Volkszählungsurteil von 1983 [63] zunächst das Recht auf informationelle Selbstbestimmung abgeleitet. Es ist ein Recht des Einzelnen gegenüber dem Staat und seinen Einrichtungen, über die Preisgabe, Erhebung und Verwendung seiner personenbezogenen Daten grundsätzlich selber zu bestimmen. Es beschränkt die Anlässe und Umfänge staatlicher Datenerhebungen und -sammlungen und fordert für sie ausdrückliche gesetzliche Eingriffsermächtigungen.

Strafrechtliche Ermittlungshandlungen berechtigen nicht nur zur Datendokumentation, sondern mehr

---

56 **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 290

57 Ebenda

58 **BVerfG**, Urteil vom 02.03.2010 - 1 BvR 256, 263, 586/08

59 Siehe auch: **CF**, Vorratsdaten, 01.01.2011; **CF**, wirre Argumentation, 22.01.2011.

60 § 15 Abs. 5 S. 5 TMG verweist auf § 14 Abs. 2 TMG, so dass die Auskunftspflicht wegen der Bestandsdaten auch für die Nutzungsdaten gilt.

61 **BVerfG**, Beschluss vom 24.01.2012 - 1 BvR 1299/05, Rn 116

62 **CF**, Trollhausen life: Das wird nichts! 26.02.2012

63 **BVerfG**, Urteil vom 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83

noch, sie verpflichten dazu [64]. Mit der Ermittlungsgeneralklausel (§ 161 Abs. 1 StPO) und der besonderen Ermächtigung zum Datenabgleich (§ 98c StPO) bestehen hinreichende Eingriffsnormen für die Dokumentation und Datenauswertung, die bereits im vorkonstitutionellen Recht angelegt sind [65].

2.3 Integrität informationstechnischer Systeme

Im Zusammenhang mit seiner Auseinandersetzung mit der Onlinedurchsuchung hat das BVerfG auch das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme [66] beschrieben, *um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann* [67]. Dies ist nur deshalb zulässig, weil die Grundrechte zum Fernmeldegeheimnis (Art 10 Abs. 1 GG), der Unverletzlichkeit der Wohnung (Art 13 Abs. 1 GG) und der informationellen Selbstbestimmung Lücken lassen, die vom Schutz der Grundrechte umfasst werden müssen [68].

Das Grundrecht … ist ... anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können [69]. Einfache Haushaltsgeräte betrifft es nicht, wenn sie nur Daten mit punktuellem Bezug zum privaten Lebensbereich des Betroffenen speichern und verarbeiten [70].

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hat bislang keine erkennbare Resonanz in der Rechtsprechung bewirkt. Was nicht weiter verwunderlich ist, weil es ein auf die Technik und ihre Vernetzungen bezogenes Schutzrecht ist, das sehr viel Ähnlichkeit mit dem Fernmeldegeheimnis hat, nur dass es nicht auf den kommunikativen Vermittlungsvorgang anspricht, sondern auf die gespeicherten und individuell bearbeiteten Daten selber, die Auskunft über persönliche Eigenschaften und Vorlieben geben.

Es ist nicht grenzenlos, setzt aber hohe Schranken für eine Eingriffsermächtigung. Sie wäre gerechtfertigt, wenn *tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen* [71].

Nach Maßgabe des BVerfG-Urteils wurde eine Ermächtigung zur Onlinedurchsuchung in das BKA-Gesetz [72] und in landesrechtliche Verfassungs-

---

[64] Siehe oben: 1.2 Dokumentation und Auswertung.

[65] **BVerfG**, Beschluss vom 16.06.2009 - 2 BvR 902/06, Rn 77 (E-Mail-Beschlagnahme)

[66] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 166

[67] Ebenda, Rn 169

[68] Ebenda, Rn 168

[69] Ebenda, Rn 203

[70] Ebenda, Rn 202

[71] Ebenda, Rn 247

[72] **CF**, Mit Hängen und Würgen und unbrauchbar,

schutzgesetze aufgenommen [73]. Ein Gesetzentwurf Bayerns zur Einführung der Onlinedurchsuchung in die StPO [74] scheiterte am Widerstand der FDP-mitgeführten Länder im Bundesrat [75].

2.4 Wohnung

Dem Schutz der Wohnung als den tiefsten Ort der persönlichen Zurückgezogenheit schützt Art 13 GG. Abs. 2 widmet sich dem Richtervorbehalt wegen der Durchsuchung (§§ 102, 103 StPO) und Abs. 3 und 4 den besonderen Voraussetzungen für den großen Lauschabgriff (§ 100c StPO), der tiefsten und am meisten eingeschränkten Eingriffsmaßnahme in der Strafprozessordnung.

Die Unverletzlichkeit der Wohnung schützt die räumliche Sphäre, *in der sich das Privatleben entfaltet*, wobei Privat-, Betriebs- und Geschäftsräume gleichermaßen geschützt werden [76]. Es schützt den Einsatz informationstechnischer Systeme, soweit sie innerhalb dieser Räume betrieben werden, nicht aber die vernetzten auswärtigen Komponenten und die Mobilgeräte *wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone* [77] und *nicht gegen die durch die Infiltration des Systems ermöglichte Erhebung von Daten, die sich im Arbeitsspeicher oder auf den Speichermedien eines informationstechnischen Systems befinden, das in einer Wohnung steht* [78].

Einschränkend für Geschäftsräume gilt: *Gespräche in Räumen, die ausschließlich zu betrieblichen oder geschäftlichen Zwecken genutzt werden, nehmen zwar am Schutz des Art 13 Abs. 1 GG teil, betreffen bei einem fehlenden Bezug des konkreten Gesprächs zum Persönlichkeitskern aber nicht den Menschenwürdegehalt des Grundrechts* [79].

2.5 Internetermittlungen und Grundrechte

Die Grundrechte bilden die stärksten individuellen Rechte. Sie werden ergänzt durch verfassungs- und einfachrechtliche Gebote (Richtervorbehalte, rechtliches Gehör, beschränkende Anwendungsvoraussetzungen), die sie unterstützen, ausprägen und gelegentlich einschränken. Dieser Abschnitt hat sich deshalb auf die wesentlichen Grundrechte konzentriert, die im Zusammenhang mit den Ermittlungen im Internet von besonderer Bedeutung sein können.

Das Fernmeldegeheimnis gewährt den Schutz der Integrität der Fernkommunikation, das Recht auf die Integrität informationsverarbeitender Systeme den Technikschutz wegen der gespeicherten und selbst verarbeiteten Daten und die informationelle Selbstbestimmung den Schutz vor staatlichen Datensammlungen und -auswertungen. Aus heutigem Wissen dürften sie alle Bereiche der Datenverarbeitung und -übermittlung abdecken.

Aus diesem Rahmen heraus fällt die Unverletzlichkeit der Wohnung, die den Technik- und Kommunikationsschutz für den tiefsten persönlichen Rückzugsbereich noch einmal verstärkt. Dieses Grundrecht hat eine besondere Bedeutung für Abhörmaßnahmen im Wohnbereich (großer Lauschangriff) und für die Onlinedurchsuchung, soweit zu ihrer Vorbereitung der Zugang zu Wohnungen oder Geschäftsräume nötig ist.

Nur der Kernbereich der Grundrechte beansprucht für sich absolute Geltung. Im Interesse der rechtsstaatlich gebotenen Rechtssicherheit, des Rechtsfriedens und damit verbunden der effektiven Strafverfolgung lässt das Verfassungsrecht grundsätzlich punktuelle Einschränkungen und mit zunehmender Stärke der Gegenrechte auch tiefere Eingriffe in grundrechtlich geschützte Bereiche zu.

21.12.2008

[73] **CF**, Online-Durchsuchung für den Verfassungsschutz, 19.01.2008

[74] **CF**, Gesetzentwurf zur Onlinedurchsuchung, 21.06.2008

[75] **CF**, im Bundesrat gescheitert, 06.07.2008

[76] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 192 (Onlinedurchsuchung)

[77] Ebenda, Rn 194

[78] Ebenda, Rn 195

[79] **BVerfG**, Urteil vom 03.03.2004 - 1 BvR 2378/98, 1 BvR 1084/99, Rn 142, 143

Sie verlangen immer nach strengen Anforderungen an die Voraussetzungen und zu einer regelmäßigen und konsequenten Prüfung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes.

Diese Zurückhaltung kennt die Cybercrime nicht. Ihre Täter nutzen alle Schwachstellen und Schwächen, um zu Erfolg und besonders zu Gewinn zu kommen. Sie setzen bedenkenlos Malware, technische Geräte und kommunikative Manipulationstechniken ein, um Daten auszuspähen, Botnetze aufzubauen oder Zahlungsvorgänge zu manipulieren.

Die Forderung nach einer allgemeinen „Waffengleichheit“ für Kriminelle und die Strafverfolgung kann in einem Rechtsstaat nicht ernsthaft erhoben werden, wenn als Flurschäden zwangsläufig auch die Rechte Unbeteiligter beeinträchtigt werden. Das wird besonders deutlich bei den „Turmdaten“. Dabei geht es darum, die Kennungen (IMSI und IMEI) aller mobilen Telekommunikations-Endgeräte zu erfassen und auszuwerten, die sich in einem umgrenzten Zeitraum an einem bestimmten Ort befunden haben. Für die Strafverfolgung geht es dabei nur darum, die Anwesenheit des mobilen Telefons eines meistens noch unbekannten Täters festzustellen und die Kontaktpersonen, mit denen er gesprochen hat. Dass Erna Müller auch mit einer Friedhofsgärtnerei und Angelo Glattelli mit einem Bordell telefoniert haben, interessiert keinen professionellen Strafverfolger. Die Daten, die diese Tatsachen belegen, müssen aber im Interesse der Aktenwahrheit gespeichert und zur Akteneinsicht des Verteidigers aufbewahrt werden, verschwinden dazu aber in einer Masse anderer Daten, unter denen sie sich nicht hervorheben.

Wegen solcher überschießenden Erhebungen von Verkehrsdaten verlangt das Gesetz (§ 100g StPO), schließlich mit Zustimmung des BVerfG [80], unter anderem den Verdacht auf eine schwere Straftat und verweist deshalb auch auf den Straftatenkatalog in § 100a Abs. 2 StPO.

Der punktuelle Zugriff auf Verkehrsdaten, wie er bei der Bestandsdatenauskunft nach § 113 TKG im Zusammenhang mit dynamischen IP-Adressen erfolgt, kennt solche hohen Schranken nicht. Ihn leitete das BVerfG 2010 nicht aus § 100g StPO ab, sondern aus der Ermittlungsgeneralklausel in § 161 Abs. 1 StPO, so dass bei jedem Verdacht auf eine Straftat ein selbständiger Auskunftsanspruch der Polizei ohne den Umweg über die Staatsanwaltschaft besteht [81].

Betroffen von der Verkehrsdatenerhebung und dem Rückgriff auf sie für eine Bestandsdatenauskunft sind dieselben Grundrechte, das informationelle Selbstbestimmungsrecht und das Fernmeldegeheimnis, aber in ganz unterschiedlicher Stärke. Das ist der Grund dafür, dass sie aus verschiedenen Eingriffsermächtigungen abgeleitet werden können [82].

Angesichts der Formen und Ausbreitung, die die Cybercrime genommen hat, wäre es fatal, die Strafverfolgung in allen wesentlichen Bereichen zu beschränken und zur Erfolglosigkeit zu verdammen. Eine – zu Recht – Freiheiten fordernde Gesellschaft ohne Biss gegen die, die sie bedenkenlos missbrauchen, muss ihre Toleranz irgendwann teuer bezahlen und das spätestens dann, wenn Angst und Verunsicherung eine so tiefe Verwurzelung erreicht haben, dass soziale Prozesse, Solidarität und Nächstenliebe der neurotischen Angst vor Missbrauch und Bösartigkeit gewichen sind.

Die Erörterung der wesentlichen Ermittlungsmethoden, die hier anschließt, hat zwei Ziele: Einerseits geht es mir darum, unsinnigen Unsicherheiten entgegen zu treten und betrachte ich die wesentlichen Maßnahmen wegen ihrer Zulässigkeit nach Gesetz, Rechtsprechung und technischem Standard. Andererseits lote ich dazu auch die Grenzen der Zulässigkeit aus, um ausufernden

[80] **BVerfG**, Urteil vom 02.03.2010 - 1 BvR 256, 263, 586/08, Leitsatz 5

[81] **BVerfG**, Beschluss vom 13.11.2010 - 2 BvR 1124/10

[82] Die jüngste Entscheidung des BVerfG verlangt aber nach mehr Normenklarheit, ohne aber die Ermittlungsgeneralklauseln zu erwähnen. Wegen der Auskünfte im Hinblick auf dynamische IP-Adressen müssen bis zum 30.06.2013 ergänzende Regeln geschaffen werden (**BVerfG**, Beschluss vom 24.01.2012 - 1 BvR 1299/05).

Eingriffen und den unweigerlichen Auseinandersetzungen in den zu erwartenden Gerichtsverfahren vorzubeugen.

3. Ermittlungsmethoden

Ungeachtet des Ermittlungsgegenstandes müssen die Ermittlungen geplant und die Erfolg versprechenden Methoden ausgewählt werden. Deshalb stellen sich zunächst immer die Fragen nach dem Anfangsverdacht, den zulässigen und den geeigneten Ermittlungsmethoden:

3.0.1 tatsächlichen Anhaltspunkte (§ 152 Abs. 2 StPO) für eine Straftat

Damit verbunden ist eine Bewertung der Fakten und die Frage, was sie einzeln betrachtet und in ihrer Gesamtschau tatsächlich aussagen [83]. Dabei ist anhand der Alltags- und der kriminalistischen Erfahrung auch zu prüfen, welchen Aussagewert sie haben [84]. Eine Orientierung ohne Anspruch auf Messgenauigkeit gibt dazu das von mir vorgeschlagene Modell vom Geltungsgrad [85]. Dadurch lassen sich starke und unsichere Fakten bestimmen und kann es sich anbieten, zunächst die unsicheren zu überprüfen.

3.0.2 welche Straftat kommt in Betracht?

Mit dieser Frage ist zunächst die klassische Subsumtion verbunden, also die Prüfung eines Sachverhalts anhand eines gesetzlichen Tatbestandes. Das Ergebnis gibt sogleich Auskunft über die Schwere der in Betracht kommenden Straftat [86], die für die Auswahl der Ermittlungsmethoden und die ständige Frage nach der Verhältnismäßigkeit [87] von ausschlaggebender Bedeutung ist. Danach entscheidet sich auch, ob tiefer in Grundrechte eingreifende Maßnahmen überhaupt in Betracht kommen.

3.0.3 Wahl der Mittel

Die Frage nach der Wahl der Mittel verlangt nach einer Bewertung der Erfolgsaussichten verschiedener Ermittlungsmaßnahmen. Bei gleicher Erfolgserwartung ist – dem Verhältnismäßigkeitsprinzip folgend – das mildere Mittel zu wählen. Mehrere Vorschriften zu schweren Eingriffsmaßnahmen heben diese Verpflichtung nochmals hervor (zum Beispiel §§ 100a Abs. 1 Nr. 3, 100c Abs. 1 Nr. 4, 100g Abs. 1 S. 2 StPO [88]), obwohl die Prüfungspflicht immer besteht.

An die Eignung der Beweismittel und Zulässigkeit der Eingriffsmaßnahme stellt das Gesetz unterschiedliche Anforderungen. Ganz niedrig setzt § 94 Abs. 1 StPO wegen der Beweisgegenstände an. Sie *sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen*, soweit ihnen auch nur eine potentielle Beweisbedeutung zukommt (wenn sie *als Beweismittel für die Untersuchung von Bedeutung sein können*). Folgerichtig lässt dagegen § 100a Abs. 1 Nr. 3 StPO die Überwachung der Telekommunikation erst zu, wenn ohne sie die *Erforschung des Sachverhalts ... auf andere Weise wesentlich erschwert oder aussichtslos wäre*.

Entscheidend für die Zulässigkeit einer Maßnahme ist auch die Rolle des Betroffenen. Wegen der Durchsuchung setzt § 102 StPO wieder einen niedrigen Maßstab an. Das gilt zunächst für den Verdachtsgrad: Die Maßnahme ist bereits gegenüber dem Verdächtigen im Rahmen der Vorermittlungen [89] zulässig, ohne dass sich der Verdacht bereits so stark verdichtet hat, dass die Straftat und die Beteiligung des (jetzt:) Beschuldigten wegen ihrer wesentlichen Einzelheiten bekannt sind (siehe Belehrung gemäß § 136 Abs. 1 S. 1 StPO).

---

[83] A.5 Geltung von Beweisen und Erfahrungen

[84] A.5.1 Geltung;
A.5.2 Geltung und Wechselwirkungen.

[85] A.5.3 Kategorisierung des Geltungsgrades

[86] Kasten: Straftaten von erheblicher Bedeutung

[87] Das Gebot der Verhältnismäßigkeit wird aus dem Rechtsstaatsprinzip abgeleitet und bindet nach Art 20 Abs. 3 GG die Rechtsprechung und die Exekutive. Siehe auch: A.1 Staatsanwaltschaft und Strafverfolgung.

[88] Das BVerfG beschränkt die Verwertung von Vorratsdaten wegen Straftaten nach § 100g Abs. 1 Nr. 2 StPO auf ihrerseits schwere Straftaten; **BVerfG**, Urteil vom 02.03.2010 - 1 BvR 256, 263, 586/08, Leitsatz 5, S. 2.

[89] A.4 Eingriffsrechte während der Vorermittlungen

Auch im Hinblick auf die gesuchten Gegenstände setzt § 102 StPO einen niedrigen Maßstab, weil bereits die Vermutung ausreicht, *dass die Durchsuchung zur Auffindung von Beweismitteln führen werde*. Dabei darf die Vermutung auch auf gesicherten Alltags- und kriminalistischen Erfahrungen beruhen.

Erheblich höher setzt § 103 StPO die Schwellen für die Durchsuchung beim unbeteiligten Dritten. Die Vorschrift verlangt nach einem verdichteten Verdacht (*Verfolgung von Spuren einer Straftat*) und konkrete Anhaltspunkte dafür, *dass die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet*. Ähnlich verhält sich § 99 StPO, der *die Postbeschlagnahme nur wegen der an den Beschuldigten gerichteten* (oder von ihm stammenden) *Postsendungen* zulässt.

Wegen Angehöriger oder Berufshelfer gewähren zum Beispiel die §§ 52, 53 StPO Zeugnisverweigerungsrechte, § 97 StPO Beschlagnahmeverbote und § 161a StPO gestaffelte Erhebungs- und Verwertungsverbote.

3.0.4 Eilbedürftigkeit

Auch der Zeitfaktor spielt bei der Wahl der Mittel eine bedeutende Rolle. Häufig zurückgestellt werden können Zeugenvernehmungen, wenn durch sie andere Ermittlungen gefährdet werden könnten. Auf der Erinnerung beruhende Aussagen verlieren zwar mit zunehmendem zeitlichen Abstand zum tatsächlichen Geschehen an Wert. Eine zwingende Notwendigkeit zur unverzüglichen Sicherung von Zeugenaussagen kann daraus nicht abgeleitet werden, weil ernsthafte Erinnerungslücken und persönliche -färbungen erst mit deutlichem zeitlichen Abstand zu erwarten sind. Aber auch unbefangene Äußerungen können unter dem Eindruck des Geschehens getrübt und unvollständig sein.

Ein unverzügliches Handeln der Staatsanwaltschaft verlangen hingegen § 143 Abs. 2 GVG und § 160 Abs. 2 StPO bei verderblichen Beweismitteln, *deren Verlust zu besorgen ist*. Diese Pflicht überträgt § 163 Abs. 1 S. 1 StPO auf die Polizei als Ermittlungspersonen der Staatsanwaltschaft (§ 152 Abs. 1 GVG). Deshalb ist bei der Wahl der Mittel auch die Frage nach der Eilbedürftigkeit von Ausschlag. Sie bekommt Brisanz zum Beispiel dann, wenn Verkehrsdaten als Beweismittel in Betracht kommen. Seitdem die Vorratsdatenspeicherung in der vom Gesetzgeber vorgesehenen Form vom BVerfG untersagt wurde, sind die nach § 96 TKG gespeicherten Verkehrsdaten vollständig nur etwa eine Woche lang verfügbar. Deshalb kann die Erhebung der Verkehrsdaten, wenn der Anfangsverdacht sie rechtfertigt, nicht bis zur Absicherung des Verdachts zurückgestellt und muss der von § 100g Abs. 2 StPO geforderte Gerichtsbeschluss eingeholt werden.

Für den hier gebotenen Überblick müssen die gezeigten Beispiele genügen. Sie belegen, dass besonders im Anfangsstadium eines Ermittlungsverfahrens eine solide Bestandsaufnahme gefordert ist, die bei den bekannten Tatsachen und ihren Aussagewerten ansetzt. Aus ihnen leiten sich der Anfangsverdacht und die Frage nach den Erfolg versprechenden und gleichzeitig zulässigen Ermittlungsmethoden ab, die immer auch unter dem Gebot der Verhältnismäßigkeit zu prüfen sind.

In den anschließenden Kapiteln werden die im Zusammenhang mit dem Internet wesentlichen Ermittlungsmaßnahmen vorgestellt.

3.0.5 materielles Cybercrime-Strafrecht

Das auf die Cybercrime passende materielle Strafrecht kann nur im Überblick vorgestellt werden. Die erste Tabelle <Folgeseite> zeigt die verschiedenen Regelungsbereiche und die einschlägigen Einstiegsnormen. Vor Allem der Funkschutz ist unvollständig, weil er das Abhören des Funks für die Frequenzen des Amateurfunks nicht verbietet [90]. Die IT-spezifischen Frequenzbänder für drahtlose Netze und den Nahfunk liegen ganz überwiegend in den Frequenzbereichen, die dem Amateurfunk zugewiesen sind.

---

[90] **CF**, Abgrenzungen, 2007

Betrug und Untreue	Programme	§ 263a Abs. 3 StGB
Funkschutz	Abhörverbot	§§ 148 Abs. 1 Nr. 1, 89 TKG
Geld- und Wertzeichenfälschung	Programme, Vorrichtungen	§ 149 StGB
gemeingefährliche Straftaten	TK-Einrichtungen	§ 317 StGB
persönlicher Lebens- und Geheimbereich	Ausspähen	§ 202a StGB
	Abfangen	§ 202b StGB
	Hackerparagraph	§ 202c StGB
	Fernmeldegeheimnis	§ 206 StGB
Sachbeschädigung	Datenveränderung	§ 303a StGB
	Computersabotage	§ 303b StGB
sexuelle Selbstbestimmung	Kinderpornographie	§ 184b StGB
Urheberrecht	Kopierschutz	§ 108b UrhG
Urkundenfälschung	technische Aufzeichnungen	§ 268 StGB
	beweiserhebliche Daten	§ 269 StGB
	Datenverarbeitung	§ 270 StGB
Wettbewerbsrecht	Geschäftsgeheimnis	§ 17 UWG

Die Beispiele zeigen, dass der Gesetzgeber auf viele neue Erscheinungsformen bereits reagiert hat. Eine saubere Systematik fehlt dem Regelwerk hingegen. Die Strafvorschriften wirken mehr zufällig bestehenden Regelungsbereichen zugeordnet und eine klare Struktur bei den strafbaren Vorbereitungshandlungen fehlt völlig.

Das belegt umso mehr die Grafik auf der <nächsten Seite>. Sie zeigt die einschlägigen Tatbestände unter dem Gesichtspunkt der Strafdrohung und der Strafrahmen. Die oben aufgeführten, hellblau unterlegten Tatbestände gehören der einfachen und mittleren Kriminalität an.

Die Darstellung belegt eine ungewöhnliche Handhabung des Gesetzgebers. Einerseits enthält sie überraschend viele Tatbestände, die im Bagatellbereich mit Höchststrafen bis zu zwei Jahren Freiheitsstrafe angesiedelt sind. Allein drei Tatbestände davon widmen sich den sonst straflosen Vorbereitungshandlungen, auch das ist ungewöhnlich.

Das „Mittelfeld“ mit Höchststrafen zwischen drei und fünf Jahren Freiheitsstrafe ist dagegen außerordentlich dünn bestellt (unteres Hell- und Mittelblau). Das ändert sich wieder bei den schweren Straftaten und Strafdrohungen, die wiederum besonders stark ausgeformt wurden (ganz unten).

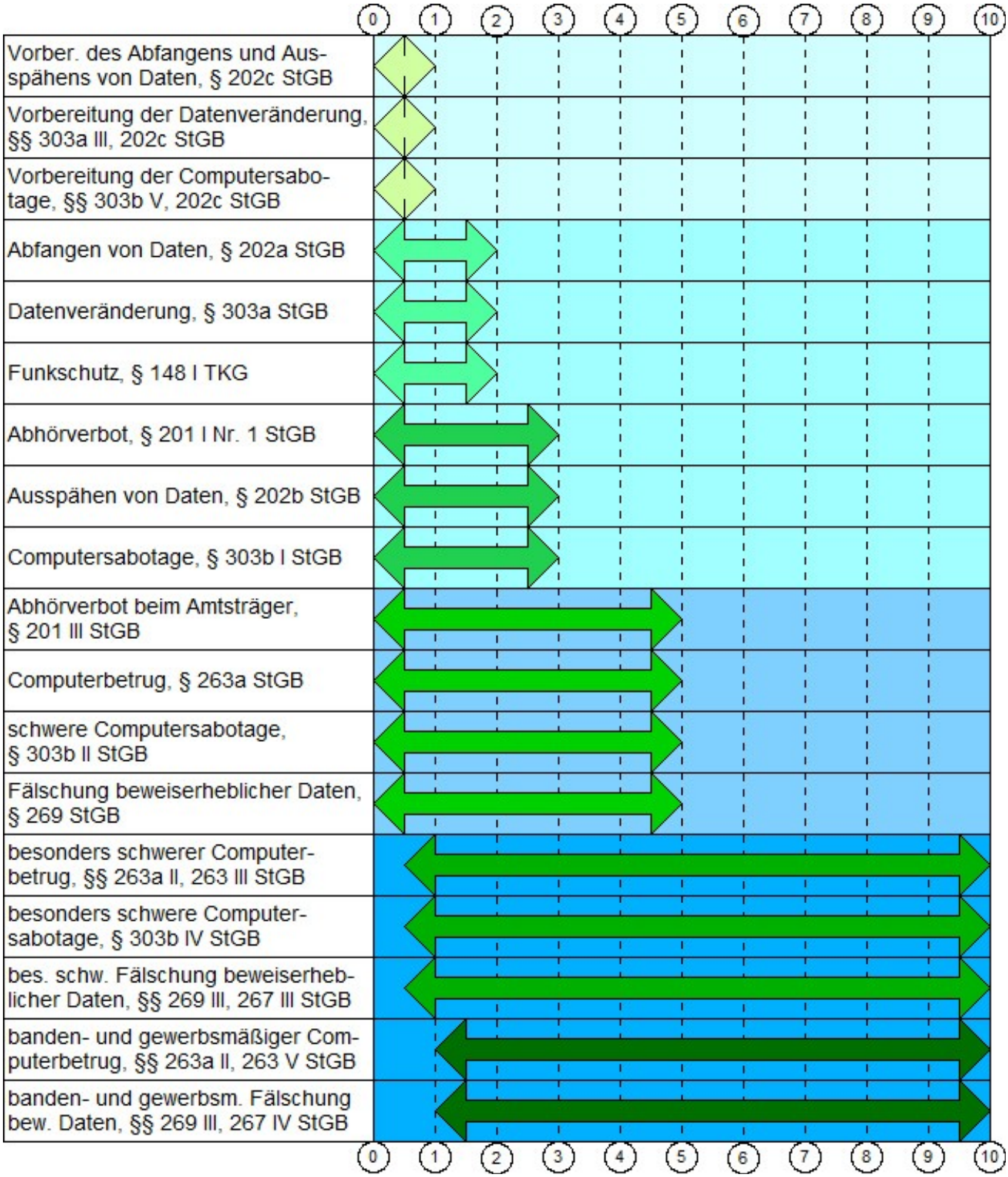
Das Skimming bleibt in der Aufstellung außer Betracht [91]. Seine Grundtatbestände sind im Verbrechensbereich angesiedelt (§ 152b StGB) und das sonst straflose Vorbereitungsstadium wird ungewöhnlich starken Strafdrohungen unterworfen (§ 149 StGB).

Den Abschluss bildet eine Tabelle <S. 25>, die einen Überblick über die Ermittlungsmaßnahmen gibt, die für die Strafverfolgung im Zusammenhang mit Internetdelikten von besonderer Bedeutung sind. Sie werden in den anschließenden Kapiteln ausgiebig erörtert.

Die Tabelleneinträge sind nach der Eingriffstiefe der Ermittlungsmaßnahmen sortiert. Den Maßnahmen werden deshalb Angaben zur Schwere der vorausgesetzten Kriminalität und zur Anordnungskompetenz zur Seite gestellt, wobei „Polizei“ bedeutet, dass alle mit der Strafverfolgung betrauten Behörden die Maßnahme anordnen können. <weiter S. 24>

[91] **Kochheim**, Skimming, #2.21, 22.04.2011

Kochheim, Verdeckte Ermittlungen im Internet, S. 23



<von S. 23> Das Kürzel „GiV“ bedeutet „Gefahr im Verzug“ und kennzeichnet, dass Eilanordnungen auch von der Staatsanwaltschaft oder der Polizei getroffen werden können. Die Ermittlungsgeneralklausel wird nicht gesondert aufgeführt und steckt hinter der Angabe „§ 161 I“.

Die Aufstellung beginnt mit den einfachen Recherchen im Internet, die vom BVerfG als Maßnahmen ohne Eingriffstiefe behandelt werden [92]. Die personalen Ermittlungsmethoden (Observationen, Verdeckter Ermittler) sind durchweg im Bereich der erheblichen Straftaten angesiedelt und die technischen Maßnahmen dürfen mit Ausnahme einzelner Observationshilfen nur zur Bekämpfung der schweren Kriminalität eingesetzt werden.

Bei den Ermittlungen mit Internetbezug wird häufig technisches und rechtliches Neuland betreten, so dass die Sachleitungsbefugnis [93] der Staatsanwaltschaft (§§ 152 Abs. 1 GVG, 161 Abs. 1 S. 1 StPO) sehr ernst genommen und auch die Maßnahmen, die die Polizei aus eigener Kompetenz anordnen kann, eng mit ihr abgestimmt werden müssen. Das gilt ganz besonders für die Einsätze technischer Oberservationshilfen [94], bei Keuschheitsproben, Scheingeschäften und Nicht offen ermittelnder Beamter sowie für die Einzelheiten ihrer Legendierung. Insoweit ist ein ***schriftliches Konzept*** zu fordern, das Aktenbestandteil wird (§ 168b Abs. 1 StPO) und ausdrücklich von der Staatsanwaltschaft genehmigt werden muss:

- Die Maßnahme wird damit umgrenzt, so dass die Staatsanwaltschaft die ihr wie dem Gericht obliegende Kontrolle der Art und Weise von Eingriffsmaßnahmen gerecht werden kann [95]. Das ist besonders wichtig wegen der Tiefe der Legendierung und der geplanten Dauer des Einsatzes.
- Die Staatsanwaltschaft wird in die Lage versetzt, die verfahrensrechtlichen Folgen abzuschätzen und vorzubereiten (Rechtsmittel, Mitteilungen ua).
- Alle anderen Verfahrensbeteiligten (Gericht, Verteidiger usw.) werden offen über die Ermittlungsschritte und über die Beweggründe informiert, die für sie ausschlaggebend waren. Das beugt häufigem Unverständnis und Streiten in der gerichtlichen Hauptverhandlung vor.

---

92 3.3 personale Ermittlungen

93 A.2 Verhältnis zur Polizei

Aus der Sachleitungsbefugnis folgert das BVerfG einen generellen Vorrang für die Sachentscheidungen der StA;
BVerfG, Beschluss vom 28.07.2008 -2 BvR 784/08, Rn 10.

94 3.2.1 technische Observationshilfen

95 Argument aus: **BVerfG**, Urteil vom 20.02.2001 - 2 BvR 1444/00, Rn 28. Siehe auch:
A.1 Staatsanwaltschaft und Strafverfolgung.

Maßnahme		StPO		Straftaten	Sanktion, Bemerkungen
allgemeine Informationen aus dem Internet	3.3	§ 161 I	Polizei	alle	
Newsletter, Foren, Informationssammlungen	3.3	§ 161 I	Polizei	alle	
Beteiligung an Diskussionen	3.3	§ 161 I	Polizei	alle	
einfache Legendierung (Fake Account)	3.3	§ 161 I	Polizei	alle	
Auskünfte von Behörden und anderen Einrichtungen	3.1.1	§ 161 I	Polizei	alle	Das BVerfG fordert jetzt zusätzliche normenklare Regeln (vor allem wegen der dynamischen IP-Adressen).
Herausgabeersuchen	3.1.6	§ 95 I	Polizei	alle	§ 95 II (Gericht)
Bestandsdaten von Provider	3.1.2	§ 161 I	Polizei	alle	Bußgeld. Siehe „Auskünfte“.
technische Observationshilfen	3.2.1	§ 100h	Polizei	alle	kurzfristige Observation, einmalig
kurzfristige Beobachtung von Verdächtigen und Beschuldigten	3.3.4	§ 161 I	Polizei	alle	
Staatsanwaltschaftliches Auskunftsersuchen	3.1.5	§ 161a	StA	alle	§ 161a II (Gericht)
Beschlagnahme	3.1.7	§ 94 II	Gericht, GiV	alle	Zwang
Verkehrsdaten und Dateien in Mobilgeräten	3.1.3	§§ 94, 100g III	Gericht, GiV	alle	Zwang
Dateien beim Hostprovider	3.1.9	§ 94 II	Gericht, GiV	alle	Zwang
Beschlagnahme von E-Mails	3.1.8	§§ 95, 99, 110 I	Gericht, GiV	alle	§ 95 II (Gericht)
offene Ferndurchsuchung	3.1.10	§ 110 III	Gericht, GiV	alle	Zwang. Annex zu §§ 102, 103
technische Observationshilfen	3.2.1	§ 100h	Gericht, GiV	erhebliche	längerfristige Observation
Scheinkauf	3.3.5	Rspr.	StA, GiV	erhebliche	
Keuschheitsprobe	3.3.6	Rspr.	StA, GiV	erhebliche	
Nicht offen ermittelnder Beamter	3.3.4	Rspr.	StA, GiV	erhebliche	„NoeP“
dauerhafte legendierte Beobachtung	3.3.4	§ 110b I	StA, GiV	erhebliche	Verdeckter Ermittler
Beobachtung von Beschuldigten ohne Kommunikation	3.3.4	§ 163f	StA, GiV	erhebliche	Längerfristige Observation
Beobachtung von Beschuldigten mit Kommunikation	3.3.4	§ 110b II	Gericht, GiV	erhebliche	Verdeckter Ermittler
IMSI-Catcher	3.2.3	§ 100i	Gericht, GiV	erhebliche	
Verkehrsdaten, Standortdaten	3.1.4	§ 100g	Gericht, GiV	schwere	§§ 100b III, 95 II
Überwachung der Telekommunikation	3.2.2	§ 100a	Gericht, GiV	schwere	§§ 100b III, 95 II
Serverüberwachung	3.2.4	§ 100a	Gericht, GiV	schwere	§§ 100b III, 95 II
Quellen-TKÜ	3.2.5	§ 100a	Gericht, GiV	schwere	§§ 100b III, 95 II
Onlinedurchsuchung	3.2.6	verboten			
Quellen-Zugriff auf nicht kommunikative Aktivitäten	3.2.7	verboten			
Spyware	3.2.8	verboten			

3.1 Auskünfte und Sachbeweise

Die Strafprozessordnung unterscheidet im Wesentlichen zwischen dem Personen- und dem Sachbeweis, wobei die besonderen Ermittlungsermächtigungen ab § 98a StPO nicht immer genau zugeordnet sind. Die Betrachtung beginnt deshalb mit den eher klassischen Methoden der Auskünfte und Sachbeweise.

3.1.1 Auskünfte von Behörden und anderen Einrichtungen

Die Ermittlungsgeneralklausel – EGK – des § 161 Abs. 1 S. 2 StPO ermächtigt die Staatsanwaltschaft dazu, wegen jeder Straftat *von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art* durchzuführen, die, so das BVerfG, *weniger intensiv in Grundrechte des Bürgers eingreifen* [96]. *Die Staatsanwaltschaft kann auf dieser Grundlage in freier Gestaltung des Ermittlungsverfahrens die erforderlichen Maßnahmen zur Aufklärung von Straftaten ergreifen ... § 161 Abs. 1 StPO bildet auch die Rechtsgrundlage für die allgemeine Erhebung personenbezogener Daten (...) und damit für eine Ermittlungsanfrage der Staatsanwaltschaft gegenüber privaten Stellen …* [97]. Diese Ermächtigung überträgt § 163 Abs. 1 S. 2 StPO auf die Polizei, wenn sie im Auftrag der Staatsanwaltschaft ermittelt [98] oder im Ersten Zugriff handelt (§ 163 Abs. 1 StPO).

Die grundsätzliche Ermächtigung zur Erteilung behördlicher Auskünfte leitet sich aus der Pflicht zur Amtshilfe ab (Art 35 Abs. 1 GG). Die Strafprozessordnung lässt mit § 96 StPO ausnahmsweise verwaltungsrechtliche Sperrerklärungen zu, wenn die *oberste Dienstbehörde erklärt, dass das Bekanntwerden des Inhalts dieser Akten oder Schriftstücke dem Wohl des Bundes oder eines deutschen Landes Nachteile bereiten würde*. Solche Sperrerklärungen müssen von den Strafverfolgungsbehörden akzeptiert werden [99], wenn sie nicht offensichtlich willkürlich erfolgt sind [100]. Der schlichten Weigerung von Behörden (ohne Sperrerklärung), Auskünfte oder Akten herauszugeben, kann mit den Zwangsmitteln der StPO begegnet werden [101].

Weitere Einschränkungen ergeben sich aus dem Gebot der Schwellengleichheit [102] (§§ 161 Abs. 2, 477 Abs. 2 S. 2 StPO) und aus besonderen Gesetzen, die zum Beispiel das Steuer- (§ 30 AO) oder das Sozialgeheimnis betreffen (§ 73 SGB 10). Soweit solche Gesetze Öffnungsklauseln zu Zwecken der Strafverfolgung aufweisen, akzeptiert das BVerfG sie großzügig im Allgemeininteresse an einer effektiven Strafverfolgung [103].

Die EGK hat das Problem der fehlenden Ungehorsamsfolgen. Solche sehen nur § 95 Abs. 2 StPO wegen des Herausgabeverlangens [104], das auch von der Polizei mit dem Hinweis auf die Folgen verbunden werden kann [105], und § 161a Abs. 2

---

96 **BVerfG**, Beschluss vom 17.02.2009 - 2 BvR 1372/07, Rn 26

97 Ebenda. Wegen der Verweise: **CF**, BVerfG: Direkte Auskunft über Bestandsdaten, 15.06.2011.

98 Wegen der Bestandsdaten hat das BVerfG einen selbständigen Auskunftsanspruch der Polizei im Rahmen der EGK festgestellt: **BVerfG**, Beschluss vom 13.11.2010 - 2 BvR 1124/10.

99 **BGH**, Urteil vom 16.02.1995 - 4 StR 733/94

100 Gute Zusammenfassung bei: **LG Potsdam**, Beschluss vom 08.08.2006 - 21 Qs 127/06.

101 Siehe schon: Heinz **Lohmeyer**, Beschlagnahme von Fahndungsakten und Steuergeheimnis, JR 1964, 171 (Faksimile).

102 Gebot der Schwellengleichheit

103 Zum Beispiel wegen der allgemeinen Auskunftsberechtigung der BAFin auf Kontoanfragen gemäß § 24c Abs. 3 S. 1 Nr. 2 KWG: **BVerfG**, Beschluss vom 13.06.2007 - 1 BvR 1550/03, 2357/04, 603/05, Rn 127.

104 Erst 2000 erkannte das erste Gericht einen strafbewehrten Herausgabeanspruch der Staatsanwaltschaft an, dem später die herrschende Meinung folgte: **LG Lübeck**, Beschluss vom 03.02.2000 - 6 Qs 3/00.

105 Ordnungsgeld, Ordnungshaft und Beugehaft kann nur das Gericht anordnen. Ob dem eine gerichtliche Androhung der Ungehorsamsfolgen vorausgehen muss, ist streitig. Die überwiegende Meinung in der Kommentarliteratur scheint die polizeiliche Androhung ausreichen zu lassen.

StPO wegen des staatsanwaltschaftlichen Auskunftsersuchens vor. Eine Stärkung der Polizei würde die im Koalitionsvertrag 2009 vorgesehene *Erscheinenspflicht von Zeugen vor der Polizei* [106] haben, die bislang nicht umgesetzt wurde.

Somit hat die EGK vor allem die Wirkung, dass sie die Herausgabe von Informationen, Schriftstücken und anderen Beweismitteln von Behörden und privaten Einrichtungen in aller Regel freizeichnet, sie aber nicht als solche erzwungen werden können. Dazu bedarf es anderer Instrumente aus der StPO.

3.1.2 Bestandsdaten

Zur Abfrage der Bestandsdaten bei den Zugangsprovidern und den Telemediendiensten [107] ist auch die Polizei aufgrund der Ermittlungsgeneralklausel des § 161 Abs. 1 S. 2 StPO in Verbindung mit § 113 TKG beziehungsweise § 14 TMG ermächtigt [108]. Neue Grenzen hat aber das BVerfG im Zusammenhang mit dem Manuellen Auskunftsverfahren (§ 113 TKG) und den Auskünften über die Nutzung dynamischer Internetadressen gesetzt [109], die nicht nur dem Telekommunikationsgeheimnis unterliegen, sondern auch nach normenklaren Auskunftsrechten der Strafverfolgungsbehörden verlangen. Es gilt eine Übergangsfrist bis zum 30.06.2013. Die Auskunftsverweigerung seitens der Zugangsprovider ist gemäß § 149 Abs. 1 Nr. 33 TKG bußgeldbewehrt [110]. Wegen der fehlenden Sanktionen nach der StPO siehe oben [111].

Bei der Bestandsdatenauskunft handelt es sich um einen nur punktuellen Zugriff auf Verkehrsdaten, auch wenn es dabei um die Auflösung dynamischer IP-Adressen geht (mittelbare Nutzung [112]). Er ist nach der bisher geltenden Rechtsprechung bei jeder Kriminalitätsform zugelassen, was auch der 1. Senat des BVerfG jetzt nicht ausdrücklich in Frage stellt.

3.1.3 Verkehrsdaten und Dateien in Mobilgeräten

Die in Mobilgeräten gespeicherten Verkehrsdaten und Dateien unterliegen nach § 100g Abs. 3 StPO ausdrücklich ***nicht*** dem besonderen Schutz dieser Vorschrift [113]. Als körperliche Gegenstände unterliegen die Geräte der gerichtlichen Beschlagnahme (§§ 94 Abs. 2, 98 StPO [114]), ohne dass Beschränkungen wegen der Schwere der Kriminalität bestehen. Sobald sich die Geräte im amtlichen Gewahrsam befinden (Sicherstellung), können sie auch ausgelesen werden. Die Daten als solche genießen keinen besonderen Schutz, der über die gegenständliche Beschlagnahme hinaus geht [115]. Allerdings *muss der Zugriff auf für das Verfahren bedeutungslose Informationen im Rahmen des Vertretbaren vermieden werden* [116]. Diese Einschränkung hat der BGH 2009 für die Beschlagnahme von E-Mails präzisiert und dafür ein dreistufiges Modell vorgeschrieben, das zunächst einen gerichtlichen Herausgabebeschluss nach Maßgabe der Anspruchsvoraussetzungen der Postbeschlagnahme (§§ 95, 99 StPO), eine Durchsicht der Daten (§ 110 Abs. 1 StPO)

---

[106] Koalitionsvertrag zwischen CDU, CSU und FDP, 24.10.2009, Zeile 5006.

[107] Die unsinnige Unterscheidung zwischen den Telediensten (Bundesrecht) und den Mediendiensten (Landesrecht, Staatsvertrag) ist mit dem TMG seit dem 26.02.2007 aufgegeben worden.

[108] **BVerfG**, Beschluss vom 13.11.2010 - 2 BvR 1124/10

[109] **BVerfG**, Beschluss vom 24.01.2012 - 1 BvR 1299/05

[110] Die zuständige Verwaltungsbehörde ist die Bundesnetzagentur - § 149 Abs. 3 TKG.

[111] 3.1.1 Auskünfte von Behörden und anderen Einrichtungen

[112] So auch schon: **BVerfG**, Urteil vom 02.03.2010 - 1 BvR 256, 263, 586/08, Leitsatz 6.

[113] Anders noch: **BVerfG**, Beschluss vom 04.02.2004 - 2 BvR 308/04. Jetzt gilt: **BVerfG**, Urteil vom 02.03.2006 - 2 BvR 2099/04.

[114] Bei Gefahr in Verzug: Anordnung der StA oder der Polizei (§ 98 Abs. 1 S. 1 StPO).

[115] **BVerfG**, Beschluss vom 12.04.2005 - 2 BvR 1027/02

[116] Ebenda, Leitsatz 2.

und schließlich einen abschließenden Beschlagnahmebeschluss (§§ 94 Abs. 2, 98 StPO) umfasst [117]. Dabei kommt aber ausdrücklich das Fernmeldegeheimnis (Art 10 GG) zum Tragen [118], so dass diese Rechtsprechung nicht auf die körperliche Beschlagnahme von Datenträgern übertragbar ist.

3.1.4 Verkehrsdaten und Funkzellendaten

Die Verkehrsdaten geben Auskunft über die äußeren Umstände der Telekommunikation und nehmen deshalb am Schutz des Fernmeldegeheimnisses teil (Art 10 GG) [119]. Auch nach dem Urteil des BVerfG zur Vorratsdatenspeicherung [120] lässt § 100g StPO die Verwertung der nach § 96 TKG gespeicherten und die Protokollierung der „laufenden" Verkehrsdaten aufgrund eines gerichtlichen Beschlusses oder einer Anordnung der Staatsanwaltschaft bei Gefahr im Verzug zu [121]. Als Hürde setzt das Gesetz, dass die Maßnahme nur zur Aufklärung schwerer Straftaten zugelassen ist [122], für die § 100a Abs. 2 StPO keine abschließende Aufzählung, aber eine gesicherte Basis liefert.

Von besonderem praktischen Interesse sind die ***Standortdaten*** (§ 98 TKG, § 100g Abs. 1 S. 3 StPO). Sie geben einerseits Auskunft über die örtliche Lage der Funkzelle, in der sich ein mobiles Endgerät aktuell befindet oder zu einem bestimmten Zeitpunkt in der Vergangenheit befunden hat, so dass sich mit ihnen Bewegungsprofile erstellen lassen, wenn sie für einen längeren Zeitraum zur Verfügung stehen. Damit lässt sich im Nachhinein nachvollziehen, ob ein Beschuldigter als Täter einer bestimmten Tat in Betracht kommt, weil sich jedenfalls sein Handy zur Tatzeit am Tatort aufgehalten hat. Dagegen liefern die Standortdaten keinen zwingenden Beweis für die Täterschaft. Sie benennen nur den geographischen Kegel einer Antenne [123], die mit dem Handy Kontakt gehabt hat. Wer das Gerät bei sich geführt hat, lässt sich daraus nicht ablesen. Dieser Schluss muss aus anderen Tatsachen geschlossen werden, zum Beispiel aus markanten Ortswechseln, die durch Spuren belegt sind, oder typischen Wiederholungen im Täterverhalten. Umgekehrt aber vermittelt das Fehlen von Standortdaten den ersten Anschein, dass sich der Täter eben nicht am Tatort befunden hat [124].

Bei einer laufenden Protokollierung der Standortdaten lässt sich nicht nur das Antennensegment erkennen, in dem sich das Handy befindet, sondern aus der Signallaufzeit auch seine Entfernung zum Antennenmast und anhand des Abstrahlwinkels lässt sich seine Position im Kegel errechnen [125]. Das kann in Betracht kommen, um einen Täter zu identifizieren oder um ihn festzunehmen.

Die Standortdaten sind andererseits für die Funkzellenauswertungen von Bedeutung, auf die unter dem Stichwort „Turmdaten" bereits eingegangen wurde [126]. Ihre Auswertung anhand verschiedener Tatorte lässt Übereinstimmungen wegen der anwesenden Handys erwarten und ihrer Verbindungen zu den Hinterleuten. Das ist zum Beispiel bei den Ermittlungen wegen Skimming-Taten sehr erfolgreich gewesen.

Vorratsdaten sind Verkehrsdaten, für die nur eine längere Speicherdauer vorgeschrieben ist. Das Verbot der Vorratsdatenspeicherung schränkt die

---

[117] 3.1.8 Beschlagnahme von E-Mails

[118] 2.1 Telekommunikationsgeheimnis

[119] 2.1 Telekommunikationsgeheimnis

[120] **BVerfG**, Urteil vom 02.03.2010 - 1 BvR 256, 263, 586/08

[121] Wegen der Formvorschriften verweist § 100g Abs. 2 StPO vor allem auf § 100b StPO. Danach bedarf die Anordnung der Schriftform und die staatsanwaltschaftliche Anordnung der gerichtlichen Bestätigung binnen drei Werktage.

[122] 1. Internet und Strafverfahrensrecht

[123] **CF**, Funkzellen, 23.08.2008

[124] Besonders versierte Täter greifen deshalb wieder auf Amateurfunkgeräte zurück, schalten ihr Handy in Tatortnähe ab oder wechseln die SIM-Karte aus.

[125] **CF**, Positionsbestimmung in Funknetzen, 17.09.2008

[126] 2.5 Internetermittlungen und Grundrechte

Strafverfolgung empfindlich ein [127] und das vor allem wegen der katalogfreien Bestandsdatenauskünfte [128]. Im Zusammenhang mit der einfachen und mittleren Kriminalität fällt den Betroffenen meistens erst lange nach Ablauf einer Woche auf, dass sie das Opfer einer Straftat geworden sind [129]. Sie haben beim gegenwärtigen Stand kaum eine Chance, gegen die hinter dynamischen IP-Adressen – oder Anonymisierern [130] - getarnten Täter ihre Ansprüche durchzusetzen oder durch Bestrafung eine gewisse Genugtuung zu erfahren.

Das politisch favorisierte Konzept vom „Quick Freeze“ [131] setzt eine laufende Beobachtung oder eine schnelle Reaktion auf die Aufzeichnungen von Sensoren voraus, um die verdächtigen Verkehrsdaten einzufrieren oder zu protokollieren. Das Vorbild dafür liefert der zynische Teil der Abmahner, die aus der Überwachung von Filesharing-Netzwerken und der Durchforstung von Hostspeichern ein Geschäftsmodell gemacht haben [132]. Die Zahlen sprechen für sich: Jeden Monat erteilen die Zugangsprovider 300.000 Bestandsdatenauskünfte an die privaten Schutzrechtverfolger [133]. Nur ein weiteres Prozent davon dürfte auf Anfragen der Strafverfolgungsbehörden beruhen [134].

Als Alternative zur sechsmonatigen Vorratsdatenspeicherung ist das „Quick Freeze“ ungeeignet [135]. Besonders peinlich an der politischen Auseinandersetzung in diesem Zusammenhang ist, dass das Einfrieren kurzfristig gespeicherter und die Protokollierung laufender Verkehrsdaten geltendes Recht geblieben ist. § 100g StPO spricht davon, dass Verkehrsdaten „erhoben“ werden dürfen, und das umfasst die gespeicherten und aktuell protokollierten Daten gleichermaßen.

3.1.5 Staatsanwaltschaftliches Auskunftsersuchen

Zeugen und Sachverständige werden von § 161a Abs. 1 StPO verpflichtet, auf Ladung bei der Staatsanwaltschaft zu erscheinen und zur Sache auszusagen. Das unentschuldigte Ausbleiben oder die Weigerung ist in der Weise strafbewehrt (§§ 161a Abs. 2, 70 StPO), dass die Staatsanwaltschaft selber die Kosten und ein Ordnungsgeld auferlegen (Art 6 EGStGB) und bei Gericht die Anordnung von Ordnungs- und Erzwingungshaft beantragen kann.

Mehrfach lässt die Strafprozessordnung im Ermittlungsverfahren anstelle der mündlichen und protokollierten Aussage eine schriftliche Äußerung zu (§§ 82, 136 Abs. 1 S. 4, 158 Abs. 1 S. 1, 163a Abs. 1 StPO). In ständiger Praxis ist deshalb anerkannt, dass in geeigneten Fällen auf § 161a StPO auch Ersuchen um schriftliche Auskünfte gestützt werden können, deren Missachtung die Ungehorsamsfolgen auslösen können. Vor allem im Umgang mit Banken und anderen Wirtschaftsunternehmen hat sich das Auskunftsersuchen als erfolgreiches Instrument bewährt, allseits aufwändige Zeugenvernehmungen zu vermeiden.

Herausgabeersuchen in Bezug auf Gegenstände, Urkunden und andere Schriftstücke können auf das Auskunftsersuchen nicht allein gestützt werden, sondern nur in Verbindung mit § 95 StPO (siehe unten).

---

[127] **CF**, Bestandsdatenauskünfte und Rechtsschutzverweigerung, 06.03.2011

[128] **CF**, Bestandsdaten: mittelbare Nutzung, 06.03.2011; 3.1.2 Bestandsdaten.

[129] **CF,** der "Wäh!" 01.02.2011

[130] **CF**, Anonymisierer, 09.07.2008

[131] **CF**, 7 Tage-Regelung, 11.06.2011

[132] **CF**, Geschäftsmodell Abmahnung, 22.12.2009

[133] Ebenda: **CF**, 7 Tage-Regelung, 11.06.2011.

[134] Ungesicherte Zahlen für 2009: **CF**, Zugangserschwerung, 28.03.2010.

[135] **BVerfG**, Urteil vom 02.03.2010 - 1 BvR 256, 263, 586/08, Rn 208

3.1.6 Herausgabeersuchen

Das Herausgabeersuchen (§ 95 Abs. 1 StPO) bezieht sich – im Gegensatz zum Auskunftsersuchen [136] – auf Gegenstände, also auf Sachbeweismittel im Sinne von § 94 Abs. 1 StPO. Für die Herausgabeersuchen der Staatsanwaltschaft ist inzwischen anerkannt, dass auf die Verweigerung das Gericht die Zwangsmittel nach § 95 Abs. 2 StPO anordnen kann [137]. Im Zusammenhang mit Bankauskünften hat sich deshalb die Praxis eingebürgert, staatsanwaltschaftliche Auskunfts- und Herausgabeersuchen zu verbinden und die Ungehorsamsfolgen aus beiden Vorschriften anzudrohen.

§ 95 Abs. 1 StPO macht keinen Unterschied zwischen Staatsanwaltschaft und Polizei und die Ermittlungsgeneralklausel gilt für beide [138]. Das spricht dafür, dass auch auf die erfolglosen Herausgabeersuchen der Polizei, die unter Hinweis auf § 95 Abs. 2 StPO erfolgten, das Gericht ohne nochmalige Androhung die Ungehorsamsfolgen anordnen kann. Das würde die Rolle der Polizei angemessen stärken und das Ermittlungsverfahren von hindernden Förmeleien entlasten.

Wegen der Sachbeweismittel stellt sich auch die Frage nach den ***Surrogaten***. Häufig handelt es sich bei den geforderten Sachen um Schriftstücke, die entweder dem Urkunds- (§ 249 Abs. 1 S. 1 StPO) oder dem Augenscheinsbeweis unterliegen (§ 86 StPO). In bestimmten Fällen kann es notwendig sein, dass das Original zur Verfügung steht, wenn etwa weitere Untersuchungen in Betracht kommen (physikalisch-technische oder Schriftgutachten) oder es besonders auf die optische Beschaffenheit ankommt. Stehen diese Gründe zurück, dann ist es nach Maßgabe des Verhältnismäßigkeitsprinzips auch gerechtfertigt anstelle des Originals eine Kopie (Surrogat) heraus zu verlangen oder sicherzustellen.

Dieselben Fragen stellen sich, wenn es um Daten geht, die sich auf einem Speichermedium befinden. Der Gegenstand der Sicherstellung ist das körperliche Speichermedium [139], in den meisten Fällen reichen aber die Kopien ausgesuchter Dateien oder eine fachgerechte Komplettsicherung aus, die der weiteren Auswertung zugrunde gelegt werden. Die Entscheidung zwischen Original und Surrogat hängt vom Inhalt der Dateien und der Rolle des Betroffenen ab. Den Nachweis der Vollständigkeit kann nur das Original liefern und bei für sich strafbaren Inhalten (zum Beispiel im Falle des § 184b StGB) verbietet sich eine Aushändigung an den Beschuldigten immer.

Surrogate kommen auch wegen Personenbeweise oder bei mehrgliedrigen Beweiserhebungen in die engere Wahl. Ein übliches Beispiel dafür ist die von Banken geforderte „Kontoverdichtung“. Das Ergebnis ist eine schriftliche Zusammenstellung über die Soll- und Habenbuchungen sowie der Salden innerhalb eines Zeitrahmens für ein bestimmtes (in aller Regel) Kontokorrentkonto. Dabei ist jedoch zunächst unklar, ob die Zusammenstellung bereits in Form eines schriftlichen Kontoabschlusses vorliegt (Sachbeweis), die Buchungsvorgänge nur einzeln vorliegen und von einem Sachbearbeiter bekundet werden können (Personenbeweis) oder von ihm zunächst zusammen gesucht, gestellt und bearbeitet werden müssen (sachverständiger Zeuge). In diesen Fällen kann es sich anbieten, im Rahmen eines staatsanwaltschaftlichen Auskunfts- und Herausgabeersuchen neben Kontoinformationen und Schriftstücken auch zur Vermeidung einer sonst nötigen Durchsuchung die Erstellung einer Kontoverdichtung zu verlangen. Sie kann nicht erzwungen werden, weil jedenfalls der Zeuge keiner Editionspflicht unterliegt.

---

[136] 3.1.5 Staatsanwaltschaftliches Auskunftsersuchen

[137] 3.1.1 Auskünfte von Behörden und anderen Einrichtungen

[138] Ebenda

[139] 3.1.3 Verkehrsdaten und Dateien in Mobilgeräten

3.1.7 Beschlagnahme

Die Beschlagnahme ist eine Form der Sicherstellung von Gegenständen, wobei die amtliche Inverwahrnahme durch Zwang erfolgt (§§ 94 Abs. 2, 98 StPO). Sie beruht auf einem gerichtlichen Beschluss oder – bei Gefahr in Verzug – auf einer Anordnung der Staatsanwaltschaft oder ihrer Ermittlungspersonen [140]. Beschränkungen wegen des Verdachtsgrades, der Schwere der Straftat oder eine besondere Verhältnismäßigkeitsprüfung sieht das Gesetz nicht vor [141].

3.1.8 Beschlagnahme von E-Mails

Die beim Hostprovider gespeicherten E-Mails unterliegen dem Schutz des Fernmeldegeheimnisses nach Art 10 GG [142]. Ihre Beschlagnahme ist dennoch bereits nach § 94 Abs. 2 StPO zulässig [143]. BVerfG: *Der Senat hat bereits entschieden, dass die §§ 94 ff. StPO diesen Anforderungen hinsichtlich der Sicherstellung und Beschlagnahme von Datenträgern und den hierauf gespeicherten Daten genügen …* [144]. *Gleiches gilt für die Sicherstellung und Beschlagnahme von E-Mails, die auf dem Mailserver des Providers gespeichert sind* [145].

Der Entscheidung liegt die Beschlagnahme von 2.500 beim Hostprovider gespeicherten E-Mails aus einem Zeitraum von gut zwei Jahren zugrunde. In einem ähnlichen Fall hat der BGH in einer kurz zuvor veröffentlichten Entscheidung schärfere Anforderungen als das BVerfG gestellt [146]: *Vielmehr ist die Beschlagnahme von E-Mails bei einem E-Mail-Provider, welche dort bis zu einem ersten oder weiteren Aufruf abgespeichert sind, auch unter Berücksichtigung des heutigen Kommunikationsverhaltens in jeder Hinsicht vergleichbar mit der Beschlagnahme anderer Mitteilungen, welche sich zumindest vorübergehend bei einem Post- oder Telekommunikationsdiensteleister befinden, bspw. von Telegrammen, welche gleichfalls auf dem Telekommunikationsweg dorthin übermittelt wurden. Daher können beim Provider gespeicherte, eingegangene oder zwischengespeicherte, E-Mails - auch ohne spezifische gesetzliche Regelung - jedenfalls unter den Voraussetzungen des § 99 StPO beschlagnahmt werden.*

Unabhängig davon, ob die E-Mail-Beschlagnahme schon nach § 94 Abs. 2 StPO oder nur unter den strengeren Voraussetzungen der Postbeschlagnahme (§ 99 StPO) gerechtfertigt ist, unterliegt sie keinen Einschränkungen wegen der Schwere der Straftaten, wohl aber wegen des Verdachtsstadiums. Die Postbeschlagnahme fordert einen Beschuldigten und kann deshalb nicht während der Vorermittlungen angeordnet werden.

Dem BVerfG war die Entscheidung des BGH bekannt und es geht über sie mit mehrdeutigen Worten hinweg: *… dadurch* <wird> *die Anwendbarkeit der §§ 94 ff. StPO nicht in Frage gestellt* [147]. Die praktischen Konsequenzen sind noch nicht geklärt, zumal der BGH später auch entschieden hat [148]: *Die Anordnung der Beschlagnahme des gesamten auf dem Mailserver des Providers gespeicherten E-Mail-Bestandes eines Beschuldigten verstößt regelmäßig gegen das Übermaßverbot.*

Auf die E-Mail-Beschlagnahme sind jedenfalls die besonders strengen Anforderungen des § 100a

---

[140] § 98 Abs. 2 StPO stellt ein gestaffeltes Rechtsschutzverfahren zur Verfügung. Erfolgte die Beschlagnahme in Abwesenheit des Betroffenen, muss die richterliche Bestätigung eingeholt werden, ansonsten nur auf Antrag des Betroffenen.

[141] Weitere Einzelheiten:
3. Ermittlungsmethoden. Wahl der Mittel.

[142] **BVerfG**, Beschluss vom 16.06.2009 - 2 BvR 902/06, Rn 52

[143] Ebenda, Rn 55 ff.

[144] Verweise auf:
BVerfG, Beschluss vom 12.04.2005 - 2 BvR 1027/02;
BVerfG, Urteil vom 02.03.2006 - 2 BvR 2099/04.

[145] **BVerfG**, Beschluss vom 16.06.2009 - 2 BvR 902/06, Rn 61

[146] **BGH**, Beschluss vom 31.03.2009 - 1 StR 76/09, S. 3

[147] **BVerfG**, Beschluss vom 16.06.2009 - 2 BvR 902/06, Rn 58

[148] **BGH**, Beschluss vom 24.11.2009 – StB 48/09 (a), Leitsatz 1

StPO für die Überwachung der Telekommunikation nicht anwendbar, was das BVerfG durch Schweigen und der BGH ausdrücklich ausführt [149].

Beiden Gerichten geht es auch um die Vermeidung unnötig überschießender Eingriffe [150] und der weiten Freigabe der Beschlagnahme von E-Mails, die das BVerfG vorgelegt hat, kann sich der BGH auf Dauer nicht verschließen, zumal auch er nicht die Verfahrensvorschriften für die Postbeschlagnahme (§ 100 Abs. 3 bis 6 StPO), sondern für die Herausgabe von Beweisstücken (§ 95 StPO) und die Durchsicht im Rahmen einer Durchsuchung hervorhebt (§ 110 Abs. 1 StPO). Nach einer zusammenfassenden Betrachtung aller drei Entscheidungen lässt sich für die E-Mail-Beschlagnahme folgern [151]:

- Grundsätzlich ist die Beschlagnahme von E-Mails auf den Speichermedien des Hostproviders nach Maßgabe von § 94 Abs. 2 StPO gerechtfertigt. Daraus folgt, dass es wegen der Schwere der Straftat keine Einschränkungen gibt.
- Wegen der Anwendungsvoraussetzungen greifen hingegen die Grundzüge der Postbeschlagnahme nach § 99 StPO. Daraus folgt, dass ein Beschuldigter bekannt oder wegen seiner Identitätsmerkmale eingegrenzt ist. Ferner folgt daraus, dass die Anordnung dem Richterprivileg unterliegt und eine Anordnung bei Gefahr im Verzug (§ 100 Abs. 1 StPO) nur von der Staatsanwaltschaft getroffen werden kann, die ihrerseits binnen 3 Werktage vom Gericht bestätigt werden muss (§ 100 Abs. 2 StPO).
- Auf die Durchführung der Maßnahme sind nicht die Formvorschriften des § 100 Abs. 2 bis 6 StPO anzuwenden, sondern ein gestaffeltes Verfahren, das sich an den §§ 95 Abs. 1 und 110 Abs. 1 StPO orientiert.
- Danach ist zunächst ein gerichtlicher Beschluss gegen den Hostprovider gemäß § 95 StPO erforderlich, der ihn verpflichtet, alle gespeicherten E-Mails (samt ihrer Anlagen, Vorlagen und Entwürfe) herauszugeben.
- Im Anschluss an die Formvorschriften für die Durchsuchung (§ 110 Abs. 1 StPO) folgt eine Durchsicht der Dateien, mit der die dazu berufene Staatsanwaltschaft ihre Ermittlungspersonen von der Polizei beauftragen kann. § 100 Abs. 2 StPO kommt nicht zur Geltung.
- Die nach der Durchsicht als beweisbedeutend erkannten Dateien werden durch einen gesonderten Beschluss beschlagnahmt (§ 98 Abs. 1 S. 1 StPO).

Es hat lange gedauert, aber die Rechtsprechung zur Beschlagnahme von E-Mails belegt, dass die obersten Gerichte die Internetdienste zunehmend in den Blick nehmen und sich vorsichtig an Lösungen herantasten. Der Mut des BVerfG ist beachtlich, weil es neue Entwicklungen aufnimmt und einerseits neue Grundrechte schafft (informationelle Selbstbestimmung und Integrität informationstechnischer Systeme) und andererseits auch die Weichenstellungen des klassischen Gesetzgebers akzeptiert und konsequent fortsetzt. Dem BGH überlässt das BVerfG regelmäßig die Einzelfallregelungen, die es dann bei Gelegenheit einer eigenen Gesamtbetrachtung unterwirft. Die angesprochenen Entscheidungen zeigen, dass sich beide obersten Gerichte um realistische Lösungen bemühen. Beendet wurde jedenfalls die Diskussion um die Anwendung des § 100a StPO (TKÜ) auf die E-Mail-Beschlagnahme [152].

---

[149] **BGH**, Beschluss vom 31.03.2009 - 1 StR 76/09, S. 3

[150] Siehe oben und **BVerfG**, Beschluss vom 16.06.2009 - 2 BvR 902/06, Rn. 88.

[151] Siehe auch: **CF**, Mythen wegen der E-Mail-Beschlagnahme, 14.02.2011

[152] So noch **LG Hamburg**, Beschluss vom 08.01.2008 - 619 Qs 1/08

3.1.9 Beschlagnahme von Dateien beim Hostprovider

Die Beschlagnahme von Dateien beim Hostprovider (Cloud-Dienste, gemieteter Webspace) erfolgt laut BVerfG auf der Grundlage des § 94 Abs. 2 StPO durch gerichtlichen Beschluss [153] oder bei Gefahr im Verzug aufgrund von Entscheidungen der Staatsanwaltschaft oder der Polizei (§ 98 Abs. 1 S. 1 StPO). Schwellen wegen der Schwere der Straftat oder besondere Anforderungen an die Verhältnismäßigkeit sind nicht vorgesehen [154]. Bei der *Beschlagnahme von Datenträgern und darauf vorhandenen Daten muss der Zugriff auf für das Verfahren bedeutungslose Informationen im Rahmen des Vertretbaren vermieden werden* [155].

Regelmäßig handelt es sich beim Betreiber des Servers um einen Dritten im Sinne von § 103 StPO, der zugleich auch ein besonderes wirtschaftliches Interesse an dem Betrieb seiner EDV hat. Deshalb dürfte fast immer eine großzügige Sicherstellung von Surrogaten [156] (Kopien von Speichermedien) in Betracht kommen.

Die Überwachung des laufenden Datenverkehrs auf einem Server ist damit nicht umfasst. Sie ist eine Form der Überwachung der Telekommunikation nach § 100a StPO [157].

3.1.10 Ferndurchsuchung. Fernzugriff

Als unselbständige Maßnahme sieht § 110 Abs. 3 StPO die Durchsicht räumlich getrennter Speichermedien vor, *soweit auf sie von dem Speichermedium aus zugegriffen werden kann* [158]. Es handelt sich um eine Vorschrift über die Durchführung von Durchsuchungen und ist deshalb vom Durchsuchungsbeschluss mit umfasst (Annex, [159]).

Voraussetzung ist zunächst eine offene Durchsuchung, die sich – das setzt die Vorschrift unausgesprochen voraus – auch auf die vorgefundenen Computer erstreckt, wenn sie beweisrelevante Daten erwarten lassen. § 110 Abs. 3 StPO sprengt sozusagen die klassische Definition der Durchsuchung, die immer nur einen räumlich eingeschränkten, im Allgemeinen an der postalischen Adresse orientierten Eingriff ermöglicht. Zeigt die Durchsicht des Computers am Durchsuchungsort, dass Daten auf auswärtige, also vernetzte Speichermedien ausgelagert sind, ist der Zugriff auf sie zugelassen, *wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist*. Die Vorschrift folgt dem weiten Beweismittelbegriff des § 94 Abs. 1 StPO (… *Untersuchung von Bedeutung sein können*) und verweist auf die Rechtswegvorschriften, die für die Beschlagnahme bei Gefahr im Verzug gelten (§ 98 Abs. 2 StPO).

Als Durchführungsvorschrift verlangt § 110 Abs. 3 StPO keine selbständigen Zulässigkeitsvoraussetzungen und schafft damit auch keine selbstständige Eingriffsmaßnahme, die unabhängig von einer offenen Durchsuchung durchgeführt werden könnte. Sie ist kein Ersatz für die vom BVerfG verbotene, heimliche Onlinedurchsuchung.

Eine andere Frage ist die, wie nach dem Abschluss einer Durchsuchung mit ***sichergestellten Zugangsdaten*** umgegangen werden darf. Hierzu gibt das BVerfG keine klare Antwort, wohl aber zur Verwendung von Zugangsdaten, die von Berech-

---

153 **BVerfG**, Beschluss vom 12.04.2005 - 2 BvR 1027/02;
BVerfG, Urteil vom 02.03.2006 - 2 BvR 2099/04.

154 3.1.7 Beschlagnahme

155 **BVerfG**, Beschluss vom 12.04.2005 - 2 BvR 1027/02, Leitsatz 2

156 3.1.6 Herausgabeersuchen. Surrogate

157 3.2.2 Überwachung der Telekommunikation

158 Ich habe insoweit den Begriff geprägt: Onlinedurchsuchung light; **CF**, Sichtung räumlich getrennter Speichermedien, 2007.

159 3. Ermittlungsmethoden. Wahl der Mittel

tigten zur Verfügung gestellt werden [160]: *Dagegen ist ein Eingriff in Art 10 Abs. 1 GG zu verneinen, wenn etwa ein Teilnehmer eines geschlossenen Chats der für die Verfassungsschutzbehörde handelnden Person seinen Zugang freiwillig zur Verfügung gestellt hat und die Behörde in der Folge diesen Zugang nutzt.*

Daraus ist zu schließen, dass die Grundsätze, die für die ***Hörfalle*** entwickelt wurden, nicht gelten. Insoweit hat das BVerfG 2002 bestimmt [161]: *Die Gewährleistung des Rechts am gesprochenen Wort als Teil des allgemeinen Persönlichkeitsrechts in Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG schützt vor der Nutzung einer Mithöreinrichtung, die ein Gesprächsteilnehmer einem nicht an dem Gespräch beteiligten Dritten bereitstellt. Art 10 Abs. 1 GG umfasst diesen Schutz nicht.*

Dieser Argumentation fehlt noch die Definition für das Grundrecht auf die Integrität informationsverarbeitender Syteme [162], nimmt sie aber vorweg. Die Schutzrichtung zielt auf die technische Integrität, mithin darauf, dass die Technik so neutral funktioniert, wie es der Techniknutzer erwartet. Darum geht es aber bei der Nutzung von Zugangsdaten durch die Strafverfolgungsbehörden nicht.

Zum Ermittlungshelfer hat der BGH ausgeführt [163]: *Hat eine Privatperson auf Veranlassung der Ermittlungsbehörden mit dem Tatverdächtigen ohne Aufdeckung der Ermittlungsabsicht ein auf die Erlangung von Angaben zum Untersuchungsgegenstand gerichtetes Gespräch geführt, so darf der Inhalt des Gesprächs im Zeugenbeweis jedenfalls dann verwertet werden, wenn es um die Aufklärung einer Straftat von erheblicher Bedeutung geht und die Erforschung des Sachverhalts unter Einsatz anderer Ermittlungsmethoden erheblich weniger erfolgversprechend oder wesentlich erschwert gewesen wäre.*

Über legendierte Kontakte hat das BVerfG schließlich ausgeführt [164]: *Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt nicht schon dann vor, wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt, wohl aber, wenn sie dabei ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde ...*

In diesem Spannungsfeld bewegt sich die Frage nach der Nutzung ***sichergestellter Zugangsdaten***. Mit ihnen werden keine Kommunikationsgeräte verändert oder missbraucht, so dass weder das Fernsprechgeheimnis noch die Integrität informationsverarbeitender Systeme betroffen sind. Der Kommunikationspartner wird hingegen über die Identität des Verwenders der Zugangsdaten getäuscht. Insoweit kann die informationelle Selbstbestimmung betroffen sein.

Die Lösungen liegen in den Besonderheiten der Einzelfälle. Ist der Partner der Zugangsdaten nur ein Automat, dann kann er kein Grundrechtsträger im Sinne der informationellen Selbstbestimmung sein, so dass die Verwendung der Zugangsdaten wegen jeder Form von Kriminalität aufgrund der Ermittlungsgeneralklausel [165] zulässig ist. Das betrifft vor allem Hostspeicher und Mediendienste, die keine menschliche Kommunikation zum Gegenstand haben.

Handelt es sich hingegen um Zugangsdaten zu geschlossenen Benutzerkreisen (Chat, Foren, Boards), dann kann eine Ausnutzung des Vertrauens *des Betroffenen in die Identität und die Motivation seines Kommunikationspartners* (siehe oben) vorliegen, so dass die Maßnahme mindestens Ermittlungen wegen erheblicher Formen der

---

[160] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 292

[161] **BVerfG**, Beschluss vom 09.10.2002 – 1 BvR 1611/96, 1 BvR 805/98, 3. Leitsatz

[162] 2.3 Integrität informationstechnischer Systeme

[163] **BGH**, Beschluss vom 13.05.1996 - GSSt 1/96, Leitsatz 1

[164] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 310

[165] 3.1.1 Auskünfte von Behörden und anderen Einrichtungen

Kriminalität voraussetzt. Im Zusammenhang mit den personalen Ermittlungen [166] werden die legendierten Ermittlungen einer genaueren Betrachtung unterzogen. Deshalb muss an dieser Stelle ein Zwischenergebnis reichen: In dem Rahmen, in dem legendierte Ermittlungen aufgrund eines gerichtlichen Beschlusses zulässig sind [167], dürfen auch sichergestellte Zugangsdaten verwendet werden. Alle einschlägigen Ermittlungsmaßnahmen setzen die Aufklärung erheblicher Straftaten voraus, so dass auch die Schwellen, die der BGH für den Privatermittler aufgestellt hat, gewahrt bleiben. Die besondere Verhältnismäßigkeit, die der BGH wegen anderer Ermittlungsmaßnahmen fordert, muss im Einzelfall geprüft werden.

3.2 technische Mittel

Einige der im ersten Abschnitt angesprochenen Eingriffsmaßnahmen zeigen bereits eine gewisse Nähe zu den technisch ausgerichteten Ermittlungsmethoden. Den Kern der rechtlichen Regeln zu den technischen Überwachungsmaßnahmen bilden aber die Überwachung der Telekommunikation – TKÜ (§ 100a StPO) – und die von der StPO nicht zugelassene Onlinedurchsuchung. Insoweit bedarf es einer genauen Abgrenzung bei Maßnahmen mit Quellenzugriff, der im Zusammenhang mit der Internettelefonie und der damit verbundenen Frage steht, ob die Überwachung der Kommunikation in einem Computer bereits eine Onlinedurchsuchung ist oder noch eine Maßnahme der TKÜ.

Der Begriff Onlinedurchsuchung macht bereits sprachlich deutlich, um was es bei ihr geht: Die heimliche Durchsicht der auf dem Computer der Zielperson abgespeicherten Daten, also eine computerbezogene Durchsuchung als verdeckte Maßnahme.

Davon unterscheidet sich die Quellen-TKÜ. Sie verlangt danach, dass der Computer der Zielperson mit einer Remote Forensic Software, also einer spezialisierten Malware, infiltriert wird, die die Kommunikationsdaten beim Verarbeitungsvorgang im Bereich des Prozessors, des Arbeitsspeichers oder der Peripheriekomponenten (Soundkarte, Mikrofon, Lautsprecher, Grafikkarte) abgreift. Das ist bei der Onlinedurchsuchung nicht anders, so dass sich die Maßnahmen nicht durch das technische Vorgehen, sondern nur durch die Art der abgegriffenen Daten unterscheiden. Die eingesetzte Malware kann ganz einfach auf den einen oder anderen Zweck angepasst werden. Das ist einer der Gründe, warum das BVerfG in seiner Entscheidung zur Onlinedurchsuchung die Quellen-TKÜ sehr kritisch betrachtet [168].

Ein Verbot der Quellen-TKÜ ist auch aus den kritischen Worten des BVerfG nicht abzuleiten. An der Ausgestaltung der geltenden Vorschriften zur TKÜ hat es maßgeblich mit seiner Spruchpraxis mitgewirkt und den Schutzbereich des Art 10 GG auf

[166] 3.3 personale Ermittlungen

[167] Das betrifft die längerfristige Observation (§ 163f StPO) und den Einsatz eines Verdeckten Ermittlers (§ 110a StPO).

[168] 3.2.5 Quellen-TKÜ

die gesamte Strecke der Fernkommunikation und ihrer Begleitumstände ausgedehnt. Darauf lassen sich die §§ 100a, 100g StPO ein und die Eingriffsnorm zur TKÜ macht keinen Unterschied danach, an welcher Stelle der Kommunikationsübertragung der Abgriff erfolgt [169]. Im Zusammenhang mit der Onlinedurchsuchung hatte das Gericht nur über diese Maßnahme im Verfassungsschutzgesetz von Nordrhein-Westfalen und nicht auch über die Quellen-TKÜ als solche zu entscheiden. Die kritischen Argumente fördern die Diskussion, haben aber keine unmittelbare Auswirkung auf die Geltung des Rechts.

Zwischen der Online-Durchsicht und der Quellen-TKÜ ist die Protokollierung der Aktivitäten am Computer angesiedelt, die keine Kommunikation sind (zum Beispiel die Schaffung und Übermittlung von Screenshots). Dazu gehören die Arbeit mit Büroanwendungen, Offline-Spiele, Buchhaltungsaufgaben, die Betrachtung und Bearbeitung von Grafiken und vieles mehr. Diese Aktivitäten sind als zweiter Anwendungsfall der Onlinedurchsuchung anzusehen und deshalb ihre Erhebung im Strafverfahren nicht zugelassen.

Die Einzelheiten der Abgrenzungen und des Meinungsstandes sind vorbildlich vom LG Landshut heraus gearbeitet worden [170]. Es betrachtet die Quellen-TKÜ im Anschluss an die herrschende Meinung als zulässig, nicht aber die im angegriffenen Fall regelmäßig abgegriffenen und übermittelten Screenshots.

Im Ergebnis sind deshalb drei sachlich verschiedene Quellenzugriffe am Computer der Zielperson zu unterscheiden, von denen eine, die Quellen-TKÜ, nach geltendem Recht zugelassen ist:

- Heimliche Online-Durchsicht der gespeicherten Daten auf dem Computer der Zielperson; Onlinedurchsuchung im engeren Sinne.
- Heimliche Protokollierung der Aktivitäten am Computer der Zielperson, die nicht Kommunikation sind; Onlinedurchsuchung im weiteren Sinne.
- Quellen-TKÜ als Anwendungsfall der Überwachung der Telekommunikation.

Besondere Anwendungsprobleme sind zu erwarten, wenn die Onlinedurchsuchung nach zulässigen Vorschriften im BKA-Gesetz oder landesrechtlichen Verfassungsschutzgesetzen durchgeführt wird und dabei Kenntnisse über Straftaten erlangt werden. Infolge des Gebots der Schwellengleichheit dürfen diese Erkenntnisse nicht vollbeweislich im Strafprozess verwendet werden, weil eine entsprechende Ermächtigung in der StPO fehlt. Sie können nur als Spur im Rahmen des Spurenansatzes verwertet werden [171].

3.2.1 technische Observationshilfen

Als *besondere für Observationszwecke bestimmte technische Mittel* (§ 100h Abs. 1 Nr. 2 StPO) werden von der Rechtsprechung vor allem auch Peilsender und die Nutzung des Global Positioning Systems – GPS – anerkannt [172]. Die Vorschrift findet nur auf Maßnahmen außerhalb von Wohnungen Anwendung und setzt Straftaten von erheblicher Bedeutung voraus. Sie verlangt keine besonderen Anordnungskompetenzen und kommt sowohl wegen der kurzfristigen Observation in Betracht (*planmäßig angelegte Beobachtung des Beschuldigten*), die von der Polizei oder der Staatsanwaltschaft angeordnet werden kann, oder wegen der vom Gericht beschlossenen längerfristigen Observation (§ 163f StPO; Gefahr im Verzug: Abs. 3) [173].

Der Anwendungsbereich der Vorschrift ist noch längst nicht ausgelotet. Sie rechtfertigt jedenfalls nicht die Übermittlung von Remote Forensic Soft-

---

[169] 3.2.2 Überwachung der Telekommunikation

[170] **LG Landshut**, Beschluss vom 20.01.2011 - 4 Qs 346/10

[171] Siehe unten: Gebot der Schwellengleichheit.

[172] Zur gleichlautenden alten Fassung unter § 100c StPO: **BVerfG**, Urteil vom 12.04.2005 - 2 BvR 581/01.

[173] **BGH**, Urteil vom 24.01.2001 - 3 StR 324/00, Leitsatz 3

Überwachung der Telekommunikation

- Festnetze
- Mobilnetze einschließlich SMS
- Auslandskopfüberwachung
- DSL-Stream
- UMTS-Stream (mobile Internetnutzung)
- Serverüberwachung
- Quellen-TKÜ (Internettelefonie)

ware [174], mit anderen Worten: von Malware, die eine Onlinedurchsuchung vorbereitet [175].

Leitend ist insoweit das, was das BVerfG im Zusammenhang mit Peilsendern und GPS-Diensten ausgeführt hat [176]: *Eingriffe in das allgemeine Persönlichkeitsrecht ... durch die Verwendung von Instrumenten technischer Observation erreichen in Ausmaß und Intensität typischerweise nicht den unantastbaren Kernbereich privater Lebensgestaltung ...; so ist es auch hier. ... Es ist deshalb nicht zu beanstanden, wenn der Gesetzgeber die Zulassung der Maßnahme bloß von einem Anfangsverdacht abhängig gemacht hat. Es war ihm auch nicht verwehrt, den Einsatz dieser Mittel an die im unmittelbaren systematischen Zusammenhang des § 100 c StPO niedrigste Subsidiaritätsstufe ("wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise weniger erfolgversprechend oder erschwert wäre") zu binden ...*

Teile der Kommentarliteratur halten deshalb den Einsatz von *E-Mail-Bestätigungsdiensten* [177] unter den Voraussetzungen von § 100h StPO für zulässig. Dem trete ich bei. Technisch geht es dabei darum, dass dem noch nicht identifizierten Täter eine E-Mail geschickt wird, die eine Eingangsbestätigung provoziert. Das kann eine manuelle Bestätigung sein, ein HTML-String, der vom Empfänger unterdrückt werden kann, oder eine (fiese) Routine, die die Antwort ohne Kontrolle des Empfängers absendet. Ihr Inhalt besteht im Wesentlichen in der IP-Adresse des Empfängers. Das gibt den Ermittlern die Chance, den Zugang des Täters zum Internet anhand seiner IP-Adresse zu lokalisieren [178].

Die Maßnahme berührt das Fernsprechgeheimnis [179], aber nicht weiter über das Maß hinaus, das das BVerfG bislang für die Bestandsdatenabfrage zugelassen hat. Verfassungsrechtliche Bedenken gegen die Handhabung greifen deshalb nicht durch, wenn nicht aus der neuen Entscheidung des 1. Senats Beschränkungen abgeleitet werden müssn.

Vor allem das BVerfG hebt hervor, dass der Täter vor dem Überraschungseffekt einer technischen Ermittlungsmaßnahme geschützt werden muss, indem klare Regeln über die Voraussetzungen, über den Kernbereichsschutz, über die Grenzen der Maßnahme und den Rechtsschutz vorhanden sein müssen. Seine Rechtsprechung verlangt aber nicht, dass die Strafverfolger weniger findig sein müssen als der Täter selber. Deshalb gibt es keinen Vertrauensschutz wegen der Dienste, die im Internet jedermann frei zugänglich angeboten werden. Das gilt für die technischen Dienste (Ping, Tracerouting, DNS-Datenbanken [WhoIs], Server-Sniffer). Auch die Intelligenz und die Fertigkeiten der Ermittler unterliegen keinen Einschränkungen, wenn sie übliche Techniken nutzen und vor allem die namentlich unzulässigen Einwirkungen unterlassen (zum Beispiel § 136a StPO).

---

[174] **CF**, Online-Zugriff an der Quelle, 08.011.2008

[175] **BGH**, Beschluss vom 31.01.2007 - StB 18/06, Rn 20

[176] **BVerfG**, Urteil vom 12.04.2005 - 2 BvR 581/01, Rn 56

[177] Meyer-Goßner, § 100h StPO, Rn 2; unter Bezugnahme auf KMR-Bär.

[178] 3.1.2 Bestandsdaten

[179] 2.1 Telekommunikationsgeheimnis

3.2.2 Überwachung der Telekommunikation

§ 100a StPO ist die zentrale Vorschrift im Zusammenhang mit den technischen Überwachungsmaßnahmen - TKÜ. Sie lässt in Fällen der schweren Kriminalität aufgrund eines gerichtlichen Beschlusses die inhaltliche Überwachung der Telekommunikation zu [180], wobei besondere Anforderungen an die Verhältnismäßigkeit (§ 100a Abs. 1 Nr. 3 StPO) und an die Form der Entscheidung gestellt werden (Schriftform, Begründung; § 100b Abs. 2 StPO). Der Straftatenkatalog in § 100a Abs. 2 StPO bestimmt die einschlägigen Straftaten abschließend. Die Staatsanwaltschaft ist zur Anordnung bei Gefahr in Verzug berechtigt (§100b Abs. 1 StPO). Ihre Entscheidung bedarf der gerichtlichen Bestätigung binnen drei Werktage.

Aufgrund der Ermächtigung in § 110 Abs. 2 TKG sind die Einzelheiten über die Art und Weise der Überwachungsmaßnahmen in der TKÜV ausgestaltet worden. Die heutige Fassung der TKÜ-Vorschriften sind das Resultat vielfacher Überprüfungen durch das BVerfG und den BGH, so dass sie als verfassungsrechtlich abgesichert gelten können.

Die Telekommunikation wird von § 3 Nr. 22 TKG als *der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen* definiert. Das BVerfG legt seiner Definition einen breiteren Ansatz zugrunde [181] und betrachtet die gesamte Strecke von Endgerät zu Endgerät über alle beteiligten Netzknoten (Zugangsprovider, Verbindungsnetze und Anschlussnetze) als Bestandteile des Telekommunikationsvorganges [182], jede Art von Endgerät [183], Sprache, Daten und Steuersignale sowie die äußeren Umstände der Telekommunikation (Verkehrsdaten [184]). Deshalb sind die Vorschriften der §§ 100a, 100b StPO nicht nur auf Telefongespräche, sondern auch auf die gleichzeitige Bildübertragung und auf jede Form des Datenverkehrs anwendbar [185]. Dabei ist es gleichgültig, an welcher Stelle der Überwachungsvorgang stattfindet, ob beim Zugangsprovider, an einem der Kommunikation dienenden Server oder wegen der Internet-Telefonie vor der Verschlüsselung am Endgerät.

Eine besondere Form der TKÜ ist die ***Auslandskopfüberwachung*** [186], deren Einzelheiten in der TKÜV angesprochen werden. Sie ist sehr aufwändig, verlangt nach einer ausdrücklichen Anordnung durch Gerichtsbeschluss und muss von allen gängigen Anschluss- und Verbindungsnetzbetreibern gleichzeitig durchgeführt werden. Drei Anwendungsfälle werden von ihr umfasst:

- Ein Mobiltelefon von einem ausländischen Zugangsprovider befindet sich im Inland und nimmt am Roaming teil [187].
- Ein überwachter Anschluss im Ausland nimmt Kontakt zu einem Anschluss im Inland auf (§ 4 Abs. 1 TKÜV). Insoweit besteht Streit. Die TKÜV spricht davon, dass der ausländische Anruf an ein inländisches Endgerät um- oder weitergeleitet wird, und in einer Äußerung der Bundesregierung wird dieser Anwendungsfall von der Auslandskopfüberwachung ausgeschlossen [188] und der Rechtshilfe unterworfen. Die Wortlaute der einschlägigen Vorschriften schließen ihn hingegen nicht aus, weil es eigentlich gleichgültig ist, ob der überwachte Anruf in das Ausland gerichtet ist oder aus ihm kommt.

---

[180] 2.1 Telekommunikationsgeheimnis

[181] 2.1 Telekommunikationsgeheimnis

[182] **BVerfG**, Beschluss vom 13.11.2010 - 2 BvR 1124/10, Rn 13

[183] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 194

[184] 3.1.4 Verkehrsdaten und Funkzellendaten

[185] Das gilt auch für die Anbindungen per DSL. Es handelt sich qualitativ um Kommunikationsdaten, für deren Transport ein besonderes Protokoll verwendet wird. Der verpflichtete Zugangsprovider muss deshalb im Beschluss nach § 100a StPO zur Herauslösung des DSL-Stromes aufgefordert werden.

[186] **CF**, Auslandskopfüberwachung, 15.01.2011

[187] **CF**, Roaming, 23.08.2008

[188] Antwort der Bundesregierung auf eine Kleine Anfrage der Abgeordneten Rainer Funke, Rainer Brüderle … vom 04.04.2005 – BT-Drs. 15/1591, S. 6.

- Ein überwachter Anschluss im Inland nimmt Kontakt zu einem Anschluss im Ausland auf (§ 4 Abs. 2 TKÜV). Das ist eine „normale“ TKÜ, die sich nur gegen einen inländischen Anschlussinhaber richtet.

§ 3 Abs. 2 S. 2 TKÜV verpflichtet die Betreiber von Verbindungsnetzen [189] ins Ausland dazu, technische Vorrichtungen für die TKÜ bereit zu halten. § 4 TKÜV regelt die Anwendungsfälle, wobei die reine Durchleitung einer Verbindung, die ausschließlich Endgeräte im Ausland betrifft, nicht erfasst werden.

Die Bedeutung der TKÜ ist nicht zu unterschätzen, zumal sich das heutige Kommunikationsverhalten weit vom stationären Telefonieren im klassischen Festnetz entfernt hat [190]. Der erste Entwicklungssprung begann mit der breiten Markteinführung der Mobiltelefonie [191] und seither verwenden die meisten Täter mehrere Handys oder wechseln häufiger die SIM-Karten, die die Anschlusskennung des Endgerätes verwalten (IMSI). Die Breitbandanbindungen im Festnetz per DSL und gleichzeitig die Flatrates mit ihren Pauschalpreisen haben die Telekommunikation revolutioniert und zu einem echten Mengenproblem werden lassen, sowohl für die Zugangsprovider und Carrier wie auch für die Überwachungsmaßnahmen. Gegenwärtig erfolgt der dritte Entwicklungssprung mit internetfähigen Handys und UMTS-Sticks für Laptops und anderen mobilen Geräten, die den Leistungsvergleich mit üblichen PCs nicht scheuen müssen. Internetcafes und die Verbindung breitbandiger UMTS-Zugänge mit Prepaid-Verträgen, die auch von Einzelhandelsketten vertrieben werden, geben den Tätern, die sich der besonderen Handlungsfreiräume im Internet bedienen, Anonymität und Bewegungsfreiheit, die in dieser Form – auch im Zusammenhang mit kriminellen Erscheinungsformen im Internet – bislang unbekannt gewesen sind. Ihnen lässt sich nur mit Ermittlungsmethoden begegnen, die technischer Natur sind (Bestands- und Verkehrsdaten, IMSI-Catcher und TKÜ) oder mit List verbunden sind (NoeP, Verdeckter Ermittler, Legenden). Dazu müssen die immer wieder von mir hervorgehobenen Zulässigkeitsvoraussetzungen vorliegen. Das sind wegen der schweren Eingriffsmaßnahmen nur schwere Formen der Kriminalität, wenn es um Verkehrsdaten, den IMSI-Catcher und die TKÜ geht, und erhebliche Formen, wenn es Verdeckte Ermittler betrifft.

Dem Schutz der durch die TKÜ oder andere verdeckte Maßnahmen gewonnenen Daten dient das ***Gebot der Schwellengleichheit***, das jetzt in den §§ 161 Abs. 2 (Import) und 477 Abs. 2 S. 2 StPO (Export) feste gesetzliche Regeln gefunden hat. Es besagt, dass Erkenntnisse, die aufgrund besonderer Eingriffsermächtigungen und unter einschränkenden Zulässigkeitsvoraussetzungen erlangt wurden, als Zufallsfunde [192] (grundsätzlich zur Durchsuchung: § 108 Abs. 1 StPO) nur dann in anderen Verfahren verwendet werden dürfen, wenn ihre Erhebung dort ebenfalls zugelassen ist [193]. Eine wichtige Ausnahme stellt der ***Spurenansatz*** dar, der vom BGH entwickelt [194] und vom BVerfG bestätigt worden ist [195]. Danach dürfen nicht schwellengleiche Spuren und Beweise zwar nicht vollbeweislich in der gerichtlichen Hauptverhandlung, wohl aber zur Begründung anderer Eingriffsmaßnahmen verwendet werden.

---

189 **CF**, TK-Netze, 2007

190 Siehe auch: **Kochheim**, Netzkommunikation, 10.07.2010.

191 **CF**, Mobilfunk, 23.08.2008; siehe auch: **CF**, TK-Netze, 2007.

192 **BGH**, Urteil vom 27.11.2008 - 3 StR 342/08

193 Einzelheiten: **Kochheim**, Verwertung verdeckt erlangter Beweise, 17.05.2009; siehe auch: **Kochheim**, Zum Umgang mit Verkehrsdaten, 08.03.2010.

194 **BGH**, Beschluss vom 18.03.1998 - 5 StR 693/97

195 **BVerfG**, Beschluss vom 29.06.2005 - 2 BvR 866/05

3.2.3 IMSI-Catcher

Der gerichtlich angeordnete Einsatz eines IMSI-Catchers gemäß § 100i StPO wird vom BVerfG als zulässige Ermittlungsmaßnahme anerkannt [196]. Das technisch aufwändige Verfahren ersetzt eine Funkzelle und verhält sich wie ein Turm für die Mobiltelefonie. Dadurch können alle mobilen Endgeräte in dem Segment ausgemessen werden, um bislang unbekannte Mobilgeräte des Täters zu erkennen. Damit lassen sich auch mobile Internetzugänge erkennen, wenn sie sich selbständiger Zugangstechniken (UMTS und andere Mobilfunk-Protokolle) bedienen. Missbräuchliche Zugänge per WLAN [197] lassen sich damit nicht erkennen.

IMSI-Catcher dienen vor Allem der Vorbereitung einer TKÜ [198]. Sie dürfen aber bereits wegen der erheblichen Kriminalität eingesetzt werden, um etwa serienmäßig handelnde Betrüger zu lokalisieren [199]. Die Staatsanwaltschaft ist zur Anordnung bei Gefahr in Verzug befugt (§ 100i Abs. 3 StPO), ihre Entscheidung muss binnen drei Werktage vom Gericht bestätigt werden.

3.2.4 Serverüberwachung

Während der Zugriff auf gespeicherte Dateien beim Hostprovider ein Fall der Beschlagnahme ist [200], geht die laufende Überwachung der Kommunikation auf einem Web- oder Mailserver bei einem Provider erheblich weiter, so dass es eines Gerichtsbeschlusses unter den Voraussetzungen des § 100a StPO bedarf. Es gelten die genannten Anforderungen [201].

3.2.5 Quellen-TKÜ

Die Quellen-TKÜ ist eine besondere Form der Überwachung der Telekommunikation gemäß § 100a StPO [202], die neben den strengen förmlichen Voraussetzungen auch technisch sehr aufwändig ist, weil sie genaue Kenntnisse über die Hardware und die Software im Computer der Zielperson verlangt. Sie setzt eine Infiltration des Zielgerätes mit einer Remote Forensic Software [203] voraus, die die Polizei in die Lage versetzt, die Kommunikationsdaten vor der Verschlüsselung bei der Internettelefonie abzugreifen (Voice over IP – VoIP, zum Beispiel beim Einsatz von Skype).

Die technischen Anwendungsvoraussetzungen sind grundsätzlich dieselben, die auch bei der Onlinedurchsuchung zum Einsatz kommen würden [204].

Das BVerfG sieht die Quellen-TKÜ wegen ihrer Nähe zur Onlinedurchsuchung problematisch [205]:

Wird ein komplexes informationstechnisches System zum Zweck der Telekomunikationsüberwachung technisch infiltriert („Quellen-Telekommu-nikationsüberwachung“), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. Erfasst werden können beispielsweise das Verhalten bei der Bedienung eines Personalcomputers für eigene Zwecke, die

---

196 **BVerfG**, Beschluss vom 22.08.2006 - 2 BvR 1345/03

197 **CF**, Wardriving: Eindringen in lokale Funknetze, 2007

198 3.2.2 Überwachung der Telekommunikation

199 Der wichtige Anwendungsfall des Stalkings (§ 238 StGB) gehört nur dann der erheblichen Kriminalität an, wenn dadurch Leute *in die Gefahr des Todes oder einer schweren Gesundheitsschädigung* geraten (§ 238 Abs. 2 StGB).

200 3.1.9 Beschlagnahme von Dateien beim Hostprovider

201 3.2.2 Überwachung der Telekommunikation

202 3.2.2 Überwachung der Telekommunikation

203 **CF**, Online-Zugriff an der Quelle, 08.11.2008

204 Zur Abgrenzung siehe: 3.2 technische Mittel

205 **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07 (Onlinedurchsuchung), Rn 188, 189.

Abrufhäufigkeit bestimmter Dienste, insbesondere auch der Inhalt angelegter Dateien oder - soweit das infiltrierte informationstechnische System auch Geräte im Haushalt steuert - das Verhalten in der eigenen Wohnung. <Rn 188>

Es kann *im Übrigen dazu kommen, dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist. In der Folge besteht für den Betroffenen - anders als in der Regel bei der herkömmlichen netzbasierten Telekommunikationsüberwachung - stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden.* <Rn 189>

Praktische Konsequenzen ergeben sich daraus nicht, so dass die mehrheitliche Meinung davon ausgeht, dass die Quellen-TKÜ dem § 100a StPO unterfällt [206]. Mit dem BVerfG ist auch darauf hinzuweisen, dass die „Telekommunikation“ die gesamte Übertragungsstrecke zwischen den Endgeräten umfasst [207] und § 100a StPO keine Beschränkungen im Hinblick auf die Überwachungsstelle macht.

3.2.6 Onlinedurchsuchung

Die Onlinedurchsuchung [208] ist vor allem eine heimliche Durchsicht der auf dem Computer der Zielperson abgespeicherten Daten, also eine computerbezogene Durchsuchung als verdeckte Maßnahme [209]. *Die "verdeckte Online-Durchsuchung" ist mangels einer Ermächtigungsgrundlage unzulässig. Sie kann insbesondere nicht auf § 102 StPO gestützt werden. Diese Vorschrift gestattet nicht eine auf heimliche Ausführung angelegte Durchsuchung* [210].

Das BVerfG hat die Maßnahme in der Form, wie sie im Nordrhein-Westfälischen Verfassungsschutzgesetz vorgesehen war, als verfassungswidrig angesehen [211], wobei es weniger auf den Grundrechtsschutz für die Wohnung abstellt [212], sondern auf das neu erkannte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme [213]. Anschließend wurde die Onlinedurchsuchung nur in das BKA-Gesetz und in die Verfassungsschutzgesetze verschiedener Bundesländer aufgenommen [214].

---

206 Statt vieler: **LG Landshut**, Beschluss vom 20.01.2011 - 4 Qs 346/10.

207 **BVerfG**, Beschluss vom 13.11.2010 - 2 BvR 1124/10, Rn 13

208 **CF**, Bundesverfassungsgericht: Onlinedurchsuchung, 05.04.2008

209 Abgrenzung zur Quellen-TKÜ: 3.2 technische Mittel.

210 **BGH**, Beschluss vom 31.01.2007 - StB 18/06.

211 **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07

212 2.4 Wohnung

213 2.3 Integrität informationstechnischer Systeme

214 Siehe oben. Die Zulässigkeit der Onlinedurchsuchung habe ich 2007 aus dem großen Lauschangriff abgeleitet (§ 100c StPO) und dabei den Wohnungsschutz falsch bewertet. Die Ausgestaltung eines neuen Grundrechts habe ich seinerzeit nicht vorhergesehen. Es steht einer analogen Anwendung entgegen.
CF, Onlinedurchsuchung, 2007.

3.2.7 Quellen-Zugriff auf nicht kommunikative Aktivitäten

Die heimliche Überwachung der laufenden, nicht-kommunikativen Aktivitäten in informationstechnischen Systemen aus der Ferne ist ein weiterer Anwendungsfall der Onlinedurchsuchung und als Eingriffsmaßnahme im strafrechtlichen Ermittlungsverfahren nicht zugelassen [215].

3.2.8 Spyware

Der gezielte Einsatz von Spyware (Keylogger, Remote Forensic Software) gegen eine unbestimmte Gruppe von Verdächtigen oder gegen einzelne Beschuldigte muss sich am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme [216] orientieren. Die StPO kennt keine Ermächtigungsgrundlage, die ausdrücklich dieses Grundrecht einschränkt. Entsprechende Maßnahmen sind also nicht erlaubt.

Bei einer nur geringfügigen Beeinträchtigung des Grundrechts könnten klassische Eingriffsbefugnisse durchgreifen, wie es das BVerfG wegen der Beschlagnahme auf Servern [217] und bei der Beschlagnahme von E-Mails ausgeführt hat [218]. Ein solcher flacher Grundrechtseingriff wird wegen der E-Mail-Bestätigungsdienste [219] als technische Observationshilfe im Sinne von § 100h StPO diskutiert.

Über deren Reichweite und die der Rasterfahndung (§§ 98a, 98b StPO) auf Ermittlungen mit Internet-Bezug gibt es noch keine gesicherten Erkenntnisse und Meinungen.

---

[215] Siehe: 3.2 technische Mittel. 3.2.6 Onlinedurchsuchung.

[216] 2.3 Integrität informationstechnischer Systeme

[217] 3.1.9 Beschlagnahme von Dateien beim Hostprovider

[218] 3.1.8 Beschlagnahme von E-Mails

[219] 3.2.1 technische Observationshilfen

3.3 personale Ermittlungen

In seinem Urteil zur Onlinedurchsuchung hat das BVerfG [220] den Schutz vor technischen Eingriffen des Staates in den Vordergrund gestellt und dazu das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme [221] formuliert. Dem stellt es die nicht beachtliche *Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner“* <Rn 290> gegenüber. Für einfache Ermittlungshandlungen der Strafverfolgung im Internet spricht das BVerfG deutliche Worte und sieht durch sie keine Grundrechte verletzt. Das gilt für

- die Kenntnisnahme aller öffentlich zugänglichen Informationen <Rn 308>,
- die Recherche in allgemein zugänglichen Informations- und Kommunikationsdiensten, *die sich zumindest an einen nicht weiter abgegrenzten Personenkreis richten* <Rn 308>,
- die Verwendung einer einfachen Legende (Fake Account) <Rn 310> und
- auch für die legendierte Kommunikation über einen längeren Zeitraum <Rn 311>.

Für diese diese einfachen Ermittlungshandlungen reicht deshalb im Anschluss an die ältere Entscheidung des BVerfG zur Bestandsdatenauskunft [222] die Ermittlungsgeneralklausel [223] als Eingriffsermächtigung aus.

Die Grenze zieht das BVerfG, wenn die staatliche Stelle bei der Kommunikation *ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation des Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde* <Rn 310>.

Das ist der Fall, wenn das Verfahrensrecht besondere persönliche Schutzvorrichtungen vorsieht. Als Beispiele dafür sollen an dieser Stelle die besonderen Belehrungspflichten zugunsten des Beschuldigten (§§ 136, 136a StPO) und das Recht auf ein faires Verfahren genügen. Sie greifen besonders dann, wenn nicht nur ein Anfangsverdacht wegen einer Straftat besteht (§ 152 Abs. 2 StPO), sondern über den Kreis von Verdächtigen hinaus konkrete Anhaltspunkte auf bestimmte Beschuldigte bestehen, ohne dass sie bereits namentlich identifiziert sind.

Nach den vom BGH entwickelten Grenzen der ***kriminalistischen List*** sind die Strafverfolgungsbeamten nicht gehalten, jeden Irrtum des Verdächtigen aufzuklären [224]: *Die bloße Ausnutzung eines bestehenden Irrtums kann einer Täuschung allenfalls dort gleichgestellt werden, wo der Irrtum des Betroffenen im Vertrauen auf eine in Wirklichkeit nicht bestehende Sachlage gründet und dieses Vertrauen schutzwürdig ist.*

Die Betrachtungen des BVerfG zur Nutzung getarnter Adressen und Identitäten (Zugangskonten und Kommunikation) betreffen nur einfache Legenden, also Täuschungen, unter denen die Tatsache verschwiegen wird, der Polizei anzugehören, und über den eigenen Namen zu täuschen. Zwischen ihnen und der Legende eines Verdeckten Ermittlers, die eine auf *Dauer angelegte, veränderte Identität* ist (§ 110a Abs. 2 StPO) und auf *entsprechende Urkunden* gestützt werden darf (§ 110a Abs. 3 StPO), ist ein weites Feld.

Für die vom BVerfG bezeichneten Kommunikationsbeziehungen im Internet, für die die einfache Täuschung reicht und die keine überprüfbaren Legenden über Herkunft, Ausbildung und Vorleben bedürfen, gibt die Ermittlungsgeneralklausel die hinreichende Grundlage. Das gilt zum Beispiel für die, auch längerfristige, Teilnahme in Sozialen Netzwerken, wobei nicht mehr an Täuschung nötig ist als die Nutzung des Szenejargons und passender Wortmeldungen.

Cardingboards und andere geschlossene Benut-

---

[220] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07
[221] 2.3 Integrität informationstechnischer Systeme
[222] **BVerfG**, Beschluss vom 13.11.2010 - 2 BvR 1124/10
[223] 1. Internet und Strafverfahrensrecht
[224] **BGH**, Urteil vom 08.10.1993 - 2 StR 400/93, Rn 28, mwN und Auseinandersetzungen mit anderen BGH-Entscheidungen.
Siehe auch: Karl-Bruno **Kaefer**, Vernehmung des Beschuldigten, Kriminalistik 6/99, 423 (424).

zergruppen in der kriminellen Szene [225] verlangen aber nach Bewerbungen mit detaillierten Angaben zu den Erfahrungen und zum Vorleben, Referenzen durch Taten oder Fürsprecher sowie Keuschheitsproben. Diese Angaben müssen nicht nur stimmig und überprüfbar sein, sondern nötigenfalls auch einer Konfrontation in der Realität standhalten.

Je feiner die Legende ausgefeilt und untermauert werden muss, desto mehr läuft der legendierte Beamte Gefahr, die vom BVerfG gezogene Grenze zum *schutzwürdigen Vertrauen des Betroffenen* zu überschreiten, zumindest in die Absprachen von Straftaten einbezogen zu werden und in einen Konflikt mit dem Legalitätsprinzip zu geraten (§ 152 Abs. 2 StPO). Schutz bietet ihm dann nur eine klare Absicherung seiner Handlungen, ihre Dokumentation und fachliche Begleitung.

Der Gesetzgeber hat dafür besondere Instrumente zur Verfügung gestellt, die jedenfalls bei einer längerfristige Beobachtung des Beschuldigten oder dauerhafte Kontaktaufnahmen zu ihm nach einer gerichtlichen Zustimmung gemäß §§ 163f oder 110b StPO bedürfen.

Maßnahmen unterhalb dieser Schwelle sind wie Scheingeschäfte und zeitlich sowie sachlich umgrenzte Ermittlungsaufträge an einen Nicht offen ermittelnden Polizeibeamten – NoeP – zu behandeln. Als Leitlinie dient der gesetzgeberische Wille, wonach jedenfalls die längerfristige Observation einer gerichtlichen Anordnung bedarf, wenn sie länger als zwei Tage andauern soll.

3.3.1 verdeckte personale Ermittlungen

Legendierte Kontakte zu Verdächtigen und Beschuldigten führen zu ständigen Auseinandersetzungen in der Rechtsprechung. Dabei geht es im Wesentlichen um drei streitige Begriffe:

- Scheinkauf
- Nicht offen ermittelnder Polizeibeamter – NoeP
- Verdeckter Ermittler

In der Anlage D [226] zu den RiStBV [227] werden insgesamt vier Rollen von Personen beschrieben, die zwar zeugenschaftliche Aussagen machen, deren Identität aber zunächst oder auf Dauer nicht offenbart werden soll, wozu es im Endeffekt einer Sperrerklärung im Sinne von § 96 StPO bedarf [228].

Privatpersonen sind der Informant und die Vertrauensperson – VP. ***Informant*** *ist eine Person, die im Einzelfall bereit ist, gegen Zusicherung der Vertraulichkeit der Strafverfolgungsbehörde Informationen zu geben* (Nr. A.I.2.1 Anlage D zu den RiStBV). Er zeichnet sich dadurch aus, dass er zu einem abgeschlossenen und umgrenzten Sachverhalt Angaben macht, die von einem Polizeibeamten anonymisiert und in dieser Form zu den Ermittlungsakten gegeben werden. Sie können zur Begründung weiterer Ermittlungsmaßnahmen genutzt und über den „führenden“ Polizeibeamten auch in die gerichtliche Hauptverhandlung eingeführt werden [229].

Vertrauensperson *ist eine Person, die, ohne einer Strafverfolgungsbehörde anzugehören, bereit ist, diese bei der Aufklärung von Straftaten auf längere Zeit vertraulich zu unterstützen, und deren Identität grundsätzlich geheimgehalten wird*

[225] Einleitung, B. Hintergrund: Carding-Boards.

[226] Richtlinien über die verdeckte Informationsgewinnung im Rahmen der Strafverfolgung durch Informantinnen und Informanten, Vertrauenspersonen, Verdeckte Ermittlerinnen und Ermittler und sonstige nicht offen ermittelnde Polizeibeamtinnen und Polizeibeamte

[227] Richtlinien für das Straf- und Bußgeldverfahren

[228] 3.1.1 Auskünfte von Behörden und anderen Einrichtungen

[229] Auf die Probleme mit dem Zeugenbeweis vom Hörensagen und dem Unmittelbarkeitsprinzip (vor Allem: § 250 StPO) wird später eingegangen.

(Nr. A.I.2.2 Anlage D zu den RiStBV). Die VP arbeitet längerfristig mit der Polizei zusammen und vermittelt ihr Informationen über kriminelle Subkulturen, über das Umfeld bestimmter Täter und über begangene oder geplante Straftaten. Über die Qualität der vermittelten Informationen lässt sich streiten. Je näher sich die VP im unmittelbaren privaten Umfeld des Täters bewegt, desto leichter kann sie enttarnt werden, so dass die Auskünfte häufig gar nicht verwendet werden können, um Gefahren für die VP zu vermeiden. Die Zusage der Geheimhaltung ist zu widerrufen, wenn die VP lügt oder Straftaten begeht (Nr. 4. Anlage zu den RiStBV).

Verdeckte Ermittler und Nicht offen ermittelnde Beamte - NoeP – sind hingegen Polizeibeamte, die ihre polizeiliche Rolle nicht offenbaren.

Verdeckte Ermittler sind Beamte des Polizeidienstes, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität (Legende) ermitteln. Sie dürfen unter der Legende am Rechtsverkehr teilnehmen (§ 110a Abs. 2 StPO). Die Einzelheiten über den Einsatz, die Pflichten und Aufgaben der Verdeckten Ermittler ergeben sich aus dem Teil A.II. der Anlage D zu den RiStBV. So darf er zum Beispiel Ermittlungen zurückstellen, zu denen er nach dem Legalitätsprinzip sofort verpflichtet wäre; *dies gilt nicht, wenn sofortige Ermittlungsmaßnahmen wegen der Schwere der neu entdeckten Tat geboten sind* (Nr. A.II.2.6.2 Anlage D zu den RiStBV).

Die Ermittlungstätigkeit sonstiger nicht offen ermittelnder Polizeibeamter richtet sich nach den allgemeinen Bestimmungen, ist die schlichte Aussage von Nr. A.II.2.9 der Anlage D zu den RiStBV. Das ist wenig aussagekräftig.

3.3.2 Grenzen zwischen VP und NoeP

Schon 1981 hat das BVerfG die Zusage der Vertraulichkeit für Informanten oder der Geheimhaltung an Vertrauenspersonen und Verdeckte Ermittler als zulässig angesehen, wenn es um die Aufklärung der schweren Kriminalität geht [230].

Gesetzliche Regelungen sind mit den §§ 110a bis 110c StPO nur für den Verdeckten Ermittler eingeführt worden. Sein Einsatz setzt als untere Schwelle Formen der erheblichen Kriminalität voraus, das heißt Serientaten in gewerbs- oder gewohnheitsmäßiger Form (§ 110a Abs. 1 S. 1 Nr. 3 StPO). Der Einsatz bedarf der Zustimmung der Staatsanwaltschaft (§ 110b Abs. 1 StPO) und dann, wenn er gegen einen bestimmten Beschuldigten gerichtet ist, einer gerichtlichen Zustimmung (§ 110b Abs. 2 S. 1 Nr. 1 StPO). Die gesetzlichen Vorschriften dienen vor allem auch dem Schutz der eingesetzten Beamten [231]: *Der Gesetzgeber wollte ihre heimliche und auf Täuschung ausgerichtete amtliche Tätigkeit, die zu den sonst für sie geltenden Täuschungsverboten und Belehrungspflichten (§§ 136a, 163a Abs. 4 und 5 StPO) in Widerspruch geraten kann, zum Schutz der Polizeibeamten auf eine die Generalklauseln ausformende spezielle Gesetzesgrundlage stellen. Eine solche Fürsorgepflicht besteht gegenüber Vertrauenspersonen nicht, weil sie die Polizei als Privatpersonen unterstützen und dabei nicht gegen sonst für sie geltende Amtspflichten verstoßen können*. <Rn 7>

Als Regelfall sieht § 110b StPO den Polizeibeamten an, der zunächst verdeckt ermittelt, in der gerichtlichen Verhandlung aber offen als Zeuge zur Verfügung steht. Erst § 110b Abs. 3 StPO lässt es als Ausnahme davon zu, dass seine Identität auch nach Beendigung des Einsatzes geheimgehalten werden kann, wenn er persönlich oder sein künftiger Einsatz gefährdet wäre. Das hat zur Folge, dass die Erkenntnisse des Verdeckten Ermittlers durch einen VE-Führer, also einem Zeugen vom

---

[230] **BVerfG**, Beschluss vom 26.05.1981 - 2 BvR 215/81

[231] **BGH**, Urteil vom 22.012.1995 – 3 StR 552/94

Hörensagen [232], oder unter Tarnung in die Hauptverhandlung eingeführt werden müssen. Insoweit schränkt das BVerfG den Beweiswert schon seit 1995 deutlich ein [233]: <Die> *von einem Vernehmungsbeamten wiedergegebenen Aussagen sind deshalb besonders kritisch zu würdigen.* [234].

Bereits 1995 hat der BGH den Scheinkauf durch einen NoeP nach Maßgabe der Ermittlungsgeneralklausel anerkannt [235] und ihn vom Verdeckten Ermittler abgegrenzt: *Entscheidend ist, ob der Ermittlungsauftrag über einzelne wenige, konkret bestimmte Ermittlungshandlungen hinausgeht, ob es erforderlich werden wird, eine unbestimmte Vielzahl von Personen über die wahre Identität des verdeckt operierenden Polizeibeamten zu täuschen, und ob wegen der Art und des Umfanges des Auftrages von vornherein abzusehen ist, dass die Identität des Beamten in künftigen Strafverfahren auf Dauer geheimgehalten werden muss. Dabei ist darauf abzustellen, ob der allgemeine Rechtsverkehr oder die Beschuldigtenrechte in künftigen Strafverfahren eine mehr als nur unerhebliche Beeinträchtigung durch den Einsatz des verdeckt operierenden Polizeibeamten erfahren können.* <Rn 7>

Ein Einsatz als verdeckter Ermittler kann danach ausscheiden, wenn ein Polizeibeamter - sei es auch unter einer Legende - lediglich als Scheinaufkäufer auftritt, ohne in die Ermittlungen darüber hinaus eingeschaltet zu sein. … <Diese Grenze ist überschritten, wenn> *der Polizeibeamte nicht nur bei einem Scheinaufkauf mitwirkte, sondern … langfristig angelegte Ermittlungsmaßnahmen gegen einen sich immer mehr vergrößernden Personenkreis durchführte.* <Rn 8>

Unterhalb dieser Schwelle handelnde NoeP unterliegen nicht den Verfahrensvorschriften für den Verdeckten Ermittler [236]. Das gilt jedoch nicht für andere Verfahrensvorschriften, die dem Recht auf ein ***faires Verfahren*** folgen. Dafür gelten die Grundsätze, die vom BVerfG aufgestellt worden sind [237]: *Eine Verletzung des Rechts auf ein faires Verfahren liegt erst dann vor, wenn eine Gesamtschau auf das Verfahrensrecht - auch in seiner Auslegung und Anwendung durch die Gerichte - ergibt, dass rechtsstaatlich zwingende Folgerungen nicht gezogen worden sind oder rechtsstaatlich Unverzichtbares preisgegeben wurde (...). Im Rahmen dieser Gesamtschau sind auch die Erfordernisse einer funktionstüchtigen Strafrechtspflege in den Blick zu nehmen (...).* [238]

Wegen der Abgrenzung zwischen Verdecktem Ermittler und NoeP ist deshalb von besonderer Bedeutung:

- Die Rechtsfigur des NoeP ist im Zusammenhang mit polizeilichen Scheingeschäften entwickelt worden. Er grenzt sich negativ vom Verdeckten Ermittler dadurch ab, dass er einen sachlich und zeitlich umgrenzten Ermittlungsauftrag hat.
- Der NoeP nimmt vor allem den Kontakt zu einer bestimmten Person auf. Seine Legende ist grundsätzlich nicht dazu bestimmt, gegenüber einer Vielzahl von Personen verwendet zu werden.
- Der Verdeckte Ermittler weist sich dadurch aus, dass er auf Dauer unter einer ihm verliehenen Legende ermittelt (§ 110a Abs. 2 StPO).

  Auf „Dauer“ (110a Abs. 2 StPO) und „längerfristig“ (§ 163f Abs. 1 StPO) sind keine synonymen Rechtsbegriffe. Mit dem Erfordernis, dass die

---

[232] Grundsätzlich zulässig: BVerfG, Beschluss vom 26.05.1981 - 2 BvR 215/81, abgedruckt bei Jens Ph. **Wilhelm**, Entscheidungssammlung zum Strafverfahrensrecht, Stand Dezember 2003, S. 7.

[233] BVerfG, Beschluss vom 19.07.1995 - 2 BvR 1142/93, abgedruckt bei Jens Ph. **Wilhelm**, Entscheidungssammlung zum Strafverfahrensrecht, Stand Dezember 2003, S. 18, 19.

[234] Zur Problematik des Zeugen vom Hörensagen: A.5.2 Geltung und Wechselwirkungen.

[235] **BGH**, Urteil vom 07.03.1995 - 1 StR 685/94

[236] **BGH**, Urteil vom 22.02.1995 – 3 StR 552/94

[237] **BVerfG**, Beschluss vom 15.10.2009 - 2 BvR 2438/08, Rn 7

[238] Siehe auch die ersten beiden in der Strafsache gegen al-Motassadeq ergangenen Revisionsentscheidungen:
BGH, Urteil vom 04.03.2004 - 3 StR 218/03,
BGH, Urteil vom 16.11.2006 - 3 StR 139/06.

längerfristige Observation vom Gericht angeordnet werden muss (§ 163f Abs. 3 StPO), gibt der Gesetzgeber aber eine Auslegungshilfe: Maßnahmen, deren Dauer zwei Tage überschreiten sollen, verlangen im Zweifel nach einer gerichtlichen Anordnung. Die Schwelle für die Schwere der Kriminalität liegt in beiden Anwendungsfällen bei den Straftaten von erheblicher Bedeutung.

- Sowohl der Verdeckte Ermittler als auch der NoeP treten mit den Verdächtigen oder Beschuldigten in persönlichen Kontakt, ohne dass sie offenbaren, dass sie Polizeibeamte sind. Im Hinblick auf die Verfahrensregeln zum Täuschungsverbot und den polizeilichen Belehrungspflichten verlangen sie deshalb im Zweifel nach einer spezialgesetzlichen Ermächtigungsgrundlage. Solange es bei einer einfachen Legende (Tarnung) bleibt, reicht dazu die Ermittlungsgeneralklausel aus [239].

  In bemerkenswerter Kleinarbeit hat der BGH 2010 die Voraussetzungen und Grenzen für den Einsatz eines Verdeckten Ermittlers herausgearbeitet [240] <Rn 14 ff.> und im Ergebnis festgestellt <Rn 21 ff.>, dass jedenfalls die Ausnutzung der situativen Unfreiheit in einem Gefängnis der Selbstbelastungsfreiheit aus Art 6 Abs. 1 MRK widerspricht <Rn 23> [241]. Von Bedeutung ist an dieser Stelle vor allem, dass allein aus der fehlenden Belehrung nach § 136 StPO kein Verwertungsverbot abgeleitet werden kann <Rn 16>: *Diese Vorschrift ist nur auf „offene" Vernehmungen anwendbar und will (lediglich) sicherstellen, dass der Beschuldigte vor der irrtümlichen Annahme einer Aussagepflicht bewahrt wird, zu der er möglicherweise eben durch die Konfrontation mit dem amtlichen Auskunftsverlangen veranlasst werden könnte.*

  Dasselbe gilt für private Ermittlungshelfer [242] und deshalb sicherlich auch für den NoeP.

- Die Absicherung einer Ermittlungsmaßnahme durch staatsanwaltschaftliche Zustimmungen oder gerichtliche Beschlüsse dient nicht nur der rechtsstaatlichen Kontrolle von Eingriffsmaßnahmen, sondern vor allem auch dem Schutz der eingesetzten Beamten.

  Insoweit gilt für den NoeP dasselbe wie für den Verdeckten Ermittler: Sie verschweigen, dass sie Polizeibeamte sind, und handeln unter Tarnidentitäten, nur dass sie das nur vorübergehend und innerhalb eines umgrenzten Ermittlungsauftrags tun.

Für die Ermittlungen im Internet ist daraus zu folgern, dass die auf Dauer angelegte Kontaktaufnahme zu „einem bestimmten Beschuldigten" einer gerichtlichen Zustimmung gemäß § 110b StPO bedarf [243].

In verschiedenen Entscheidungen zu besonderen Eingriffsmaßnahmen hat sich das BVerfG immer wieder für eine effektive gerichtliche Kontrolle ausgesprochen, die nicht nur die Anordnung als solche, sondern auch die Art und Weise der Durchführung betrifft. Damit verbindet es auch die Gefahr der Umgehung des Richtervorbehalts [244]. Den Grundgedanken daraus hat der Gesetzgeber bei der Schaffung des geltenden § 101 StPO übernommen. Angesichts der bestehenden gesetzlichen Regelungen zum Einsatz eines Verdeckten Ermittlers müssen deshalb die Anwendungsfälle unterhalb des Schwellenbereiches zum Verdeckten Ermittler begrenzt und klar definiert werden.

Deshalb sind nur kurzfristige Kontakte, die dem Scheingeschäft vergleichbar sind, unterhalb dieser Schwelle angesiedelt. Das gilt etwa für Scheingeschäfte im Internet oder für andere Kontaktaufnah-

---

239 3.3 personale Ermittlungen

240 **BGH**, Beschluss vom 18.05.2010 – 5 StR 51/10

241 So auch: **BGH**, Beschluss vom 27.01.2009 - 4 StR 296/08

242 **BGH**, Beschluss vom 31.03.2011 - 3 StR 400/10, Rn 8, 9

243 Im Einzelnen: 3.3.3 Verdeckter Ermittler im gewalttätigen Umfeld.

244 Zuletzt im Zusammenhang mit der längerfristigen Observation: **BVerfG**, Beschluss vom 02.07.2009 – 2 BvR 1691/07, Rn 75.

men, die der Identifizierung oder Ergreifung des Beschuldigten dienen. Insoweit ist der üblichen Praxis folgend das Einvernehmen mit der Staatsanwaltschaft als Herrin des Ermittlungsverfahrens zu suchen.

Nach dem Modell des Gesetzgebers besteht ein vierstufiges Modell für die personalen Ermittlungen ohne Offenlegung der Polizisten-Rolle:

- Sachlich umgrenzter Einsatz eines NoeP mit Zustimmung der Staatsanwaltschaft, zum Beispiel im Zusammenhang mit einem Scheingeschäft oder zur Identifizierung eines Täters durch eine direkte Kontaktaufnahme. Seine spätere Geheimhaltung kann nur eine Ausnahme im Einzelfall sein (Nr. A.II.2.9 S. 2 Anlage D zu den RiStBV).
- Verdeckter Ermittler mit Zustimmung der Staatsanwaltschaft nach § 110b Abs. 1 StPO
- Verdeckter Ermittler mit gerichtlicher Zustimmung nach Maßgabe von § 110b Abs. 2 StPO
- Geheimhaltung gemäß § 110b Abs. 3 StPO

3.3.3 Verdeckter Ermittler im gewalttätigen Umfeld

Verdeckte Ermittler werden bevorzugt in gewaltbereiten Umfeldern der schweren, vor allem der Betäubungsmittel- und Organisierten Kriminalität [245] im übrigen eingesetzt, die in aller Regel eine persönliche Gefährdung oder die von Angehörigen erwarten lassen. Dadurch hat sich das polizeiliche Leitbild darauf verengt, grundsätzlich jeden Verdeckten Ermittler als einen Polizeibeamten anzusehen, dessen Identität in eigenem Interesse und zur Sicherung seiner Wiederverwendung geheim gehalten werden muss.

Das stände im Einklang mit der Position, die Volker Krey 1994 entwickelt hat [246]: *In der Legaldefinition für den VE in § 110 a II StPO in der Fassung des OrgKG ist jene Geheimhaltung zwar nicht mehr ausdrücklich genannt; sie ist aber gemäß § 96 i.V.m. § 110 b III StPO weiterhin für den VE-Einsatz typisch, und zwar sowohl in der Rechtswirklichkeit als auch gemäß den Anforderungen des geltenden Rechts. Denn in der Regel wird entweder der Gesichtspunkt der Gefährdung von Leben, Leib oder Freiheit des VE (bzw. einer anderen Person, etwa seiner Angehörigen) oder der Aspekt der Gefährdung der Möglichkeit seiner weiteren Verwendung eine Geheimhaltung seiner Identität gebieten. Mithin ist für den VE charakteristisch, dass seine Identität im Strafverfahren nicht offenbart wird.*

Krey sieht deshalb zwischen dem NoeP und dem Verdeckten Ermittler den qualifizierten Scheinaufkäufer angesiedelt, der unter einer ihm verliehenen Legende immer wieder, aber in verschiedenen Ermittlungsverfahren eingesetzt und dessen Identität geheim gehalten wird. Dem folgt die verbreitete rechtliche Legende, alle Einsatzformen unterhalb der Geheimhaltungsschwelle seien polizeiliche NoeP-Einsätze, für die es keines gerichtlichen Beschlusses bedürfe.

Dem widerspricht bereits das vom Gesetzgeber geschaffene Leitbild mit den mehrstufigen Zulassungsanforderungen an den Verdeckten Ermittler. Die großzügige Annahme von NoeP-Einsätzen birgt die Gefahren, dass Polizeibeamte ohne förmliche Ermächtigung längerfristige verdeckte Ermittlungen durchführen, dass die gebotene gerichtliche Kontrolle unterlaufen wird und schließlich Beweisverwertungsverbote drohen [247]. Sie lässt sich mit den heutigen Anforderungen an die sachlichen und formellen Voraussetzungen grundrechtsrelevanter Eingriffsmaßnahmen nicht mehr in Einklang bringen.

So fordert der BGH inzwischen eine strenge Einhaltung der formellen Voraussetzungen [248]: *Zwar sind die von einem Verdeckten Ermittler gewonnenen Erkenntnisse im Grundsatz verwertbar, wenn*

---

[245] Siehe Nr. 2 Anlage E zu den RiStBV.

[246] Volker **Krey**, Rechtsprobleme des Einsatzes qualifizierter Scheinaufkäufer im Strafverfahrensrecht, ZKA Köln 1994, S. 33

[247] 2. Grundrechte und Eingriffsmaßnahmen

[248] **BGH**, Beschluss vom 27.01.2009 - 4 StR 296/08, Rn 8

die Voraussetzungen für seinen Einsatz und die hierfür erforderliche richterliche Zustimmung (§§ 110a Abs. 1 Satz 4, 110b Abs. 2 Nr. 2 StPO) vorlagen … Auch der Europäische Gerichtshof für Menschenrechte fordert verstärkt *eine gesetzliche Grundlage, die spezifische und detaillierte Anforderungen an die Zulässigkeit dieser heimlichen Ermittlungsmaßnahme stellt und damit einen hinreichenden Schutz gegen Willkür bietet* [249].

Ein Verwertungsverbot kann <zwar> *nur verfassungsrechtlicher Natur sein* [250] und *es besteht kein Rechtssatz des Inhalts, dass ein Beweiserhebungsverbot in jedem Fall ein Beweisverwertungsverbot nach sich zieht* [251]. Insoweit sind die Grenzen, die eine Verletzung des Rechts auf ein faires Verfahren erwarten lassen, sehr hoch gesetzt [252]. Dennoch lässt gerade ein Verstoß gegen die formellen Einsatzvoraussetzungen schnell befürchten, *dass rechtsstaatlich zwingende Folgerungen nicht gezogen worden sind oder rechtsstaatlich Unverzichtbares preisgegeben wurde* [253].

Das schränkt die Zulässigkeit von NoeP-Einsätzen auf die Fälle ein, die der BGH schon 1995 herausgearbeitet hat, nämlich auf *einzelne wenige, konkret bestimmte Ermittlungshandlungen* [254]. Dem Leitbild des Gesetzgebers folgend sind deshalb die länger dauernden Beobachtungen eines Beschuldigten im Internet nach Maßgabe der Vorschriften über die Observation und den Verdeckten Ermittler zu beurteilen.

Dieser Schluss steht der weiten Öffnung nicht entgegen, die das BVerfG wegen der einfachen Ermittlungshandlungen im Internet formuliert hat [255], weil es nur einfache Legenden nach Maßgabe der vier einschlägigen Grundrechte [256] vor Augen hatte und nicht auch die bundesrechtlichen Anforderungen an die formelle Gerechtigkeit und das faire Verfahren.

3.3.4 Beobachtungen und Kommunikation bei Internetermittlungen

Keinen maßgeblichen Grundrechtseingriff lassen die einfachen Internetermittlungen erwarten, die das BVerfG hervorgehoben hat [257]:

- Kenntnisnahme aller öffentlich zugänglichen Informationen,
- Recherche in allgemein zugänglichen Informations- und Kommunikationsdiensten, *die sich zumindest an einen nicht weiter abgegrenzten Personenkreis richten*,
- Verwendung einer einfachen Legende (Fake Account) und
- legendierte Kommunikation über einen längeren Zeitraum.

Sie sind von der Ermittlungsgeneralklausel in § 161 Abs. 1 StPO abgedeckt.

Zwei Einschränkungen sind zu machen:

Im Hinblick auf die „Fake Accounts“ hat das BVerfG nur eine einfache Legende vor Augen, die sich mehr oder weniger auf das Verschweigen der Rolle als Polizist beschränkt. Ausgefeilte Legenden nach Maßgabe von § 110a Abs. 3 StPO erfordern mindestens die Zustimmung der Staatsanwaltschaft (§ 110b Abs. 1 StPO).

Die Frage nach der zulässigen Dauer einfach legendierter Ermittlungen ist noch ungeklärt. Die Entscheidung des Gesetzgebers, für die längerfristige Observation dann eine gerichtliche Zustimmung zu fordern, wenn sich die Maßnahme gegen einen bestimmten Beschuldigten richtet und länger als zwei Tage dauern soll (§ 163f Abs. 1 StPO), ist eine Auslegungshilfe ohne zwingende Sperrwirkung.

---

[249] Zum Einsatz von Aufzeichnungsgeräten am Verdeckten Ermittler: **EGMR** Nr. 4378/02 - Urteil der Großen Kammer vom 21.01.2009 (Bykov v. Russland), Leitsatz 1. Siehe auch § 161 Abs. 3 StPO.

[250] **BGH**, Beschluss vom 18.01.2011 - 1 StR 663/10, Rn 22

[251] Ebenda, Rn 25.

[252] Siehe oben: Faires Verfahren. **BVerfG**, Beschluss vom 15.10.2009 - 2 BvR 2438/08, Rn 7.

[253] BVerfG ebenda.

[254] **BGH**, Urteil vom 07.03.1995 - 1 StR 685/94

[255] 3.3 personale Ermittlungen

[256] 2. Grundrechte und Eingriffsmaßnahmen

[257] 3.3 personale Ermittlungen

Allgemeine Internet-Patrouillen und die längerfristige, auch aktive Teilnahme in sozialen Netzwerken sind von der Freizeichnung des BVerfG sicherlich gedeckt. Das gilt auch für die Foren und Boards, die zwar kriminelle Angebote erwarten lassen, aber keine besonderen Zugangssperren aufweisen. Verdichtet sich der Verdacht so stark, dass Beschuldigte identifiziert werden können, bedürfen längerfristige Beobachtungen des Beschuldigten ohne kommunikative Kontakte eines Beschlusses nach § 163f Abs. 3 StPO, wobei die zeitliche Grenzziehung von zwei Tagen beachtlich ist. Der Beschluss setzt erhebliche Straftaten voraus und die Staatsanwaltschaft und die Polizei sind zur Anordnung bei Gefahr in Verzug berechtigt. Ihre Anordnung muss binnen drei Werktage gerichtlich bestätigt werden.

Sachlich und zeitlich begrenzte kommunikative Kontakte für ein Scheingeschäft oder eine Identifikation des Beschuldigten sind von der Ermittlungsgeneralklausel abgedeckt. Lassen die Gesprächskontakte in einem Forum oder Board die Vorbereitung von Straftaten oder eine Beutesicherung erwarten, dann ist eine staatsanwaltschaftliche Zustimmung zu weiteren Gesprächskontakten nach § 110b Abs. 1 S. 1 StPO geboten, die bei Gefahr in Verzug von der Polizei ersetzt werden darf. Die polizeiliche Anordnung bedarf der staatsanwaltschaftlichen Zustimmung binnen drei Werktage.

Das führt zu folgender Staffelung:

- Die allgemeine Informationsbeschaffung, Nutzung von Fake Accounts und Kommunikation in Sozialen Netzwerken, Foren und Boards sind von der Ermittlungsgeneralklausel abgedeckt, auch wenn sie längerfristig aufrecht erhalten werden.
- Die Kommunikation mit einem Beschuldigten, um ein Scheingeschäft abzuwickeln oder ihn anhand weniger Kontakte zu identifizieren, ist ein anerkannter NoeP-Einsatz, der von der Ermittlungsgeneralklausel gerechtfertigt ist. Der Einsatz ist nach Maßgabe der Sachleitungsbefugnis der Staatsanwaltschaft mit ihr abzustimmen [258].
- Legendierte längerfristige Gesprächskontakte in Foren und Boards, die kriminelle Inhalte aus dem Bereich der erheblichen Kriminalität erwarten lassen, bedürfen als Einsatz eines Verdeckten Ermittlers der Zustimmung der Staatsanwaltschaft (§ 110b Abs. 1 StPO). Sie *ist schriftlich zu erteilen und zu befristen* (§ 110b Abs. 1 S. 3 StPO) und kann verlängert werden (§ 110b Abs. 1 S. 4 StPO).
- Die über zwei Tage hinaus gehende Beobachtung eines Beschuldigten ohne Gesprächskontakt zu ihm bedarf einer gerichtlichen Zustimmung gemäß § 163f Abs. 3 StPO. Sie setzt Formen der erheblichen Kriminalität voraus und kann bei Gefahr im Verzug von der Staatsanwaltschaft oder der Polizei ersetzt werden. Diese Anordnung muss binnen drei Werktage gerichtlich bestätigt werden. Es gelten die formellen Anforderungen des § 100b Abs. 2 StPO (Schriftform, Bestimmtheit).
- Legendierte längerfristige Gesprächskontakte in Foren und Boards mit Beschuldigten, die ihren Merkmalen nach identifiziert sind, bedürfen eines gerichtlichen Beschlusses nach § 110b Abs. 2 StPO, wenn sicher zu erwarten ist, dass die Maßnahme länger als zwei Tage dauern wird. § 163f Abs. 2 StPO dient insoweit als Auslegungshilfe.
- Die Geheimhaltung des verdeckt ermittelnden Beamten über den Einsatz hinaus ist jedenfalls im Zusammenhang mit den Ermittlungen in Foren und Boards im Internet eine Ausnahme (§ 110b Abs. 3 StPO). Gewalttätige Tätergruppen sind nach den bisherigen Erfahrungen die Ausnahme und Erfahrungen mit der „Wiederverwendung“ sind mir jedenfalls nicht bekannt.

---

[258] In diesen Fällen ist ein schriftlicher Einsatzplan zu empfehlen, in dem die Art, Dauer und Umstände ausgeführt sind und der zu den Akten genommen wird. Er beschreibt vor allem auch die verwendete Legende und muss von der Staatsanwaltschaft genehmigt werden.

3.3.5 Scheinkauf

Die gerichtliche Auseinandersetzung mit dem Scheinkauf hat ihren Ursprung bei den Ermittlungen im Zusammenhang mit Rauschgiften. Er dient einerseits dazu, Rauschgift und andere gefährliche Gegenstände (Waffen, Falschgeld, Fälscherwerkzeuge, Arzneien) dem kriminellen Schwarzmarkt zu entziehen und andererseits die handelnden Täter zu fassen. Die Zulässigkeit des Scheinkaufes wird zusammen mit der Zulässigkeit des NoeP-Einsatzes seit 1995 von BGH vertreten [259]. Wichtig für ihn ist, dass die Grenzen zur unzulässigen Tatprovokation gewahrt bleiben [260] und das ist der Fall, wenn der Täter bereits tatgeneigt ist und nur noch die Einzelheiten des kriminellen Geschäftes vereinbart und abgewickelt werden müssen. Das ist der Fall, wenn der Polizist *nur die offen erkennbare Bereitschaft zur Begehung oder Fortsetzung von Straftaten ausnutzt* [261].

Nach der Systematik des Gesetzes, das längerfristige Observationen und Verdeckte Ermittler bereits im Bereich der erheblichen Straftaten zulässt, ist das auch für den Scheinkauf anzunehmen [262].

Der von der Polizei überwachte Scheinkauf führt grundsätzlich zu einem *schuldunabhängigen Strafmilderungsgrund* [263], so dass die Sachleitungsbefugnis der Staatsanwaltschaft deren Zustimmung verlangt.

3.3.6 Keuschheitsprobe

Nr. A.II.2.2 S. 1 Anlage D zu den RiStBV formuliert einen ehernen Grundsatz, der für alle verdeckten Ermittlungen gilt: *Verdeckte Ermittler dürfen keine Straftaten begehen*. Das schränkt den Zugang zu geschlossenen Benutzerkreisen ein, wenn sie das Begehen einer Straftat zur Voraussetzung für den Zugang machen.

In diesen Fällen sind der kriminalistischen List keine weiteren Grenzen gesetzt, weil die Abrede und Durchführung von Straftaten keinen Grundrechtsschutz genießt [264]. Die absolute Grenze ist erreicht, wenn die Vorbereitung oder Leistung der Keuschheitsprobe eine Straftat darstellt. Sie ist zum Beispiel bei der Beschaffung und Weitergabe kinderpornographischer Abbildungen überschritten, deren Besitz bereits nach § 184b Abs. 4 StGB strafbar ist.

In diesem Zusammenhang wird häufig der rechtfertigende Notstand (§ 34 S. 1 StGB) bemüht: *Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt*. Eine derart ***gegenwärtige Gefahr*** lässt sich aus dem Verbreiten betagten Bildmaterials jedenfalls nicht herleiten. Sie kann auch keine generelle Freizeichnung für eine bestimmte Art von Kriminalität oder Ermittlungsmaßnahme sein, weil sie nur einen extremen Einzelfall betreffen kann.

---

259 3.3.2 Grenzen zwischen VP und NoeP; **BGH**, Urteil vom 07.03.1995 - 1 StR 685/94.

260 Einzelheiten und Nachweise: **CF**, keine Tatprovokation, 20.04.2008.

261 **BGH**, Urteil vom 18.11.1999 - 1 StR 221/99, Rn 55

262 Die Rechtsprechung bezieht sich in aller Regel auf die schwere Kriminalität.

263 **BGH**, Urteil vom 18.11.1999 - 1 StR 221/99, Rn 65

264 2. Grundrechte und Eingriffsmaßnahmen

Anhang

Der Cyberfahnder beschäftigt sich immer wieder mit grundsätzlichen Fragen des Strafverfahrensrechts. Die erste Einführung stellte ausgewählte, praxisrelevante Einzelfragen vor [265]. Aus ihr ist ein Aufsatz über die Gefahr in Verzug hervorgegangen [266]. Beide Beiträge sind seit 2007 nicht mehr aktualisiert worden, so dass ihre grundlegenden Aussagen noch immer zutreffen, aber nicht den aktuellen Stand der Rechtsprechung wieder geben. Das gilt besonders für die Auseinandersetzung mit den Bestands- und Verkehrsdaten, die im vorliegenden Aufsatz gründlich dargestellt sind.

Auch aus 2007 stammt ein einführender Beitrag über die rechtliche Definitionen verschiedener Verdachtsstufen [267], also

- dem Anfangsverdacht, der nach der Einleitung eines Ermittlungsverfahrens verlangt (§ 152 Abs. 2 StPO),
- dem dringenden Verdacht, der für die Untersuchungshaft ausschlaggebend ist, und
- dem hinreichenden Verdacht, der für die Anklageerhebung und ihre Zulassung zur Hauptverhandlung erforderlich ist.

Drei Aufsätze ergänzen die grundlegenden Auseinandersetzungen mit dem Strafverfahrensrecht und haben direkte Einflüsse auf die in diesem Aufsatz angeschnittenen Fragen. Sie werden im Anhang in überarbeiteter Form zusammen gefasst:

- Eingriffsrechte während der Vorermittlungen, 12.08.2009
- Geltung von Beweisen und Erfahrungen, 29.11.2009
- strafprozessuale Maßnahmen, 31.01.2011

---

265 **CF**, Auskünfte, Aussagen, Beweismittel, 2007; Dieter **Kochheim**, Auskünfte, Aussagen, Beweismittel. Einführung in das allgemeine Beweismittelrecht, 02.07.2007 (PDF)

266 **CF**, Gefahr im Verzug, 2007

267 **CF**, Verdacht, 2007

A.1 Staatsanwaltschaft und Strafverfolgung [268]

Die Aufgaben der Strafverfolgung und der Anklageerhebung obliegen der Staatsanwaltschaft (§ 152 Abs. 1 StPO) in eigener Verantwortung [269]. Sie ist die Herrin des Ermittlungsverfahrens (§ 160 Abs. 1 StPO) und eine von den Gerichten unabhängige (§ 150 GVG) Verwaltungsbehörde (Exekutive), die mehr als die Verwaltung im übrigen dem Legalitätsprinzip unterworfen (§ 152 Abs. 2 StPO) und als selbständiges Organ in die Rechtspflege eingegliedert ist [270]. Staatsanwaltschaft und Gericht erfüllen gemeinsam die Aufgabe der "Justizgewährung" [271], wobei das Gericht im Ermittlungsverfahren grundsätzlich nur auf Antrag der Staatsanwaltschaft (oder aufgrund eines Rechtsmittels) tätig wird (§ 162 Abs. 1 StPO).

Dabei muss der Richter *dafür Sorge tragen, dass die sich aus der Verfassung und dem einfachen Recht ergebenden Voraussetzungen der Durchsuchung genau beachtet werden* (… [272]). *Als Kontrollorgan der Strafverfolgungsbehörden trifft ihn die Pflicht, durch eine geeignete Formulierung des Durchsuchungsbeschlusses im Rahmen des Möglichen und Zumutbaren sicherzustellen, dass der Eingriff in die Grundrechte messbar und kontrollierbar bleibt*. [273]

Staatsanwälte unterliegen einerseits den Anweisungen ihrer Vorgesetzten (§ 146 GVG), die alle "Amtsverrichtungen" selbst übernehmen (Devolutionsrecht) oder mit ihrer Wahrnehmung einen anderen Beamten beauftragen können (Substitutionsrecht, § 145 Abs. 1 GVG [274]). Im Außenverhältnis sind sie andererseits uneingeschränkt zu allen der Staatsanwaltschaft zugewiesenen Amtshandlungen berechtigt (§ 144 GVG). Dabei richtet sich die örtliche Zuständigkeit des Staatsanwalts nach der des Gerichts, für das er bestellt ist (§ 143 Abs. 1 GVG), darüber hinaus ist er zu allen Amtshandlungen verpflichtet, bei denen Gefahr in Verzug ist (§ 143 Abs. 2 GVG, § 163 Abs. 1 StPO). Diese Verpflichtung gilt auch für den Richter (Notstaatsanwalt, § 165 StPO).

A.2 Verhältnis zur Polizei

Im Rahmen strafrechtlicher Ermittlungen sind die Polizeibeamten "Ermittlungspersonen der Staatsanwaltschaft" und müssen ihren Anweisungen Folge leisten (§ 152 Abs. 1 GVG; § 161 Abs. 1 S. 2 StPO [275]). Das betrifft nicht ihre ordnungspolizeilichen Aufgaben wie die Gefahrenabwehr und die Prävention. Ermittlungspersonen können auch aus anderen Verwaltungszweigen stammen (zum Beispiel Feuerwehr, Förster, Bergamt), wenn ihnen die Landesverwaltung diese Aufgabe überträgt (§ 152 Abs. 2 S. 1 GVG). Dadurch sind sie zu allen Maßnahmen berechtigt, die die Strafprozessordnung den Ermittlungspersonen besonders bei Gefahr in Verzug zuweist. Eine einzigartige Rolle haben die Finanzbehörden, denen im Steuerstrafverfahren bis einem bestimmten Grad die Aufgaben der Staatsanwaltschaft übertragen sind (§ 399 Abs. 1 AO).

---

[268] Die Beiträge A.1 bis A.3 sind zuerst erschienen unter: **CF**, strafprozessuale Maßnahmen, 31.01.2011.

[269] **BVerfG**, Urteil vom 20.02.2001 - 2 BvR 1444/00, Rn. 27

[270] **BVerfG**, Beschluss vom 05.11.2001 - 2 BvR 1551/01, Rn. 10

[271] Im Anschluss an Eberhard Schmidt: **BVerfG**, Urteil vom 19.03.1959 - 1 BvR 295/58, Rn. 21.

[272] *Der einzelne soll nicht nur Objekt der richterlichen Entscheidung sein*: **BVerfG**, Beschluss vom 08.01.1959 - 1 BvR 396/55, Rn. 22, 27.

Verlangt wird vom Richter eine *unabhängige, neutrale Prüfung, ob die gesetzlichen Voraussetzungen für die Durchführung dieser Maßnahme vorliegen und der Verhältnismäßigkeitsgrundsatz gewahrt ist*: **BVerfG**, Beschluss vom 16.06.1981 - 1 BvR 1094/80, Rn. 40, 44 (Wohnungsdurchsuchung im Rahmen einer Zwangsvollstreckung).

[273] **BVerfG**, Urteil vom 20.02.2001 - 2 BvR 1444/00, Rn. 28

[274] Anschaulich: Roland **Hefendehl**, Strafprozessrecht (SoS 2006), Uni Freiburg 05.05.2006

[275] Früher: Hilfsbeamte der Staatsanwaltschaft.

Die §§ 160 Abs. 1, 161 Abs. 1 S. 2 StPO und 152 Abs. 1 GVG stufen die Anordnungskompetenz, so dass vorrangig die Staatsanwaltschaft zur Entscheidung berufen ist [276].

Die Polizei hat das Recht zum ersten Zugriff (§ 163 Abs. 1 StPO) und muss dann ohne Verzug ihre "Verhandlungen" der Staatsanwaltschaft übersenden (§ 163 Abs. 2 S. 1 StPO). Im Massengeschäft führt die Polizei in aller Regel zunächst die Ermittlungen zu Ende, bevor sie die Vorgänge an die Staatsanwaltschaft abgibt.

Das Weisungsrecht der Staatsanwaltschaft ist ein institutionelles und kein persönliches. Die Polizeibehörde als solche muss die Aufträge der Staatsanwaltschaft ausführen. Die innere Organisation de Polizei bleibt davon unberührt. Sie entscheidet darüber, welcher Beamte eingesetzt wird.

A.3 Verfahren der Strafrechtspflege

Die Staatsanwaltschaft ist die leitende Behörde im Ermittlungsverfahren (§ 160 Abs. 1 StPO), die Anklagebehörde (§ 152 Abs. 1 StPO) und notwendiger Beteiligter an der gerichtlichen Verhandlung (siehe nur § 226 Abs. 1 StPO) sowie schließlich Vollstreckungsbehörde (§ 451 Abs. 1 StPO). Außerdem ist sie dem gerichtlichen Verfahren bei Ordnungswidrigkeiten vorgeschaltet (§ 69 Abs. 3 OWiG) und den Steuerstrafverfahren, soweit sie von der Finanzverwaltung selber betrieben werden (§ 406 AO).

Für die Vorermittlungen muss ein Anlass bestehen. Er verlangt nach Tatsachen (Merkwürdigkeiten [277]), die eine harmlose Erklärung haben oder auf eine Straftat schließen lassen können. Beispiele dafür sind die ungeklärte Todesursache einer Leiche, der Ausbruch eines Brandes, die Eröffnung eines Insolvenzverfahrens oder Fische, die bäuchlings auf einem Teich treiben. Die weiteren Ermittlungen dienen der Ursachenerforschung.

Ist danach eine Straftat die überwiegend wahrscheinliche Ursache, dann beginnt das Stadium des Anfangsverdachts und des vom Legalitätsprinzip geforderten Ermittlungsverfahrens. Besonders stark in Persönlichkeitsrechte eingreifende Ermittlungshandlungen erfordern deshalb nach Maßgabe der Verhältnismäßigkeit in aller Regel nicht nur nach einer gewissen Schwere der Kriminalität, sondern auch nach einem verdichteten, also durch Tatsachen untermauerten Anfangsverdacht.

A.3.1 Vorfeldermittlungen

Vorfeldermittlungen (Initiativermittlungen) erfolgen ohne ausdrücklichen Anlass. Sie dienen zur verfahrensübergreifenden Auswertung von Erkenntnissen im Interesse der polizeilichen Prävention und zur Eingrenzung noch unbekannter Kriminalitätsfelder. So ermächtigt zum Beispiel Nr. 4.5 der Anlage E zur RiStBV die Staatsanwaltschaft und die Polizei wegen der Organisierten Kriminalität ausdrücklich zu Ermittlungen, um die Frage zu klären, ob ein Anfangsverdacht besteht.

Während der Vorfeldermittlungen dürfen keine besonderen Eingriffsbefugnisse der StPO angewandt, sondern nur eigene Vorgänge, öffentliche Informationen und im Wege der Amtshilfe erlangte Erkenntnisse verwertet werden.

A.3.2 Vorermittlungen

Vorermittlungen sind hingegen anlassbezogen und dienen der Frage, ob eine Straftat begangen wurde. Im Zusammenhang mit Leichensachen werden Vorermittlungen von der StPO ausdrücklich verlangt und geregelt.

---

[276] Diese Handhabung wird mit einem gewissen Recht seit Jahrzehnten von den Rechtswissenschaften kritisiert. Unter verfahrensökonomischen Gesichtspunkten wäre es jedoch eine reine Förmelei, wenn wegen aller einfach gelagerten Ermittlungsverfahren zunächst die Staatsanwaltschaft eingeschaltet würde, die nichts anderes machen könnte als die Akten für den Abschluss der Ermittlungen wieder zurück zu senden.

[277] Wegen der Einzelheiten siehe A.4 Eingriffsrechte während der Vorermittlungen.

Vorermittlungen bei Leichensachen

Wenn Anhaltspunkte für einen nicht natürlichen Tod bestehen oder wenn die Identität einer gefundenen Leiche unbekannt ist, muss die Staatsanwaltschaft unterrichtet werden (§ 159 Abs. 1 StPO). Nur sie darf die Leiche zur Bestattung freigeben (§ 159 Abs. 2 StPO).

Die StPO regelt das weitere Vorgehen:

Leichenschau - § 87 Abs. 1 StPO

Ausgrabung - § 87 Abs. 3, 4 StPO

Identitätsfeststellung - § 88 Abs. 1 StPO

Entnahme von Körperzellen - § 88 Abs. 1 S. 2 StPO

Leichenöffnung - § 87 Abs. 2 StPO

... durch zwei Ärzte - § 87 Abs. 2 StPO

Kopf-, Brust- und Bauchhöhle - § 89 StPO

neugeborenes Kind - § 90 StPO

Verdacht einer Vergiftung - § 91 StPO

In diesem Zusammenhang spreche ich von Merkwürdigkeiten. Dabei handelt es sich um tatsächliche Anhaltspunkte im Sinne von § 152 Abs. 2 StPO, die harmlose Erklärungen haben, aber auch die Folge einer Straftat sein können. Die StPO lässt dafür einige elementare Ermittlungshandlungen zu [278].

A.3.4 unbekannte Täter

Sobald feststeht, dass eine Straftat begangen wurde, beginnt das vom Legalitätsprinzip bestimmte Ermittlungsverfahren. Es richtet sich auch gegen nicht identifizierte und namhaft gemachte Täter (sog. UJs-Verfahren). Es dient zunächst zu ihrer Identifizierung.

A.3.5 bekannte Täter

Erst nach bekannten Tätern kann gefahndet und gegen sie Anklage erhoben werden. Mit der Anklage endet das Ermittlungsverfahren (§ 169a StPO).

Das gerichtliche Verfahren kennt vor allem das Zwischenverfahren nach der Anklageerhebung (§§ 199 ff. StPO) und das gerichtliche Verfahren selber, die Hauptverhandlung (§§ 226 ff. StPO). Im Einzelfall können Rechtsmittelverfahren anschließen (§§ 296 ff. StPO; Beschwerde: §§ 304 ff. StPO, Berufung: §§ 312 ff. StPO, Revision: §§ 333 ff. StPO).

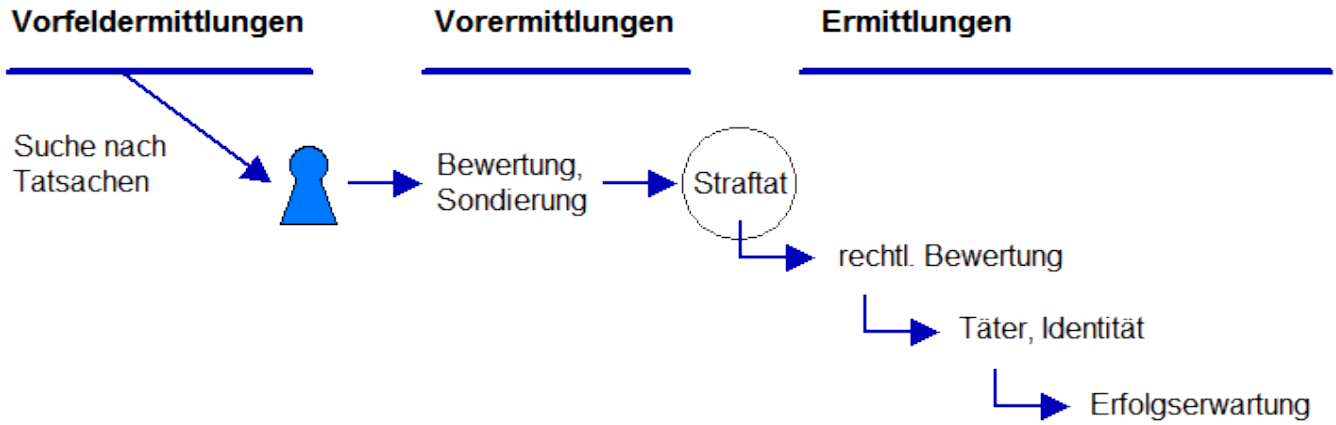
Nach rechtskräftiger Verurteilung folgt das Vollstreckungsverfahren (§ 449 StPO).

Für den Strafvollzug, also die tatsächliche Vollstreckung von Freiheitsstrafe, gilt Landesrecht. Die Vollstreckungsbehörde regelt nur ihren äußeren Rahmen wie die Zuführung, Strafzeitberechnung oder den Strafaufschub (§ 456 StPO).

Die inneren Vollzugsabläufe obliegen den Justizvollzugsanstalten selber.

[278] Nach der Aktenordnung handelt es sich um AR-Verfahren (Allgemeine Rechtssachen).

Kochheim, Verdeckte Ermittlungen im Internet, S. 56



A.4 Eingriffsrechte während der Vorermittlungen [279]

§ 152 Abs. 2 StPO enthält zwei das Ermittlungsverfahren bestimmende Aussagen. Das ist zum Einen das ***Legalitätsprinzip***, das die Staatsanwaltschaft zum Einschreiten gegen Straftaten verpflichtet, wenn nicht im Besonderen Einschränkungen und Ausnahmen bestimmt sind. Die zweite wichtige Aussage ist die, dass eine Straftat nur dann zu verfolgen ist, wenn hinreichende ***Tatsachen*** vorliegen, die sie begründen.

Nicht jede Tatsache für sich alleine begründet einen Verdacht, sondern erst ihre fachliche und rechtliche Bewertung und das auch nur beim Zusammenspiel von verschiedenen Tatsachen und gesicherten Erfahrungssätzen. Die Rechtsprechung und die Literatur erkennen deshalb eine dem Ermittlungsverfahren vorgelagerte Phase der ***Vorermittlungen*** an. Sie dient der Staatsanwaltschaft und der Polizei zur Sondierung, das heißt zur Sammlung von Spuren, Beweismitteln und mündlichen Aussagen, die ein vorläufiges Gesamtbild vom Geschehen, seinen Beteiligten (Täter, Opfer, Zeugen) und zur rechtlichen Einordnung geben. Die Pflicht zum Einschreiten gemäß § 152 Abs. 2 StPO beginnt dann, wenn die Tatsachen dafür sprechen, dass eine Straftat geschehen ist. Die Identität der Beteiligten und der genaue Ablauf des Geschehens muss dazu noch längst nicht feststehen.

Die wesentliche Frage, die sich bei den Vorermittlungen stellt, ist die nach den Zwangsmaßnahmen, die während der Sondierung angeordnet werden dürfen. Sie stellt sich besonders dann, wenn es die Tatsachen unklar lassen, ob eine Straftat vorliegt oder einen in strafrechtlicher Hinsicht harmlosen Grund haben. Das kann bei einem Verkehrsunfall ebenso der Fall sein wie beim Fund einer Leiche oder bei den Ermittlungen über Brandursachen. Immer stellt sich dabei die Frage, ob Personen oder Sachen durchsucht, Gegenstände beschlagnahmt oder Personen auch festgenommen werden dürfen.

Eine herrschende Linie gibt es in der Rechtsprechung und der Literatur dazu nicht. Das liegt unter anderem daran, dass die Strafprozessordnung keine klare Aussage dazu trifft, ob die Untersuchung, von der § 94 Abs. 1 StPO spricht, auch die Vorermittlungen umfasst oder nicht.

Aus verschiedenen gesetzlichen Pflichten und dem Wortlaut besondere Einzelfälle regelnder Paragraphen lässt sich jedoch ableiten, dass bereits während der Vorermittlungen eine Beweissicherungspflicht besteht, die von strafverfahrensrechtlichen Eingriffsrechten begleitet werden. Sie lassen den Schluss zu, dass die Vorermittlungen ein Teil der strafrechtlichen Untersuchung sind, in denen einzelne Eingriffsmaßnahmen zulässig sind, wenn der Gesetzgeber keine weiteren Handlungsschranken gesetzt hat.

---

[279] Ersterscheinung: **CF**, Eingriffsrechte während der Vorermittlungen, 12.08.2009

A.4.1 Vorermittlungen nach der StPO

Vorermittlungen sind davon geprägt, dass bereits "ungewöhnliche" Tatsachen bekannt sind (Merkwürdigkeit), die nach der kriminalistischen Erfahrung eine Straftat vermuten lassen und deshalb zur Erforschung der Ursachen zwingen.

Solche Ursachenermittlungen sind der Strafprozessordnung nicht fremd, wie einige Kommentatoren zu Unrecht meinen [280]. Im Zusammenhang mit Leichenfunden enthält die StPO detaillierte Regeln und strukturiert damit diesen Sonderfall der Vorermittlungen.

Daran schließt sich der BGH an, der die Auffassung vertritt, "Leichensachen" gemäß §§ 159, 87 StPO seien keine Ermittlungsverfahren [281]. Das betrachtet er jedoch aus einer besonderen Sicht, nämlich nach dem Maßstab des § 22 Nr. 4. StPO, wonach der Richter dann sein Amt nicht ausüben kann, wenn er bereits in der Sache als Staatsanwalt tätig gewesen ist. "Ermittlungsverfahren" und "Untersuchung" im Sinne von § 94 Abs. 1 StPO sind hingegen keine deckungsgleichen Begriffe. Der Begriff des Ermittlungsverfahrens ist geprägt von § 152 Abs. 2 StPO und setzt voraus, dass die Staatsanwaltschaft davon überzeugt ist, dass eine Straftat begangen wurde. Genau das steht während der Vorermittlungen noch nicht fest.

Um aus den Vorermittlungen zum Ermittlungsverfahren überzuleiten, bedarf es nach herrschender Meinung eines Willensaktes der zuständigen Strafverfolgungsbehörde, der erst möglich ist, wenn sie davon überzeugt ist, dass eine Straftat begangen wurde.

A.4.2 Prävention und Vorfeld

Die Kriminalitätsvorbeugung (Prävention) ist eine polizeiliche Aufgabe. Davon macht die StPO einige Ausnahmen.

Der Erkennungsdienst wird von § 81b StPO nur knapp angesprochen und hat eine strafverfahrensrechtliche ("Durchführung des Strafverfahrens") und eine polizeiliche Ausrichtung ("Erkennungsdienst" im engeren Sinne), deren Einzelheiten in den Polizeigesetzen der Länder geregelt werden. Er umfasst vor allem Messungen am Körper (Größe, Armlänge usw.), die Erfassung von Merkmalen (Narben, fehlende Glieder), die Fertigung von Fotografien und die Abnahme von Fingerabdrücken [282].

Eine große Bedeutung hat die molekulargenetische Untersuchung erlangt (genetischer Fingerabdruck [283], § 81g StPO), die ausdrücklich zur Aufklärung künftiger Straftaten dient [284].

Polizei und Staatsanwaltschaft sind darüber hinaus zum Abgleich von Dateien befugt (§ 98c StPO), um Straftaten aufzuklären. Die sehr allgemein gehaltene Formulierung umfasst auch die Erkundung von Tat- und Täterzusammenhängen sowie von organisierten Strukturen, die noch im Vorfeld angesiedelt sind. Die Strafverfolgungsbehörden dürfen hierzu auch gemeinsame Datensammlungen erstellen (§§ 483 ff. StPO).

---

[280] z.B. Werner Beulke in LR, § 152 StPO, Rn. 33

[281] **BGH**, Urteil vom 02.12.2003 - 1 StR 102/03, Rn 20

[282] **CF**, biometrische Erkennungsverfahren, 01.02.2009

[283] **CF**, genetischer Fingerabdruck, 27.03.2009

[284] BVerfG zur eingehenden Prognosebegründung: **CF**, genetischer Fingerabdruck, 19.06.2009;

BVerfG, Beschluss vom 22.05.2009 - 2 BvR 287/09, 400/09

A.4.3 beobachtete Erscheinungsformen

Durch Verwaltungsvorschriften (MiZi, MiStra [285]) sind Gerichte, Verwaltungs- und Strafverfolgungsbehörden zur gegenseitigen Unterrichtung in bestimmten Fällen verpflichtet. Das gilt zum Beispiel wegen der Eidesstattlichen Versicherungen über die Vermögenslosigkeit von Privatpersonen und Firmen sowie über die Eröffnung von Insolvenzverfahren. In diesen Fällen prüft die Staatsanwaltschaft, ob ein Anfangsverdacht wegen Betrug (§ 263 StGB), Untreue (§ 266 StGB), Bankrott (§ 283 StGB) oder Verletzung der Insolvenzantragspflicht (§ 15a InsO) besteht, indem sie die gerichtlichen Vorgänge einsieht oder z.B. den Insolvenzverwalter wegen der Insolvenzgründe und den Zeitpunkt der Überschuldung oder Zahlungsunfähigkeit befragt. Dabei prüft sie auch, ob die Vorschriften über die Buchhaltung und die Termine für die Aufstellung von Jahresabschlüssen eingehalten wurden (§ 242 HGB, §§ 41, 42a GmbHG).

Ich rechne diese Prüfungsaufgaben den Vorermittlungen zu, weil sie anlassbezogen sind und der Anlass die tatsächlichen Anhaltspunkte für die Prüfung liefert.

A.4.4 Initiativermittlungen

Nr. 4.5 der Anlage E zu den RiStBV ermächtigt die Staatsanwaltschaft und die Polizei wegen der Organisierten Kriminalität ausdrücklich zu Ermittlungen, um die Frage zu klären, ob ein Anfangsverdacht besteht. Dazu darf die Staatsanwaltschaft die Ermittlungen gegen Nebentäter zurückstellen, um zunächst die Haupttäter zu identifizieren und ihre Beteiligung zu klären. Dabei handelt es sich um Vorfeld- und Vorermittlungen.

Die Ermächtigung zu Initiativermittlungen ist eine typische Ausformulierung des Verhältnismäßigkeitsgrundsatzes. Ihm liegt eine Güterabwägung zugrunde, die das Strafverfolgungsinteresse der Allgemeinheit nach qualitativen und quantitativen Gesichtspunkten trennt und der Ermittlungstiefe den vorübergehenden Vorzug gibt. Daraus ist kein Verzicht auf Strafverfolgung abzuleiten, sondern die Anweisung, die besonders gefährlichen Strukturen im Umfeld der schwersten Kriminalität aufzuklären. Dazu wird eine mildere Verfolgung der Nebentäter in Kauf genommen.

Die ausdrückliche Benennung der Organisierten Kriminalität bedeutet hingegen nicht, dass die Güterabwägung nicht auch für andere Kriminalitätsbereiche gilt. Je nach der Schwere der Kriminalität greifen auch dort die gleichen Grundsätze. Der populistische Merksatz, "die Kleinen bestraft man ...", gilt nach verfassungs- und strafverfahrensrechtlichen Grundsätzen eben nicht.

A.4.5 Ermächtigung zu Vorermittlungen

§ 160 Abs. 1 StPO verpflichtet die Staatsanwaltschaft zu Ermittlungen, sobald sie Kenntnis von einer Straftat erhält. Das heißt aber noch nicht, dass zu ihrer sicheren Überzeugung eine Straftat begangen wurde. In dieselbe Richtung geht § 160 Abs. 2, 2. Halbsatz StPO, der die Staatsanwaltschaft zur Erhebung und Sicherung der Beweise verpflichtet, deren Verlust zu besorgen ist. Beide Vorschriften verlangen nach staatsanwaltschaftlichen Handlungen im Zusammenhang mit Vorermittlungen. Dem schließt sich mit klaren Worten der § 163 StPO an. Er verpflichtet die Polizei zum ersten Zugriff. Sie hat *Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten*. § 163 Abs. 1 S. 2 StPO gibt den hier interessierenden Auftrag: Bei Gefahr in Verzug muss die Polizei alle Anordnungen treffen, zu denen sie befugt ist.

Diese Befugnisse richten sich nach dem Verdachtsgrad. Die Postbeschlagnahme darf sich nur gegen Beschuldigte richten (§ 99 StPO) und setzt voraus, dass tatsächliche Anhaltspunkte für eine Straftat bestehen. Dasselbe gilt für andere geheime Ermittlungen (§ 101 Abs. 1 StPO), nicht aber zum Beispiel für die Beschlagnahme (§ 94 Abs. 2 StPO) und die Durchsuchung beim unbeteiligten Dritten (§ 103 StPO).

---

[285] Mitteilungen in Zivilsachen – MiZi;
Mitteilungen in Strafsachen – MiStra.

Die Strafprozessordnung stammt aus 1877 und ist jetzt mehr als 130 Jahre alt. Ihre Grundstruktur und Gliederung ist noch immer dieselbe, wenn auch viele neue Bereiche eingeführt wurden, die der technischen und gesellschaftlichen Entwicklung geschuldet sind. Sie gehört zu den klassischen Bollwerken des Rechts, zu denen auch das Strafgesetzbuch, das Bürgerliche und Handelsgesetzbuch, die Zivilprozessordnung und nicht zuletzt das Gerichtsverfassungsgesetz gehören. Alle übrigen Gesetzeswerke dürften jünger sein (vielleicht abgesehen vom Höferecht und anderen kleineren Exoten).

Sie ist kaiserlich und wilhelminisch geprägt. Sie weist den Polizeistaat in Grenzen, indem sie mit der Staatsanwaltschaft eine quasi-gerichtliche Behörde schafft, die eine Schimäre aus Verwaltungsbehörde und Gericht und gleichzeitig Vollstreckungsbehörde ist. Andere Rechtsordnungen haben diese Trennung nachhaltiger vollzogen, indem sie einen Ermittlungsrichter eingeführt (Frankreich) oder die Ermittlungskompetenz des Staatsanwalts begrenzt haben (Österreich). Ob sie damit mehr Rechtsstaat geschaffen haben, wage ich zu bezweifeln.

Für das Verständnis von den staatsanwaltschaftlichen und (ihnen folgend: polizeilichen) Eingriffsmaßnahmen ist diese geschichtliche Dimension hingegen wichtig: Dem klassischen Gesetzgeber ging es um die Schaffung eines Rechts, das im Zusammenhang mit der Kriminalität Rechtssicherheit schafft. Sie ist jedoch nicht allein durch die Verfolgung von Straftätern zu schaffen, sondern muss auch in das Vorfeld greifen.

Die meisten der hier aufgeführten Vorschriften sind bereits in der Urfassung der StPO enthalten gewesen und spiegeln ihre Ausrichtung wider. Sie kennzeichnen noch eine Gemengelage von polizeilichen Erkundigungen und gradliniger Strafverfolgung.

Diese Ausrichtung hat der aktuelle Gesetzgeber nicht ernsthaft in Frage gestellt. Er hat klarere Vorstellungen davon, was Polizei- und was Strafverfahrensrecht ist, und hat das Ermittlungsrecht mit

Das Tatbestandsmerkmal "bestimmte Tatsachen" in § 100a Satz 2 StPO erfordert, dass die Verdachtsgründe über vage Anhaltspunkte und bloße Vermutungen hinausreichen müssen. Bloßes Gerede, nicht überprüfte Gerüchte und Vermutungen reichen nicht. Erforderlich ist, dass auf Grund der Lebenserfahrung oder der kriminalistischen Erfahrung fallbezogen aus Zeugenaussagen, Observationen oder anderen sachlichen Beweisanzeichen auf die Eigenschaft als Nachrichtenmittler geschlossen werden kann.

BVerfG, Beschluss vom 30.04.2007 - 2 BvR 2151/06

Einzelregeln angereichert, die auf qualifizierte Verdachtsstufen aufbauen. Den arrondierenden Bereich zwischen beiden (man nennt das heute Schnittstelle) hat er jedoch unangetastet gelassen.

Die Ermächtigung zu Initiativermittlungen ist klaren Schranken unterworfen. Gegen konkret bevorstehende Straftaten von Bedeutung muss die Staatsanwaltschaft einschreiten, sobald sie von ihnen Kenntnis erlangt. Das gilt besonders dann, wenn das Leben, die Gesundheit oder andere wichtige Rechte der Betroffenen gefährdet sind.

Problematisch sind die Grenzfälle, in denen zum Beispiel nach Serientätern gefahndet wird und sich die Frage stellt, ob sie bei einer Tat festgenommen oder nur beobachtet werden sollen, um ihre Mittäter, Hehler oder Beutelager zu identifizieren. Dabei sind die Schwere der Tat und die zu befürchtenden Verletzungen von Freiheitsrechten zu berücksichtigen.

Drohen Gefahr für Leib oder Leben oder für erhebliche Vermögenswerte, dann kann sich das Ermessen auf "Null" reduzieren.

Anders sieht das aus bei von der Polizei beobachteten Kurierfahrten im Zusammenhang mit Betäubungsmitteln oder Waffen, bei der ("ungefährlichen") Schleusung von Ausländern oder bei dem kontrollierten Abtransport von Diebstahlsbeute. Droht deren Verlust, zum Beispiel bei einem Grenzübertritt, so ist in aller Regel der Zugriff erforderlich.

Stufen der Verdachtsprüfung

1 **tatsächliche Anhaltspunkte**
Fakten, Fakten, Fakten

2 **Inhalt ihrer Aussage**
wortgetreue und grammatische Beschreibung der Anhaltspunkte

3 **Geltungssicherheit, Absicherung**
Wiederholbarkeit, Häufigkeit, Seltenheit; Bewertung der Anhaltspunkte selber

4 **Zusammenwirken**
Schlussfolgerungen aus der Summe der Anhaltspunkte (Gesamtschau)

5 **Geltungssicherheit, Absicherung**
Bewertung des Zusammenwirkens der Fakten

A.4.6 Merkwürdigkeiten

Um eine Ausuferung von Eingriffsrechten im Stadium der Vorermittlungen zu vermeiden, bedarf es einer genauen Definition, die sich an § 160 Abs. 1 StPO orientiert: Staatsanwaltschaft und Polizei sind zur Handlung und Prüfung nach Maßgabe des Werkzeugs, das die StPO zur Verfügung stellt, und des Verhältnismäßigkeitsgrundsatzes verpflichtet, sobald sie Kenntnis von der Möglichkeit einer Straftat erhalten. Die Quelle ihrer Kenntnis ist dabei egal. Es kann sich gleichermaßen um die Empörung eines Bürgers (Strafanzeige), die Beobachtungen von Streifenpolizisten, öffentliche Anschläge (Presse, Internet) oder ihre Kenntnisse aus anderen Vorgängen handeln.

Das begrenzende sachliche Kriterium ist das, was ich als Merkwürdigkeit bezeichne: "Merkwürdig" sind Vorgänge, die von der Alltagserfahrung abweichen und naturgesetzlich eher unwahrscheinlich sind. Sie können sich durch eine Leiche, bäuchlings auf Flüssen treibenden toten Fischen, verheerenden Bränden oder anderen Erscheinungen äußern, die ungewöhnlich sind, nicht zwingend auf eine Straftat schließen lassen und sie jedoch nahe legen.

Die Beispiele zeigen, dass die "Merkwürdigkeit" nur mit Tatsachen begründet werden kann, die eine Straftat als wahrscheinlich erscheinen lässt, ohne dass es sich um eine "überwiegende" Wahrscheinlichkeit handeln müsste. Alle weiteren Ermittlungshandlungen unterliegen dem Gebot der Verhältnismäßigkeit. Ein schwacher Verdacht rechtfertigt nur flache Eingriffsmaßnahmen und ein stärkerer entsprechend tiefere. Besonders tiefe Eingriffsmaßnahmen hat der Gesetzgeber im Einzelfall bestimmt und damit aus den Vorermittlungen ausgeschlossen.

Die Vorermittlungen finden im Übergangsbereich zwischen dem Polizei- und dem Strafverfahrensrecht statt. Sie rechtfertigen noch polizeirechtliche Maßnahmen, etwa zur Störerabwehr oder zur Eigentumssicherung, und schon strafprozessuale Maßnahmen, wenn sie zur Klärung einer möglichen Straftat dienen. Das gilt besonders für die Sicherstellung und Beschlagnahme von Beweismitteln. Sie lässt der Gesetzgeber bereits zu, wenn sie eine auch nur mögliche Beweisbedeutung haben (§ 94 Abs. 1 StPO).

A.4.7 Eingriffsrechte im Stadium der Vorermittlungen

Das Stadium der Vorermittlungen wird sachlich von der Merkwürdigkeit geprägt. Dieser von mir stammende und keineswegs Allgemeinüblichkeit beanspruchende Begriff verlangt nach einem Sachverhalt, der eine Straftat wahrscheinlich erscheinen lässt, ohne strafrechtlich harmlose Prozesse ausschließen zu können. Die §§ 160 und 163 StPO bestimmen bereits in diesem Stadium eine flache Handlungspflicht für die Staatsanwaltschaft und die Polizei, wobei der Gesetzgeber nur wenige Eingriffsmaßnahmen für dieses Stadium der Untersuchung eröffnet hat. Dazu gehören Anhörungen (163 Abs. 1 S. 2 StPO), förmliche Vernehmungen (§ 161 Abs. 1 StPO), behördliche Auskünfte (§ 161 Abs. 1 StPO), Beschlagnahmen (§§ 94, 95 StPO) und Durchsuchungen (§§ 102, 103 StPO).

Eine einsame Entscheidung ist die des LG Offenburg von 1993 [286]. Es hat die Ermittlungskompetenz der Staatsanwaltschaft im Stadium der Vorermittlungen anerkannt und eine richterliche Zeugenvernehmung angeordnet, bezieht sich jedoch

[286] LG Offenburg, Beschluss vom 25.05.1993 - Qs 41/93, NStZ 1993, 506.

nach meiner Auffassung zu sehr auf Meinungen in der Literatur, die prognostisch sein können, aber häufig wechselnden Moden unterliegen. Ich bevorzuge deshalb eine dogmatische Argumentation, die sich am Wortlaut und dem Zweck des Gesetzes orientiert.

A.4.8 Fazit

Das Legalitätsprinzip greift erst dann, wenn feststeht, dass eine Straftat begangen wurde. Die ersten, auch noch unsicheren sachlichen Anhaltspunkte für eine Straftat lassen eine Prüfungspflicht der Strafverfolgungsbehörden entstehen, die das Stadium der Vorermittlungen einleitet. Es rechtfertigt Eingriffsmaßnahmen nur in dem Maße, wie sie der Gesetzgeber ausdrücklich zugelassen hat. Daraus folgt, dass die Vorermittlungen zur Prüfung, ob eine Straftat vorliegt, ein vorgelagerter Bestandteil der strafrechtlichen Untersuchung sind, auf die § 94 Abs. 1 StPO Bezug nimmt.

Darin unterscheiden sich die Vorermittlungen von den Vorfeldermittlungen. Sie gründen auf Tatsachen und kriminalistischen Erfahrungen, die noch keine konkrete Straftat erkennen lassen. Für sie dürfen zwar alle Kenntnisse herangezogen werden, die die Strafverfolgungsbehörden haben, aber nur zur Bewertung und Analyse sozialer Prozesse. Daraus dürfen neue Verdächte abgeleitet und Eingriffsmaßnahmen begründet werden, wenn die Fakten Straftaten erkennen lassen.

Die Zulässigkeit der Eingriffsmaßnahme richtet sich hingegen danach, welchen Verdachtsgrad der Gesetzgeber als Schwelle bestimmt. Das kann dazu führen, dass die Grenzen zwischen Vorfeld- und Vorermittlungen sowie zu den Ermittlungen selber verschwimmen. Bestimmend sind jedoch die klaren Anweisungen des Gesetzgebers, unter welchen sachlichen Voraussetzungen er welche Eingriffsmaßnahmen zulässt.

A.5 Geltung von Beweisen und Erfahrungen [287]

Die Themen Beweise und Verdacht werden im Cyberfahnder immer wieder aufgegriffen, weil sie von zentraler Bedeutung für die Ermittlungsarbeit und das Strafverfahren sind.

In diesem Beitrag geht es um den Aussagewert von Beweisen, den ich als ***Geltung*** bezeichne, und den Erfahrungen, mit denen sie gewürdigt werden.

Die Grundlagen für die Beurteilung des Verdachts sind Tatsachen. Sie bedürfen einer fachkundigen Bewertung, in die einerseits die Glaubwürdigkeit der Quelle ebenso einfließt wie die Glaubhaftigkeit der Tatsache selber und andererseits das Allgemein- und Fachwissen des Beurteilers.

Kriminalistische Erfahrungen sind solche, die die Fachleute in der Strafverfolgung anhand vergleichbarer Situationen, des Täterverhaltens, der Interaktion von Personen und des Fachwissens aus Einzelfällen gewonnen haben. Je nach ihrem Erfahrungshorizont kann es aus tiefem technischen, naturwissenschaftlichen, medizinischen und psychologischen Wissen bestehen, das aus einer Mischung aus Alltagserfahrungen, professioneller Sensibilität und fachmännischer Beratung entstanden ist.

Kriminalistisches Wissen ersetzt kein handwerkliches oder akademisches Spezialwissen, wohl aber das Grundlagenwissen, das in sich wiederholenden Fällen immer wieder zugrunde liegt. Dazu gehören die normalen Naturgesetze ebenso wie die Wahrnehmungen im Alltagsleben, die eine überwiegende Wahrscheinlichkeit wegen ihrer Ursachen aufdrängen. Das können die individuellen Wirkungen bei Trunkenheit, Solidarisierungseffekte bei Menschengruppen, chemische und physikalische Prozesse im Zusammenhang mit Umwelt-

Geltungsgrad für Erfahrungswerte	
5	sichere Erkenntnis, für die keine Ausnahmen bekannt oder denkbar sind
4	sichere Erkenntnis, für die Ausnahmen bekannt oder denkbar sind
3	Erfahrung mit überwiegender Wahrscheinlichkeit
2	Erfahrung, die aus verschiedenen Einzelfällen gewonnen wurde
1	Erfahrung aus einem Einzelfall
0	ohne Bedeutung

delikten oder Brandsachen ebenso sein wie die schlichte Alltagserfahrung, ob der Fahrer nach einer Karambolage, bei der der Kotflügel seines Autos völlig versemmelt wurde, den Unfall bemerkt haben muss oder nicht.

Kriminalistische Erfahrungen und gerichtliches Wissen ersetzen die sachverständige Klärung von Standardfragen, die immer wieder auftauchen, längst geklärt sind und einen gewissen Grad an Langweiligkeit haben. Sie müssen nicht immer wieder neu entdeckt, sondern nur dann thematisiert werden, wenn es neue, eben noch nicht geklärte Aspekte und Besonderheiten gibt.

Sie stellen jedoch an die kriminalistisch gebildeten Fachleute die Anforderung, ihre Messlatte kritisch zu hinterfragen und zu überprüfen. Kriminalistische Erfahrungen dürfen nicht zu platten und unumstößlichen Vorurteilen werden.

---

[287] Ersterscheinung: **CF**, Geltung von Beweisen und Erfahrungen, 29.11.2009. Auf die Erörterung der kriminalistischen Erfahrungen im Zusammenhang mit dem Skimming wird an dieser Stelle verzichtet: **CF**,Erfahrungswerte wegen des Skimmings, 29.11.2009.

> *Für die Feststellung von inneren Tatsachen genügt nämlich, dass ein nach der Lebenserfahrung ausreichendes Maß an Sicherheit besteht, an dem vernünftige Zweifel nicht aufkommen können. Außer Betracht zu bleiben haben solche Zweifel, die keinen realen Anknüpfungspunkt haben, sondern sich auf die Annahme einer bloß abstrakt-theoretischen Möglichkeit gründen …*
>
> BGH, Urteil vom 15. 11. 2001 - 1 StR 185/01, Rn. 78

A.5.1 Geltung

Die Bewertung von einzelnen Tatsachen orientiert sich zunächst an ihrem individuellen Aussagewert.

So sagen Funkzellendaten zunächst nichts anderes aus, als dass sich die SIM-Karte mit der betreffenden Anschlusskennung zu einem bestimmten Zeitpunkt irgendwo in dieser Funkzelle befunden hat. Sie sagen nichts darüber aus, wer das Mobiltelefon getragen hat, und lassen offen, ob es die Anschlusskennung noch ein weiteres Mal gibt.

Die Frage nach der mehrfachen Anschlusskennung lässt sich verhältnismäßig einfach klären. Die IMSI ist einmalig und wenn sie mehrfach vorkommen sollte (es gibt selten mehrere Karten, die gleichzeitig angesprochen werden), dann lassen sich die weiteren Umstände recht einfach klären.

Komplizierter ist die Frage danach, wer das betreffende Handy getragen hat. Hat derselbe Mensch das Telefon erfahrungsgemäß immer selber genutzt, dann ist es sehr unwahrscheinlich, dass es im entscheidenden Fall ein Anderer war. Dasselbe gilt, wenn im Zusammenhang mit gleichartigen Straftaten immer wieder dieselbe Anschluss- oder Zielnummer auftaucht. Das rechtfertigt die Annahme, dass dieselben Personen auftreten, die jedoch ständig kritisch überprüft werden muss.

Die grundsätzlich offene Frage danach, wer mit Funkzellendaten in Verbindung gebracht werden kann, lässt sich also nur bei der Betrachtung der Rahmenbedingungen klären - oder auch nicht.

Ich habe mir angewöhnt, die Frage nach der Aussagebedeutung von Tatsachen als Geltung zu bezeichnen.

Damit gibt es eine Geltung, die der Tatsache selbst innewohnt, und eine höhere Geltung, die sie im Zusammenspiel mit anderen Tatsachen erlangt, die sie bestätigen. Umgekehrt können diese anderen Tatsachen ihre Geltung auch wieder entkräften.

Der Sinn dieser Betrachtung ist ein ganz einfacher: Die Suche nach der "Wahrheit" ist ein Prozess [288], der zunächst nach Fakten fragt, die wegen ihrer Aussage im Einzelnen und dann in der Gesamtschau bewertet werden müssen. Die Erkennung einer "absoluten Wahrheit" ist nur bei ganz einfachen Sachverhalten möglich. Der Vorgang, "Apfel fällt vom Baum", ist die Wirkung eines Naturgesetzes. Der nähere Grund dafür - Reife, Wurmstichigkeit oder äußere Beeinflussung - ist eine Frage, die anhand weiterer Tatsachen geklärt werden muss. Wenn die Zeit der Apfelernte ist und auch andere Äpfel vom Baum fallen, zudem der betrachtete Apfel keine äußeren Verletzungen und im Innern keine Würmer hat, dann dürfte seine Reife als Grund für seine Lösung vom Baum feststehen.

Alle weniger einfachen Sachverhalte verlangen danach, dass alternative Ursachen nach Wahrscheinlichkeitsgesichtspunkten ausgeschlossen werden. Der deus ex machina der griechischen Tragödie, esoterische Fernwirkungen oder geisterhafte Protagonisten haben dabei keinen Platz.

---

[288] Siehe auch: **BGH**, Beschluss vom 18.01.2011 – 1 StR 663/10, Rn 22.

Kann der Tatrichter die erforderliche Gewißheit nicht gewinnen und zieht er die hiernach gebotene Konsequenz ..., so hat das Revisionsgericht dies zwar regelmäßig hinzunehmen. Die Beweiswürdigung ist Sache des Tatrichters; es kommt nicht darauf an, ob das Revisionsgericht angefallene Erkenntnisse anders gewürdigt oder Zweifel überwunden hätte. Daran ändert sich auch nicht allein dadurch etwas, daß eine vom Tatrichter getroffene Feststellung 'lebensfremd erscheinen' ... mag (...). Es gibt nämlich im Strafprozeß keinen Beweis des ersten Anscheins, der nicht auf Gewißheit, sondern auf der Wahrscheinlichkeit eines Geschehensablaufs beruht (...). Eine Beweiswürdigung ist demgegenüber etwa dann rechtsfehlerhaft, wenn sie lückenhaft ist, namentlich wesentliche Feststellungen nicht erörtert, widersprüchlich oder unklar ist, gegen Gesetze der Logik oder gesicherte Erfahrungssätze verstößt oder wenn an die zur Verurteilung erforderliche Gewißheit überspannte Anforderungen gestellt sind (st. Rspr. ...). Dies ist auch dann der Fall, wenn eine nach den Feststellungen naheliegende Schlußfolgerung nicht gezogen ist, ohne daß konkrete Gründe angeführt sind, die dieses Ergebnis stützen können ...

BGH, Urteil vom 14.09.2004 - 1 StR 180/04

A.5.2 Geltung und Wechselwirkungen

Der Beweiswert, also mit meinen Worten die Geltung von Beweisen, wird in der Rechtsprechung vielfach angesprochen. Mehrere Beispiele zeigen die Probleme im Einzelfall.

Der Beweisführung mit dem genetischen Fingerabdruck liegt eine statistische Methode zugrunde mit der Aussage, dass die gleichen biochemischen Eigenschaften einer Probe mit einer bestimmten Wahrscheinlichkeit bei verschiedenen Menschen desselben Geschlechts auftreten. Im Frühstadium der forensischen Verwertung der DNA-Analyse bewegte sich die statistische Genauigkeit in einem Bereich von 1 : 10.000. Das bedeutete, dass in einem großstädtischen Umfeld Hundert oder mehr Personen desselben Geschlechts über dieselben DNA-Merkmale verfügen konnten. Erst nachdem die biochemischen und statistischen Methoden verfeinert und verbessert wurden und die Wahrscheinlichkeitsaussagen im Bereich von 1 : 1 Mio. (und größer) liegen, erkennt der BGH die DNA-Spur als Vollbeweis an [289]- nicht ohne zu mahnen, dass das Gericht den Zusammenhang zwischen der Spur und der Tat genau betrachten muss. Das Beispiel zeigt, wie sich die Geltung von Beweisen durch die Verbesserung der Kriminaltechnik verbessern kann.

1995 hat das BVerfG im Anschluss an seine ständige Rechtsprechung über den Zeugen vom Hörensagen ausgeführt, dass seine Bekundungen besonders sorgfältig zu prüfen und dann nicht zur Verurteilung geeignet sind, wenn sie nicht durch weitere Beweise und Spuren bestätigt werden [290].

Dahinter steckt derselbe Grundgedanke. Die zum Zeugenbeweis entwickelten Grundsätze zur persönlichen Glaubwürdigkeit einer Auskunftsperson und zur inhaltlichen Glaubhaftigkeit lassen sich nur auf die Auskunftsperson selber anwenden. Der Zeuge vom Hörensagen berichtet zwar auch über seine Wahrnehmungen, also über das, was ihm gesagt worden ist, hat jedoch keine Wahrnehmungen vom Grundgeschehen selber. Das ihm Gesagte kann ebenso gut gelogen und übertrieben sein. Die Geltung des Gesagten ist umso geringer, je weniger sich das Gericht und die anderen Gerichtspersonen einen Eindruck von der Person verschaffen können, die vom Grundgeschehen aus eigener Wahrnehmung berichtet haben soll.

Der BGH hat deshalb zurecht zur Vorsicht gemahnt, wenn es um "gehörtes Hörensagen" [291] geht. Die dadurch gewonnenen Kenntnisse sind der Beweisführung nicht völlig entzogen, müssen jedoch besonders kritisch gewürdigt und beim leisen Zweifel verworfen werden [292].

Bei den Opfern von Posttraumatischen Belas-

---

289 **BGH**, Beschluss vom 21.01.2009 - 1 StR 722/08

290 BVerfG, Beschluss vom 19.07.1995 - 2 BvR 1142/93, abgedruckt bei Jens Ph. **Wilhelm**, Entscheidungssammlung zum Strafverfahrensrecht, Stand Dezember 2003, S. 18, 19

291 **CF**, gehörtes Hörensagen und gesperrte Beweise, 08.08.2009

292 **BGH**, Urteil vom 07.02.2008 - 4 StR 502/07

tungsstörungen [293] können sich ihre Erinnerungsbilder verzerren, so dass sie nicht in der Lage sind, die räumliche und zeitliche Abfolge ihrer Erinnerungen zu differenzieren. Dafür tragen sie keine Schuld, sondern ihre Krankheit ist dafür verantwortlich. Die Würdigung ihrer Aussagen kann nur mit Bedacht und unter Abgleich mit anderen Spuren und Fakten mit der für eine Verurteilung gebotenen Sicherheit erfolgen [294]. Hinzu kommt, dass PTB-Opfer nicht allein deshalb die besseren Menschen sind: Sie können auch lügen [295].

A.5.3 Kategorisierung des Geltungsgrades

Die Bewertung der Geltung von Erfahrungssätzen und von Beweisen beruht auf Erfahrungswissen und entzieht sich einer strengen, quasi naturwissenschaftlichen Skalierung. Mit gehörigen Vorbehalten lassen sich grobe Kriterien als Qualitätsmaßstab und Stufung entwickeln.

Die hier vorgestellte Skalierung soll Anhaltspunkte für die Qualität von Beweismitteln und Erfahrungen liefern. Ihre Eignung muss sie erst noch beweisen.

Ich gehe von einer fünfstufigen Skala aus (siehe Kasten oben), deren höchste Stufe mit der Ziffer 5 einer naturgesetzlichen Gewissheit gleicht.

Die Geltung mit der Stufe 4 ist ebenfalls eine gesicherte Erkenntnis, für die jedoch entweder Ausnahmen bekannt oder jedenfalls denkbar sind. Sie muss im Hinblick auf ihre Ausnahmen geprüft werden, wobei ein Maßstab zu verlangen ist, der sich nicht mit allen Verästelungen befassen muss. Ein Beispiel dafür ist die Beweisführung mit DNA-Merkmalen nach Maßgabe der jüngsten Rechtsprechung (siehe oben).

Die Stufe 3 kennzeichnet eine überwiegende Wahrscheinlichkeit. Sie verlangt nach einer genauen Betrachtung der Umstände im Einzelfall und nach einer Auseinandersetzung mit der Bedeutung dieser Umstände.

Für die gerichtliche Überzeugungsbildung ist anerkannt, dass es solche Feststellungen treffen darf, die keinen vernünftigen Zweifeln unterliegen [296]. In ständiger Rechtsprechung sind dazu Grundsätze entwickelt worden, die der BGH 2004 erneut zusammen gefasst hat [297]. Diese Art der Auseinandersetzung ist die, die ich in Bezug auf die Stufen 3 und 4 meine, wobei mit dem BGH schließlich auch keine überzogenen Anforderungen an die Gewissheit gestellt werden dürfen.

Untermauerte Erfahrungswerte sehe ich in der Stufe 2 angesiedelt. Sie verlangen immer nach einer Bestätigung im Einzelfall, also nach begleitenden Beweisen, die sich gegenseitig bestätigen und keine Widersprüche zueinander aufweisen. Der Wert solcher Erfahrungswerte ist vergleichbar dem, der für die Aussagen eines Zeugen vom Hörensagen gilt.

Einfache Erfahrungswerte, die ich in der Stufe 1 ansiedele, können nur eine bestätigende Bedeutung haben oder als Hilfsargument verwendet werden. Sie haben eine nur schwache Bedeutung.

A.5.4 Bewertung von Beweisen und Erfahrungssätzen

Eine schematische und sklavische Bewertung in der hier vorgeschlagenen Art birgt die Gefahr eines scheinobjektiven und pseudowissenschaftlichen Herangehens, weil sie ein subjektiver Vorgang ist und bleibt und besonders stark von dem Erfahrungs- und Wissenshorizont des Bewertenden abhängt.

Die Geltungsskala ist bewusst so grob gestrickt, dass sie zu den von der Rechtsprechung in Einzelfällen entwickelten Grundsätzen zur Beweiswürdigung passt. Sie dient zur kritischen Reflexion in der Ermittlungspraxis, wenn man sie auf allge-

---

[293] **CF**, Posttraumatische Belastungsstörung, 20.02.2009

[294] Zu den Anforderungen an ein "aussagepsychologisches Gutachten": **BGH**, Urteil vom 30.07.1999 - 1 StR 618/98.

[295] Siehe auch: **CF**, Beweisführung, 31.01.2011,

[296] **BGH**, Urteil vom 15. 11. 2001 - 1 StR 185/01, Rn. 78

[297] **BGH**, Urteil vom 14.09.2004 - 1 StR 180/04

meine Aussagewerte beschränkt:

Erfahrungswerte mit naturgesetzlicher Ausschließlichkeit bedürfen keiner kritischen Hinterfragung. Sie sind Ausnahmen und dürfen keinen denklogischen Zweifeln unterliegen.

Je höher die Geltung ist, desto weniger muss die Erfahrungstatsache mit weiteren Tatsachen untermauert werden.

Je geringer die Geltung ist, desto mehr verlangt die Erfahrungstatsache der Untermauerung. Fehlt es daran, dann ist sie nur als Arbeitshypothese, nicht aber zur Begründung von Eingriffsmaßnahmen geeignet.

B. Hintergrund: Carding-Boards

Eine allgemein gehaltene Auseinandersetzung mit der „Cyberkriminalität“ haben unlängst Brodowski und Freiling vorgelegt [298]. Im Zusammenhang mit der Schattenwirtschaft nehmen sie auch knapp Stellung zum Phänomen „Carding“ <ebd. S. 70>, ohne aber auf Einzelheiten oder die Carding-Boards einzugehen. Zum Einstieg muss ich mich deshalb auf journalistische Quellen beziehen.

Einer der ersten Berichte über kriminelle Hackerforen im Internet stammt von Moritz Jäger aus dem Jahr 2006 [299]. Er berichtete von organisierten kriminellen Strukturen, die sich in der Hackerszene herausgebildet haben, ihren Onlinebörsen und Foren, in denen neben gestohlenen Daten nahezu alle illegalen Dienstleistungen zu bekommen sind: Gefälschte Zahlungskarten, die dazu nötige Hardware, sichere Konten für die Beute (Drops), Malware (einschließlich Support), Cracks (geknackte Sicherheitseinrichtungen und Kennwörter) und schließlich Botnetze [300]. Schon seinerzeit verdienten die Forenbetreiber daran, Treuhandaufträge für ihre Kunden durchzuführen, wobei zur Abwicklung das auf Edelmetallwerten beruhende Verrechnungssystem E-Gold besonders begehrt war [301]. Zur Nachwuchsförderung boten die Foren bereits Anleitungen an (Tutorials), in denen erfahrende Nutzer ihr Wissen weiter gaben. Die Verfasser steigerten damit ihre Bekanntheit und dokumentierten ihre Loyalität zur kriminellen Szene.

Die von Jäger beschriebenen Zustände haben sich seither verbreitet und weiter entwickelt. Im September 2009 haben Marc-Aurél Ester und Ralf Benzmüller [302] eine Studie veröffentlicht, die sich mit deutschsprachigen Foren beschäftigt und darunter das „Elite-Forum“ besonders beleuchtet hat. Ihr Fazit:

Wo früher Hacker damit geprahlt haben, dass sie sich mit gefälschten Daten einen kostenlosen Zugang zu einem der unzähligen Erotikangebote im Internet verschafft haben, so brüsten sie sich heute damit, wie viele Kreditkartendaten sie mit ihrem Botnetz bereits gestohlen haben. Bemerkenswert ist, dass sich diese Daten nun in klingende Münze verwandeln lassen. (S. 2)

Die Palette reicht von persönlichen Daten wie Name, Anschrift etc. über Bankverbindungen bis hin zu Datenbank-Dumps mit hunderten oder mehreren tausend User-Daten. Hinter dem Begriff Datenbank-Dumps verstecken sich Kopien der Datenbanken von Onlineshops oder auch von Foren, in denen die Benutzerdaten gespeichert sind. (S. 8)

Die Autoren haben neue Strukturen bei den Rogue-Providern erkannt [303], die sie Bulletproof Hoster nennen: Anbieter von „Bulletproof Hosting“ versorgen ihre Kunden mit einem Server-Standort, der sicher vor Zugriffen internationaler Ermittler ist. Die wohl bekanntesten Namen in diesem Geschäft sind das Russian Buiness Network (RBN) und der amerikanische Hoster McColo gewesen. (S. 10) Schließlich gehen die Autoren auf den Handel mit gefälschten Dokumenten (S. 13), das Einkaufen mit gefälschten oder ausgespähten Identitäten (Carding, S. 13), das Skimming und den anderen modernen Erscheinungsformen der Cybercrime ein.

Nachdem das Elite-Forum im Herbst 2009 von der Polizei geschlossen worden war haben Ester und Benzmüller im Frühjahr 2010 in einer zweiten Studie von den Veränderungen in der Szene berichtet

---

[298] Dominik **Brodowski**, Felix C. **Freiling**, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, Forschungsforum öffentliche Sicherheit 01.03.2011

[299] Moritz **Jäger**, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel 20.09.2006.

[300] **CF**, professionelle Einzeltäter, 05.10.2008

[301] **CF**, Verrechnungssysteme auf der Basis von Edelmetallen, 2007. E-Gold und andere Verrechnungssysteme auf der Basis von Edelmetallen sind inzwischen bedeutungslos und wurden von WebMoney und anderen „grauen“ Bezahlsystemen abgelöst: **CF**, graue Bezahlsysteme, 08.12.2010.

[302] Marc-Aurél **Ester**, Ralf **Benzmüller**, G Data Whitepaper 2009. Underground Economy, 19.08.2009

[303] Siehe: **CF**, Schurken-Provider und organisierte Cybercrime, 13.07.2008

[304]. Neben der üblichen Aufnahmegebühr für jedes Mitglied (zum Beispiel 10 € per PaySafeCard) konnten 2009 noch zwei verschiedene Arten von Verkaufslizenzen in den Boards erworben werden:

Monopollizenz (Patent); berechtigte zum exklusiven Verkauf einer Warengruppe (zum Beispiel gehackte Kreditkarten) und kostete mehrere Hundert Euro.

Shop-Lizenz; berechtigte zum Verkauf beliebiger Leistungen mit Ausnahme der Monopol-Dienste und war günstiger zu bekommen.

Seit 2010 gibt es nur noch normale Händlerlizenzen. Die so genannten Verkaufspatente wurden abgeschafft. Nun muss jeder Verkäufer einen Betrag zahlen, um die Verkaufsberechtigung zu erhalten. Das Prinzip spült Geld in die Board-Kasse und soll vor internen Scammern, Betrügern, schützen.

Daneben seien neue Webshops entstanden, schreiben die Autoren, und einige "etablierte" seien weiterhin tätig. Ihre Betreiber könnten die Betreiber der Boards selber oder jedenfalls in deren Umfeld angesiedelt sein.

Am Fall des „1337 Crew“ Forums haben viele Mitglieder im Untergrund erkannt, dass sie nicht so sicher sind, wie es wohl viele von ihnen gedacht hatten. Viele Onlinekriminelle haben sich auch aus dem Untergrund-Tagesgeschäft zurück gezogen, vielleicht nur temporär, um nicht „mit laufendem Rechner“ von der Polizei erwischt zu werden.

Eine der tiefsten Auseinandersetzungen mit der internationalen Cybercrime-Szene stammt von François Paget, dem Leiter der McAfee Labs in Frankreich [305], die ich mit eigenen Worten nacherzählt habe [306]. Er widmet sich besonders dem 2001 in Odessa gegründeten Carding-Board CarderPlanet <S. 7 f.> und berichtet über dessen diversen Nachfolgeveranstaltungen <S. 36>. Die Carding-Boards sind eine besondere Ausgestaltung der Hacker-Boards. „Carding“ bezeichnet den Umgang mit Kredit- und anderen Zahlungskarten, genauer: Den Diebstahl, den Handel und den Missbrauch von Kartendaten. In der Zeit nach 2001 entstanden vor allem in den USA andere Boards, in denen vermehrt auch gefälschte Personalpapiere und Universitätsabschlüsse angeboten wurden. Der „Datenhandel“ qualifizierte sich in der Zwischenzeit. Seit mehreren Jahren werden nicht nur einfache Kontozugangsdaten, sondern ganze Identitäten samt Ausweispapiere, persönlichen Vitae und mit den in den USA besonders wichtigen Sozialversicherungsnummern gehandelt. Die „1337 Crew“ und das heute noch aktive Board carders.cc [307] widmen sich hingegen der ganzen Palette krimineller Erscheinungsformen im Zusammenhang mit dem Internet, neben dem klassischen „Datenhandel“ besonders dem Verkauf von Malware und technischen Geräten zum Skimming, dem Vermieten von Botnetzen und geschütztem Speicherplatz [308] und Hilfen zur Beutesicherung. Das sind in erster Linie die Vermittlung von Finanz- und Warenagenten, unter falschen Identitäten eingerichtete Packstationen und der Transfer der inzwischen besonders favorisierten Zahlungsmittel, Spielkasinos im Internet und Verrechnungssysteme [309], also webmoney, PaysafeCard, ukash und schließlich Kreditkarten auf Guthabenbasis

---

[304] Marc-Aurél **Ester**, Ralf **Benzmüller**, Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data 22.04.2010

[305] François **Paget**, Cybercrime and Hacktivism, McAfee Labs 15.03.2010

[306] Dieter **Kochheim**, Cybercrime und politisch motiviertes Hacking. Über ein Whitepaper von François Paget von den McAfee Labs, 20.10.2010. Daraus entstand: Dieter **Kochheim**, Eine kurze Geschichte der Cybercrime, 03.11.2010.

[307] .cc ist das Namenskürzel für die Top Level Domain der Kokosinseln. Der Namensraum wird von einem Subunternehmen von VeriSign verwaltet (USA). Eine nationale Zuordnung lässt sich daraus nicht zwingend schließen.

[308] Dazu gehören die schon genannten Bulletproof Hoster, die ich Schurkenprovider nenne: **Kochheim**, Schurken-Provider und organisierte Cybercrime, 13.07.2008.
Siehe auch: **Kochheim**, Basar für tatgeneigte Täter, 11.04.2010 (Schurkenprovider).

[309] Siehe: **CF**, Graue Bezahlsysteme, 08.12.2010.

[310], mit denen sich die Beute am Geldautomaten an der nächsten Ecke erlösen lässt.

[310] **CF**, Kreditkarte auf Guthabenbasis, 17.08.2010.