Thomas J. Primig

Formalrechtliche Möglichkeiten und Grenzen nationaler Telekommunikationsüberwachung

Formalrechtliche Möglichkeiten und Grenzen nationaler Telekommunikationsüberwachung

Aufgrund der Tatsache, daß sich sowohl die Häufigkeit der im oder unter Zuhilfenahme des Internet begangenen Straftaten im Allgemeinen, als auch das Auftreten krimineller Verbindungen im Zusammenhang mit Formen moderner Kommunikation im Speziellen erhöht hat, ergeben sich für den Rechtsanwender grundlegende Probleme in der Auslegung österreichischen materiellen Rechts. Ungeachtet dessen, daß im Zusammenhang mit der Bekämpfung der Organisierten Kriminalität die Problemkreise rund um den „Lauschangriff" oder die „Rasterfahndung" - welche ja allesamt den Bestand moderner Technologien voraussetzen - ausführlich erörtert wurden, wurden Fälle einer sicherheitsbehördlichen oder strafgerichtlichen Erhebung im Internet, bzw der „Überwachung der Telekommunikation"[1], bis vor einiger Zeit kaum diskutiert,[2] obwohl mit der Novelle der StPO[3] - und damit auch der Bestimmungen der Fernmeldeüberwachung[4] - dieser Themenbereich endlich einer einheitlichen Regelung unterworfen werden soll. Vor allem in Hinblick auf die jüngeren Entwicklungen im Computer(straf-)recht auf europäischer[5], wie auch auf internationaler[6] Ebene geht es nicht an, daß der österreichische Gesetzgeber sich vor den Möglichkeiten, welche ein Medium wie das Internet auch der Strafverfolgung, insbesondere im Hinblick auf das Ermittlungsverfahren, bietet, verschließt. Welche Regelungen der österreichischen

---

[1] Mit der Reform der Bestimmungen über die Überwachung des Fernmeldeverkehrs durch das „Strafrechtsänderungsgesetz 2002" (BGBl I 134/2002) soll nicht nur eine Anpassung dieser Regelungen selbst an die Eigenheiten des Internet, sondern auch eine begriffliche Übernahme der Bestimmungen des Telekommunikationsgesetzes erfolgen.

[2] So *Wessely*, Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet, ÖJZ 1996, 612.

[3] Vgl dazu unten, 5.5.2.

[4] §§ 149a bis c StPO BGBl 631/1975.

[5] Siehe dazu beispielsweise die Entwicklungen in bezug auf die Erarbeitung der diversen „*Enfopol*" - Dokumente zur Regelung technischer Standards der Telekommunikationsüberwachung oder das Arbeitspapier „*eEurope 2002*" der Europäischen Kommission, wie auch die verschiedenen Materialien zur Erarbeitung eines „*Internet Action Plan*".

[6] Beispielsweise mit der „*Convention on Cyber-Crime*" in der endgültigen Fassung vom 23.11.2001.

(Straf-) Rechtsordnung dennoch brauchbare formellrechtliche Grundlagen für die Verfolgung von Delikten, die unter Zuhilfenahme moderner Formen der Telekommunikation begangen werden, darstellen, soll im Folgenden erörtert werden.

1. Allgemeines

Dabei sollen zuerst die allgemeinen Befugnisse der Sicherheitspolizei dargestellt und sodann auf Straftaten mit Internet-Bezug angewandt werden. Besondere Bedeutung kommt hierbei auch dem Problemkreis der Trennung sicherheitspolizeilicher Ermittlungshandlungen von jenen der Strafprozeßordnung zu. In diesem Zusammenhang wird auch die Thematik der „verdeckten Ermittlung“, sowie des „Lausch- und Spähangriffs“, welcher ja sowohl zu sicherheitspolizeilichen, als auch zu strafprozessualen Zwecken in bestimmten Fällen zulässig ist, einer näheren Betrachtung unterzogen. Auch auf die Bestimmungen zur sicherheitspolizeilichen Überwachung des Fernmelde- bzw Telekommunikationsverkehrs wird näher eingegangen und es werden jene im Lichte moderner Kommunikationsformen betrachtet.
Unter der Überschrift „Ermittlungsmaßnahmen im Bereich der StPO“ wird alsdann die Bestimmung des § 149d StPO diskutiert, insbesondere ob diese auch bei Ermittlungshandlungen in Datennetzen zur Anwendung kommen kann, das „Lauschen“ und „Spähen“ im Internet somit rechtlich zulässig und technisch durchführbar ist.
Als letzter großer Themenkreis werden schließlich die bestehenden Bestimmungen zur „Überwachung des Fernmeldeverkehrs“ erörtert, wobei der Problematik der Erfassung von Stamm- Vermittlungs- und Inhaltsdaten – auch unter dem Aspekt möglicher Grundrechtseingriffe – besonderes Augenmerk geschenkt wird. In diesem Zusammenhang werden auch die Bestimmungen der „Überwachungsverordnung“ vorgestellt und die Neuerungen, welche das „Strafrechtsänderungsgesetz 2002“ im Bereich der Telekommunikationsüberwachung bringt, angeführt.

2. Allgemeine Überlegungen zu sicherheitspolizeilichen und strafprozessualen Ermittlungshandlungen

Das Ringen um eine Definition der Begriffe „Organisiertes Verbrechen", „Kriminelle Organisation", „Kriminelle Verbindung" oder – neuerdings – der kriminellen Vereinigung und der terroristischen Vereinigung, scheint zwar mühsam und langwierig, ist aber zur Bestimmung der Anwendungsvoraussetzungen des „Lauschangriffs"[7], der „Rasterfahndung"[8] oder der Regelungen zur Überwachung des Fernmeldeverkehrs[9] - und damit auch der Überwachung von Datentransfers in Computernetzen und schließlich im Internet – unumgänglich.

Ein wirksames Vorgehen des Staates insbesondere gegen die Erscheinungsformen Organisierter Kriminalität erfordert weitreichende gesetzliche Ermächtigungen, die demselben ein beträchtliches Eingriffspotential in verfassungsgesetzlich gewährleistete Rechte des Betroffenen gewähren.[10] Ebenso verhält es sich bei allen sicherheitspolizeilichen und strafprozessualen Ermittlungsmaßnahmen, welche eine Abkehr von einer „offenen Verbrechensbekämpfung"[11] darstellen, da auch diese oftmals mit einem schwerwiegenden Eingriff in Persönlichkeitsrechte untrennbar verbunden sind. So verfolgen die Regelungen der optischen und akustischen Überwachung von Personen grundsätzlich das Ziel, ein zusätzliches (sachliches) Beweismittel zu erlangen, welches zwar unter Mitwirkung des Betroffenen, aber ohne sein Wissen zustande kommt.[12] Es beeinträchtigt beispielsweise ein Lauschangriff die Privatsphäre, vielleicht

---

[7] § 149d StPO (BGBl 631/1975 idF BGBl I 134/2002); § 54 SPG.

[8] § 149i StPO (BGBl 631/1975 idF BGBl I 134/2002).

[9] § 149a StPO.

[10] Vgl *Funk*, Sicherheitspolizeiliche Maßnahmen zur Bekämpfung Organisierter Kriminalität, JRP 1996, 27.

[11] Der ursprüngliche Geist der StPO war vom Grundgedanken einer offenen Strafverfolgung geprägt, da man damals gerade das andere Extrem des - gegenüber dem Betroffenen wie auch gegenüber der Öffentlichkeit - geheimen Inquisitionsprozesses, eingebettet in den Metternichschen Polizeistaat, überwunden hatte. So zeigt sich diese Offenheit gegenüber dem Beschuldigten zB in den Regelungen der §§ 200 und 202 StPO, als auch im Verbot des Einsatzes von „Lockspitzeln" nach § 25 StPO. Siehe dazu va *Schmoller*, Geändertes Erscheinungsbild staatlicher Verbrechensbekämpfung, ÖJZ 1996, 22 f.

[12] *Miklau/Pilnacek*, Optische und akustische Überwachungsmaßnahmen zur Bekämpfung schwerer Organisierter Kriminalität („Lauschangriff") – Paradigmenwechsel im Verfahrensrecht? JRP 1997, 291.

sogar den Intimbereich[13], das Recht am gesprochenen Wort[14], sowie uU das Hausrecht[15], während die Rasterfandung das Recht auf Datenschutz[16] bzw auf informationelle Selbstbestimmung[17] einschränkt. Dies gilt auch für jede rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr[18], beispielsweise in den Anwendungsfällen der „Fangschaltung“[19], wie auch für die Bestimmungen der Strafprozeßordnung zur Fernmelde- bzw Telekommunikationsüberwachung.[20]

Bei der Schaffung von Eingriffsbefugnissen durch den Staat muß also ein Ausgleich zwischen dem Recht auf Freiheit, welches einen Schutz der individuellen Freiheitssphäre bedingt (*status negativus*) und dem Recht auf Sicherheit im Sinne einer positiven Pflicht des Staates, Sicherheit zu gewährleisten (*status positivus*)[21] geschaffen werden. Es besteht also ein Spannungsverhältnis, weil der Staat nicht zugleich unbegrenzt Freiheit und Sicherheit garantieren kann.[22] Da die beiden Grundrechte einander bedingen, muß – um Freiheit zu ermöglichen – Sicherheit vorhanden sein.[23]

Weitgehend wird aber dahingehend argumentiert, daß Maßnahmen zur besseren Bekämpfung schwerer Kriminalität, wie der Einsatz technischer Mittel zur akustischen und optischen Personenüberwachung, die Rasterfahndung sowie der Ausbau der verdeckten Ermittlung dann rechtsstaatlich vertretbar sind[24], wenn den damit verbundenen Nachteilen und Gefahren hinreichend entgegengesteuert wird.[25]

---

[13] Art 8 EMRK.

[14] § 16 ABGB; vgl *Posch* in *Schwimann*, Praxiskommentar zum ABGB[2] (1997) § 16 RZ 26.

[15] Art 9 StGG; Art 8 EMRK.

[16] § 1 DSG 2000 BGBl I 165/1999.

[17] Vgl *Schmoller*, Geändertes Erscheinungsbild staatlicher Verbrechensbekämpfung, ÖJZ 1996, 22 f

[18] Zu dieser Problematik vgl unten, 5.5.1.1.

[19] § 100 TKG; vgl dazu ausführlich unten, 5.3.1.1.

[20] Siehe dazu „Die strafprozessuale Fernmelde- bzw Telekommunikationsüberwachung“, unten, 5.5.

[21] *Walter/Mayer*, Grundriß des österreichischen Bundesverfassungsrechts[9] (2000) RN 1325, 1327.

[22] Vgl *Aichinger*, Neue Fahndungsmethoden zur Bekämpfung organisierter Kriminalität (1997) 26.

[23] *Fuchs*, Grundsatzgedanken und Zweckrationalität in der aktuellen kriminalpolitischen Diskussion, FS *Platzgummer* (1995) 450.

[24] Vgl JAB 812 BlgNR 20. GP 2 f.

[25] *Schmoller*, Geändertes Erscheinungsbild staatlicher Verbrechensbekämpfung, ÖJZ 1996, 29; *Miklau/Pilnacek*, Optische und akustische Überwachungsmaßnahmen zur Bekämpfung schwerer Organisierter Kriminalität („Lauschangriff“) – Paradigmenwechsel im Verfahrensrecht? JRP 1997, 289.

Mit dem Beginn des Jahres 2002 wurden, im Zuge einer Novelle der Strafprozeßordnung[26], die Bestimmungen zur optischen und akustischen Überwachung von Personen ins Dauerrecht übernommen, was aber weniger daran liegt, daß sich diese Methoden in besonderer Weise bewährt hätten,[27] sondern daß sich „unter dem Eindruck der...Terroranschläge in den USA ein erhöhtes Sicherheitsbedürfnis eingestellt zu haben scheint."[28] In diesem Sinn hat auch der Rechtsschutzbeauftragte in seinen Bericht an den Bundesminister für Justiz hervorgehoben, daß besondere Ermittlungsmaßnahmen rechtmäßig und unter besonderer Beachtung des Verhältnismäßigkeits- und Subsidiaritätsgrundsatzes eingesetzt werden.

Weiters hat er seiner Einschätzung Ausdruck verliehen, daß die Voraussetzungen, die den Gesetzgeber zur Einführung besonderer Ermittlungsmaßnahmen veranlaßten, nämlich die Bedrohungen durch qualitativ neue Erscheinungsformen organisierten Verbrechens, nicht weggefallen sind.[29]

In Anbetracht des zuletzt im Sicherheitsbericht der Bundesregierung[30] dargestellten Erscheinungsbildes der organisierten Kriminalität und der dort getroffenen Feststellung, wonach Formen der Überwachung meist die einzigen Ermittlungsmethoden darstellen, um bei den polizeilichen Ermittlungen bis in die Leitungsebene einer OK-Organisation eindringen zu können, haben sich die Formen der akustischen und optischen Überwachung als effizientes und notwendiges Instrumentarium erwiesen, um diesen Formen der Kriminalität im Sinne der Schutzfunktion eines Rechtsstaates wirksam entgegentreten zu können.[31]

---

[26] Bundesgesetz, mit dem die Strafprozeßordnung 1975 und das Bundesgesetz BGBl I 105/1997 im Bereich besonderer Ermittlungsmaßnahmen geändert werden (Strafprozeßnovelle 2001) BGBl I 130/2001.

[27] Nur sieben Beschlüsse für einen „großen Lauschangriff" wurden bisher gefaßt, fünf davon durchgeführt (Quelle: *http://www.heise.de/tp/deutsch/inhalt/te/9806/1.html*); die EB zur RV der StPO-Novelle (EBRV 755 BlgNR 21. GP) sprechen hingegen, ohne die Angabe konkreter Zahlen, nur davon, daß „auf Grund des Berichts der Bundesminister für Justiz und für Inneres über die Erfahrungen mit der Anwendung, Durchführung und Kontrolle dieser besonderen Ermittlungsmaßnahmen...die genannten Bestimmungen mit 1.Jänner 2002 ohne weitere Befristung in den Rechtsbestand übernommen werden (sollen)".

[28] *Zarzer*, Österreich übernimmt Lauschangriff und Rasterfahndung ins Dauerrecht, Telepolis, das Magazin für Netzkultur vom 13.10.2001 unter *http://www.heise.de/tp/deutsch/inhalt/te/9806/1.html*.

[29] Siehe dazu auch die Gesamtberichte des Bundesministers für Justiz über den Einsatz besonderer Ermittlungsmaßnahmen in den Jahren 1998 und 1999, III-25 BlgNR 20. GP bzw III-64 BlgNR 21. GP.

[30] Bericht der Bundesregierung über die innere Sicherheit in Österreich (1999) 183.

[31] Vgl EBRV 755 BlgNR 21. GP 5.

Im Folgenden sollen nun die für elektronische Ermittlungsmaßnahmen, bzw Ermittlungen in elektronischen Medien, relevanten österreichischen Normen näher erörtert werden.

2.1. Zur „Doppelfunktionalität" sicherheitspolizeilicher Ermittlungsmaßnahmen

Die Sicherheitspolizei gehört zum Kernbereich der ordnend eingreifenden Verwaltung und ist den klassischen Ordnungsfunktionen des Staates zugeordnet.[32]
Durch die Doppelfunktion[33] der (Vollzugs-) Polizei als Zuständigkeitssubjekt sowohl der präventiven Gefahrenabwehr, wie auch der repressiven Strafverfolgung, ist schon grundsätzlich ein Problem angelegt, welches in seiner dogmatischen Tiefe und tatsächlichen Brisanz nicht weitgehend geklärt scheint.[34] So ist die Trennung von Gefahrenabwehr und Strafverfolgung mit kompetenzrechtlichen, grundrechtlichen und rechtspolitischen Gesichtspunkten in Beziehung zu setzen.[35]
Für die Zuständigkeit grundlegend ist somit die Frage, wann die Sicherheitsbehörden im Dienst der Gefahrenabwehr, und wann sie im Dienst der Strafverfolgung tätig werden müssen.[36] Zum einen geht es um eine effektivere nachträgliche Strafverfolgung und damit um Änderungen der StPO, zum anderen soll die Möglichkeit eines präventiven Einschreitens gegen geplante Straftaten verbessert und insoweit das SPG ergänzt werden. Grundsätzlich ist die Abgrenzung klar: Strafprozeßrecht ist das Recht der *Aburteilung* und *Aufklärung* begangener Straftaten, es ist somit *vergangenheitsgerichtet* und dient repressiven Zwecken, während das Polizeirecht als Recht der Gefahrenabwehr *zukunftsgerichtet* – also präventiv – wirkt.[37]

---

[32] *Funk*, Das neue Sicherheitspolizeirecht – Kodifikation und Reform einer klassischen Verwaltungsmaterie, JBl 1994, 137.

[33] Zu dieser Doppelfunktion ausführlich *Dearing*, Sicherheitspolizei und Strafrechtspflege, FS-*Platzgummer* (1995) 249 ff.

[34] *Schmidt-Jortzig*, Möglichkeiten einer Aussetzung des strafverfolgerischen Legalitätsprinzips bei der Polizei, NJW 1989, 129.

[35] Siehe dazu *Funk*, Das neue Sicherheitspolizeirecht, JBl 1994, 142.

[36] *Aichinger*, Fahndungsmethoden 32.

[37] Vgl *Wiederin*, Einführung in das Sicherheitspolizeirecht (1998) 68.

Gerade im Zusammenhang mit der Bekämpfung Organisierter Kriminalität kann es zu einer Überschneidung beider Bereiche kommen, weil die Strafverfolgung mit der Verhinderung künftiger strafbarer Handlungen, also einem präventiven Element, zusammentrifft.[38] Beide Rechtsbereiche verfolgen also mit manchen Bestimmungen Ziele, die in den jeweils anderen hineinragen.[39]

In der Praxis treten also Sachverhalte auf, in denen die Agenden der Sicherheitspolizei schwer von denen der Kriminalpolizei zu unterscheiden sind. Folgendes Beispiel soll dies verdeutlichen:

Im Zuge einer Routinekontrolle in einem Computerfachgeschäft wird beobachtet, wie zwei Angestellte plötzlich eine Computerfestplatte in ein Waschbecken werfen und versuchen, mit einem weiteren Datenträger die Flucht anzutreten Wie sich später herausstellt, befinden sich auf den Speichermedien kinderpornographische Materialen. Für das erste unmittelbare Einschreiten der Behörden, dh für die Sicherstellung der Beweismittel, ist die Rechtsgrundlage im SPG zu suchen, während die Einvernahme der Täter sowohl in den Kompetenzbereich der Sicherheitspolizei, als auch in jenen der Strafverfolgung fällt.

Auch ist beispielsweise das Sperren einer Newsgroup oder eines Chat-Rooms, wo offensichtlich gerade raubkopierte Software getauscht wird, Aufgabe der Sicherheitspolizei, während im Bereich der Festnahme und Einvernahme der Täter die Kriminalpolizei zuständig sein kann.[40]

Entscheidend für die Frage der Abgrenzung zwischen SPG und StPO ist die Unterscheidung zwischen dem Zeitraum *während* eines gefährlichen Angriffs und dem Zeitraum *nach* einem gefährlichen Angriff. § 16 (2) SPG definiert iVm Abs 3 den „gefährlichen Angriff". Ein solcher liegt demnach vor, wenn Rechtsgutbedrohungen durch Handlungen, die den Tatbestand einer der taxativ aufgezählten Straftaten verwirklichen, sowie diesbezügliche Vorbereitungshandlungen, soweit diese Handlungen nicht ausnahmsweise gerechtfertigt sind, immanent sind.[41] § 16 (2) SPG umschreibt das Stadium, welches im strafrechtlichen Sinn mit dem Versuch beginnt, während § 16 (3) SPG diesen Begriff in den Bereich der straflosen

---

[38] Vgl *Schmoller*, geändertes Erscheinungsbild staatlicher Verbrechensbekämpfung, ÖJZ 1996, 21.

[39] Vgl *Wiederin*, Sicherheitspolizeirecht 69.

[40] Siehe auch die Beispiele bei *Aichinger*, Der Lauschangriff für Sicherheits- und Kriminalpolizei, JAP 1996, 120.

[41] Vgl *Keplinger*, Handbuch zum Sicherheitspolizeigesetz (1993) 85.

Vorbereitungshandlungen, jedoch zeitlich so weit eingeschränkt, daß nach dem Täterplan die Verwirklichung des Tatbestandes demnächst einzutreten hat, ausdehnt. Ein „gefährlicher Angriff" umfaßt somit in einem dynamischen System den Zeitraum *vor* der ersten Tathandlung bis hin zur Vollendung.[42]

Wenn der gefährliche Angriff jedoch noch nicht vollendet ist, liegt eine Schnittstelle von sicherheitspolizeilichen und strafprozessualen Agenden vor, da durch ein und dieselbe Tätigkeit sowohl die Gefahr abgewendet wird, als auch Beweismittel zum Zwecke der Strafverfolgung sichergestellt werden.[43] Es kann nun argumentiert werden, daß für die Frage der Zuständigkeit maßgeblich ist, welchen „wirklichen Willen" zur Funktionserbringung die tätigwerdende Behörde selbst hatte und, wenn dieser nicht eindeutig erkenntlich ist, welches überwiegende Aussehen und Gewicht[44] der Polizeimaßnahme nach dem Gesamteindruck zukommt.[45] Es kann aber auch dem Sicherheitspolizeirecht pauschal Vorrang gegenüber der StPO eingeräumt werden.[46] Auch die Möglichkeit einer kumulativen Anwendung von SPG und StPO nach dem freien Willen der Sicherheitsbehörden wurde diskutiert.[47] Um dem Legalitätsprinzip Rechnung zu tragen, ist jedoch eher die erste Variante - also das Abstellen auf das Schwergewicht der polizeilichen Maßnahme - vorzuziehen.[48]

Während der Verfolgung muß die Sicherheitsbehörde entscheiden, ob vom Täter ein weiterer gefährlicher Angriff zu erwarten ist und muß – wenn dieser Fall eintritt – nach dem SPG vorgehen.[49]

Mit der vollendeten Beeinträchtigung des geschützten Rechtsgutes endet der gefährliche Angriff; die Entscheidung darüber, ob mit einem weiteren gefährlichen Angriff gerechnet werden muß, obliegt dabei der Sicherheitspolizei. Diese Tätigkeit dient der

---

[42] Vgl *Trawnicek/Lepuschitz*, Das neue österreichische Sicherheitspolizeigesetz[3] (2000) 162.

[43] Vgl *Aichinger*, Fahndungsmethoden 33.

[44] Vgl *Welp*, Erkenntnisse aus präventiv-polizeilichem Lauscheingriff, NStZ 1995, 602.

[45] Vgl die Nachweise bei *Schmidt-Jortzig*, Möglichkeiten einer Aussetzung des strafverfolgerischen Legalitätsprinzips bei der Polizei, NJW 1989, 129.

[46] Vgl § 21 (2) SPG: „Die Sicherheitsbehörden haben gefährlichen Angriffen ein Ende zu setzen. Hiefür ist dieses Bundesgesetz auch dann maßgeblich, wenn bereits ein bestimmter Mensch der strafbaren Handlung verdächtig ist".

[47] Vgl *Schmidt-Jortzig*, Möglichkeiten einer Aussetzung des strafverfolgerischen Legalitätsprinzips bei der Polizei, NJW 1989, 129.

[48] *Aichinger*, Fahndungsmethoden 33.

[49] Vgl *Aichinger*, Fahndungsmethoden 36.

Gefahrenerforschung, worunter man die Feststellung einer Gefahrenquelle und des für die Abwehr einer Gefahr maßgeblichen Sachverhaltes versteht.[50] Die Befassung mit dem bereits abgeschlossenen Angriff ist Aufgabe der Kriminalpolizei. Dadurch wird eine parallele Anwendung der StPO und des SPG normiert.[51]

Schwieriger zu treffen ist eine Abgrenzung im Bereich der bandenmäßigen oder organisierten Kriminalität: Es ist strittig, ob das Bestehen einer kriminellen Organisation (Verbindung) bereits einen gefährlichen Angriff, welcher sicherheitspolizeiliches Einschreiten erfordert, darstellt. *Hauer/Keplinger*[52] vergleichen das Verhältnis von gefährlichem Angriff und organisierter Kriminalität zueinander mit dem Bild zweier sich überlappender Kreise: Sofern eine kriminelle Organisation einen Straftatbestand erfüllt, ist dies sowohl als gefährlicher Angriff, als auch als organisierte Kriminalität zu beurteilen. Da der Begriff der kriminellen Organisation weiter ist, als jener der organisierten Kriminalität, würde nach dieser Auffassung jede organisierte Kriminalität auch einen gefährlichen Angriff darstellen.

In der Gründung von oder Mitgliedschaft bei einer Kriminellen Organisation liegt jedoch keine konkrete Bedrohung eines Rechtgutes, welche die Voraussetzung für einen gefährlichen Angriff darstellt. Plausibel scheint daher die Meinung von *Fuchs*[53], wonach die umfassenden sicherheitspolitischen Befugnisse zur Gefahrenabwehr nur dann bestünden, wenn ein konkretes Rechtsgut wie Leib, Leben, Freiheit oder Vermögen gegenwärtig oder unmittelbar bedroht ist.

2.2. Zur Reform des strafprozessualen Vorverfahrens

Vor allem im Bereich der Bekämpfung organisierter Kriminalität zeigt sich, wie eben ausgeführt, daß Maßnahmen wie der Lauschangriff oder die Rasterfahndung sehr weit in den Bereich der Prävention und damit auf das Gebiet der Sicherheitspolizei übergreifen können. Gerade bei Informationseingriffen sind Grenzverwischungen und Überschneidungen im Verhältnis zwischen Sicherheitspolizei und Strafverfahren geradezu vorgegeben. Es stellt sich somit die Frage, wie eine solche Konkurrenz von

---

[50] § 16 (4) SPG; vgl *Aichinger*, Der Lauschangriff für Sicherheits- und Kriminalpolizei, JAP 1996, 121.

[51] Vgl *Hauer/Keplinger*, Sicherheitspolizeigesetz[2], § 22 Rz 18.

[52] *Hauer/Keplinger*, Sicherheitspolizeigesetz[2], § 16 Rz 5.

[53] Vgl *Fuchs*, Sicherheitspolizei und Gefahrenbegriff, FS *Moos* (1997) 190.

Eingriffen zu bewältigen ist und ob eine allfällige Kumulation von Maßnahmen mit dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit und dem Übermaßverbot vereinbar ist.[54]

Schon vor Jahrzehnten, vor allem aber mit dem Inkrafttreten des SPG[55], wurde erkannt, daß die dringend notwendige Reform des strafprozessualen Vorverfahrens[56] durch das SPG weder vorweggenommen noch beeinflußt wird, „wenngleich die Gestaltung der rechtsstaatlichen Garantien im SPG einen Standard vorgeben, hinter dem eine künftige Reform der StPO wohl kaum zurückbleiben kann".[57] Bereits im Arbeitsprogramm des Justizressorts für die 19. Gesetzgebungsperiode[58] fand sich der Hinweis, daß die Bemühungen um die Reform des strafprozessualen Vorverfahrens als weitere Etappe einer umfassenden Neuerung der Strafprozeßordnung mit Nachdruck vorangetrieben werden müßten. [59]

Als Ergebnis dieser Bemühungen wurde schließlich das „Bundesgesetz, mit dem zur Bekämpfung Organisierter Kriminalität besondere Ermittlungsmaßnahmen in die Strafprozeßordnung eingeführt, sowie das Strafgesetzbuch, das Mediengesetz, das Staatsanwaltschaftsgesetz und das Sicherheitspolizeigesetz geändert werden" erlassen.[60]

Für das strafprozessuale Vorverfahren fanden sich jedoch bislang, abgesehen von den nunmehrigen Regelungen durch das BG gegen die OK, in der StPO nur rudimentäre Bestimmungen, welche die dringend erforderliche Abgrenzung zwischen *inquisitio generali*s und *inquisitio specialis*[61] garantieren. Tatsächlich nämlich verfolgen die Bestimmungen gegen die organisierte Kriminalität sowohl das Rechtsziel einer Gefahrenabwehr, als auch das der Aufklärung von Straftaten fließend.[62]

---

[54] *Funk*, Sicherheitspolizeiliche Maßnahmen zur Bekämpfung Organisierter Kriminalität, JRP 1996, 39.

[55] Mit Ausnahme der Bestimmung des § 62 SPG ist das Gesetz am 01.05.1993 in Kraft getreten.

[56] Siehe dazu *Ellinger*: Die Reform des strafprozessualen Vorverfahrens (1993); *Moos*, Grundsatzfragen zur Reform des strafprozessualen Vorverfahrens, ÖJZ 1996, 886; *ders*, Reform des strafprozessualen Vorverfahrens, in: *Soyer* (Hrsg), Strukturreform des Vorverfahrens, ÖSD Bd 96, 41; *Schmoller*, Grundstrukturen eines künftigen strafprozessualen Vorverfahrens, ÖJK 1999, 115; *Vogl*, Reform des strafprozessualen Vorverfahrens, ÖJK 1999, 115.

[57] *Funk*, Das neue Sicherheitspolizeirecht – Kodifikation und Reform einer klassischen Verwaltungsmaterie, JBl 1994, 143.

[58] Arbeitsprogramm des Justizressorts für die 19. Gesetzgebungsperiode 71.

[59] Vgl *Pleischl*, Reform des strafprozessualen Vorverfahrens aus der Sicht der Justiz, ÖJK 1994, 14.

[60] BGBl I 105/1997.

[61] Vgl *Machacek*, Die Bekämpfung der organisierten Kriminalität in Österreich, ÖJZ 1998, 555.

[62] *Machacek*, Die Bekämpfung der organisierten Kriminalität in Österreich, ÖJZ 1998, 564.

Konkrete Formen einer Änderung des strafprozessualen Vorverfahrens und damit einer eindeutigen Zuordnung sicherheitspolizeilicher Kompetenzen auf der einen Seite und der Kompetenzen der Strafverfolgungsbehörden andererseits wurden durch das, nunmehr als Regierungsvorlage veröffentlichte, Strafprozeßreformgesetz[63] geschaffen. Ziel dieses Regelwerkes[64] ist es, dem sich praeter legem entwickelten „sicherheitsbehördlichem Vorverfahren" eine Rechtsgrundlage und den durch Ermittlungen der Sicherheitsbehörden betroffenen Personen einen ausreichenden und hinreichend bestimmten Rechtsschutz zu bieten. Das Gesetz zielt darauf ab, kriminalpolizeiliche Aufgaben und Befugnisse, ebenso wie die Rechte der von der Ausübung dieser Befugnisse betroffenen Personen, eindeutig zu regeln und ein einheitliches Vorverfahren vorzuschlagen, welches einerseits die eigenständige Ermittlungskompetenz der Kriminalpolizei anerkennt und andererseits Koordinations- und Leitungsbefugnisse der Staatsanwaltschaft als Garantin der Justizförmigkeit des Verfahrens vorsieht. Aufgaben und Zuständigkeiten sollen klar verteilt werden, um der faktischen Ermittlungskompetenz der Kriminalpolizei und der rechtlichen Zuständigkeit der Justiz im Sinne eines Kooperationsmodells gerecht zu werden.

§ 1 Abs 2 StPORefG gibt Aufschluß über Beginn und Ende des Strafverfahrens.[65] Diese Bestimmung ist auf das Ziel eines einheitlichen Ermittlungsverfahrens ausgerichtet; so soll bereits jede Erhebung des Sachverhalts zum Strafverfahren zählen, womit eine Abgrenzung der allgemeinen Vorklärung des Verdachts einer Straftat zur speziellen Untersuchung der Anschuldigung einer Person und damit eine Zweiteilung des Verfahrens in eine formfreie Aufklärungsphase und ein förmliches Verfahren vermieden werden soll. Ein Strafverfahren soll somit mit jeder auf den Zweck des Verfahrens gerichteten - idR polizeilichen - Ermittlung, welche auf die Gewinnung von

---

[63] „Regierungsvorlage betreffend Bundesgesetz, mit dem die Strafprozessordnung 1975 neu gestaltet wird (Strafprozessreformgesetz)", 1165 BlgNR 21. GP.

[64] Siehe auch die verschiedenen Stellungnahmen zum Ministerialentwurf, beispielsweise jene von *Wegscheider*, im Internet unter *http://www.uni-linz.ac.at/Strafprozeßrecht/Strafprozeßreformgesetz.htm,* jene der Staatsanwaltschaft Graz, im Internet unter *http://www.parlinkom.gv.at/pd/pm/21./ME/his/002/ME0021408.html* oder jene des OGH, im Internet unter *http://www.parlinkom.gv.at/pd/pm/21./ME/his/002/ME0021424.html*.

[65] So wird bestimmt, daß „das Strafverfahren beginnt, sobald zur Aufklärung des Verdachts einer strafbaren Handlung gegen eine bekannte oder unbekannte Person ermittelt oder Zwang gegen eine verdächtige Person ausgeübt wird" und daß das „Strafverfahren durch Einstellung, Absehen oder Rücktritt von der Verfolgung durch die Staatsanwaltschaft (endet)".

Informationen oder Beweisen zur Aufklärung des Verdachts einer strafbaren Handlung abzielt, beginnen.[66] Die aus dem Präventionsauftrag abgeleitete (sicherheitspolizeiliche) Aufgabe zur vorbeugenden Bekämpfung von Straftaten hat dort zu enden, wo hinreichende tatsächliche Anhaltspunkte für eine Straftat vorliegen.[67]

Besonders interessant lesen sich die §§ 18 f des Entwurfs, in denen die Zuordnung kriminalpolizeilicher Aufgabenerfüllung zum Strafrechtswesen und die Abgrenzung von der Sicherheitspolizei ihren Niederschlag findet.[68] Dabei soll der Begriff „Kriminalpolizei" als funktioneller Oberbegriff polizeilicher Tätigkeit im Dienste der Strafrechtspflege eingeführt werden.[69] Die Aufgabe der Kriminalpolizei besteht darin, die Tatumstände soweit zu klären, als dies für die Erhärtung oder Entkräftung des Tatverdachts vonnöten ist und nicht etwa darin, in einer formellen Aufklärungsphase festzustellen, ob hinreichende Anhaltspunkte für den Verdacht einer gerichtlich strafbaren Handlung gegen eine bestimmte Person vorliegen; sobald die Sachverhaltsaufnahme solche hinreichenden Verdachtsmomente aufwirft, wird die kriminalpolizeiliche Aufgabenstellung der Aufklärung strafbarer Handlungen wirksam, die von den zuständigen Behörden wahrzunehmen ist.[70]

Die Aufgaben dieser „kriminalpolizeilichen Behörden" werden schließlich in § 18 Abs 2 StPORefG[71] definiert. Das Gesetz bedient sich dabei der Technik des Verweises auf die Bestimmungen des Sicherheitspolizeigesetzes über die Organisation der Sicherheitsverwaltung, weil grundsätzlich auf bestehende Behörden und deren

---

[66] Vgl EBRV 1165 21. GP 25.

[67] EBRV 1165 21. GP 26.

[68] § 18 (1) StPORefG lautet: „Kriminalpolizei besteht in der Wahrnehmung von Aufgaben im Dienste der Strafrechtspflege (Art. 10 Abs. 1 Z 6 B-VG), insbesondere in der Aufklärung und Verfolgung strafbarer Handlungen nach den Bestimmungen dieses Gesetzes".

[69] Vgl *Dearing*, Sicherheitspolizei und Strafrechtspflege, FS *Platzgummer* 225; *Funk*, Zur Reform des strafrechtlichen Vorverfahrens, Verfassungsrechtliche Aspekte und Beziehungen zum Sicherheitspolizeirecht, in: Entwicklungslinien im Straf- und Strafprozeßrecht, Schriftenreihe des BMJ, Bd 82 (1996) 96.

[70] Vgl EBRV 1165 21. GP 40 f.

[71] „Kriminalpolizei obliegt den Sicherheitsbehörden, deren Organisation und örtliche Zuständigkeit sich nach den Vorschriften des Sicherheitspolizeigesetzes über die Organisation der Sicherheitsverwaltung richten. Aufgaben und Befugnisse, die den Sicherheitsbehörden in diesem Bundesgesetz übertragen werden, stehen auch den ihnen beigegebenen, zugeteilten oder unterstellten Organen des öffentlichen Sicherheitsdienstes zu."

Exekutivorgane zurückgegriffen und nicht in die Organisationshoheit des Bundesministeriums für Inneres eingegriffen werden soll.[72]

Im 2. Abschnitt, betitelt „Kriminalpolizei und Ermittlungsverfahren", bestimmt § 99 (2) StPORefG, daß die Kriminalpolizei bei Gefahr im Verzug auch ohne Anordnung der Staatsanwaltschaft – sofern eine solche vonnöten ist - Zwang ausüben oder Beweise aufnehmen darf. Die Kriminalpolizei soll in einem solchen Falle von sich aus tätig werden können, muß aber, sofern nachträglich keine Genehmigung der Maßnahme erfolgt, die Ermittlungshandlung sogleich beenden und den ursprünglichen Zustand soweit wie möglich wieder herstellen.

Darüber hinaus enthält die Regierungsvorlage Bestimmungen zu „Observation, verdeckte Ermittlung und Scheingeschäft" (§§ 129-133), zur „Beschlagnahme von Briefen, Auskunft über Standort- und Vermittlungsdaten, sowie Überwachung von Nachrichten" (§ 135)[73], zur „optischen und akustischen Überwachung von Personen" (§ 136) und zum automationsunterstützten Datenabgleich" (§§ 141-143).

Zusammenfassend läßt sich also festhalten, daß es im Rahmen der Verfolgung von gerichtlich strafbaren Handlungen nach der StPO zu einer „transfunktionellen Zusammenarbeit"[74] zwischen verschiedenen staatlichen Organen bzw Organtypen kommt, welche durch Arbeitsteilung und Kooperation gekennzeichnet ist.[75]

Es soll sich dabei an der derzeitigen Praxis kriminalpolizeilicher Ermittlungen insofern kaum etwas ändern, als kriminalistische Initiative und ebensolches Know-How weiterhin gefordert sein wird. Es soll der Tätigkeit der Kriminalpolizei ein rechtlicher Rahmen gegeben werden, welcher – nicht zuletzt im Interesse der agierenden Beamten selbst – modernern rechtsstaatlichen Anforderungen genügt.[76]

---

[72] Vgl EBRV 1165 21. GP 41.

[73] Vgl dazu unten, 5.5.2.3.

[74] *Funk*, Zur Reform des strafrechtlichen Vorverfahrens: Verfahrensrechtliche Aspekte und Beziehungen zum Sicherheitspolizeirecht, in: Entwicklungslinien im Straf- und Strafprozeßrecht, Schriftenreihe des BMJ, Bd 82, 99.

[75] Vgl *Hauenschild*, Das Zusammenwirken der Strafverfolgungsbehörden – verfassungsrechtliche Fragen zum Entwurf der Strafprozeßreform, RZ 2000, 186.

[76] Vgl die EBRV 1165 21. GP 137.

3. Der „Lausch- und Spähangriff“

Kaum ein Terminus hat im Zuge einer Strafrechtsreform medial so hohe Wellen geschlagen, wie die Einführung des „Lausch- und Spähangriffs“ im Zuge der StPO-Reform 1996[77], obwohl dieser, vor allem in Zusammenhang mit der verdeckten Ermittlung, schon mit dem Erlaß des Sicherheitspolizeigesetzes in der österreichischen Rechtsordnung verankert wurde.[78] Die Installierung dieses Instruments mit Inkrafttreten des SPG per 01. Mai 1993 erfolgte – so hat es den Anschein – quasi ungewollt und unbemerkt.[79]

Mit einem negativen Beigeschmack versehen, wurde diese Form der Ermittlung in der Lehre heftigst diskutiert[80], selbst Befürworter des Lausch- und Spähangriffs traten für eine Beschränkung desselben auf die StPO ein und wandten sich gegen parallele Ermächtigungen im Polizeirecht.[81] Auch in Deutschland setzte sich ein Teil der Lehre dafür ein, die alleinige *richterliche* Anordnungskompetenz für den Lauschangriff festzulegen, „da es sich hierbei nun einmal um einen schwerwiegenden Eingriff in die Intimsphäre des Bürgers handelt und man sich zum anderen kaum eine Situation vorstellen kann, in der ein Richter für eine solche Beschlußfassung nicht erreichbar ist, zumal solche Situationen Vorbereitungen notwendig machen“.[82] Vorgeschlagen wurde auch, die Termini „Lauschangriff“ oder „Spähangriff“ durch „akustische Beweissicherung“, „Elektronische Wohnraumüberwachung“ oder „Verbrechensbekämpfung mit elektronischen Mitteln“ zu umschreiben[83], da mit erstgenannten Begriffen in Österreich weitgehend Negatives verbunden wird und jede

---

[77] BGBl I 105/1997 „Bundesgesetz, mit dem zur Bekämpfung Organisierter Kriminalität besondere Ermittlungsmaßnahmen in die Strafprozeßordnung eingeführt, sowie das Strafgesetzbuch, das Mediengesetz, das Staatsanwaltschaftsgesetz und das Sicherheitspolizeigesetz geändert werden“.

[78] Vgl § 54 (4) SPG idF BGBl 566/1991.

[79] Vgl *Soyer*, Lauschangriffe in Österreich, JRP 1994, 270

[80] Beispielsweise bei *Ellinger*, Der „Lauschangriff“. Begriff und Manipulation, in: Der Kriminalbeamte 4/1994, 12; *Lisken*, Vorfeldeingriffe im Bereich der „Organisierten Kriminalität“ – Gemeinsame Aufgabe für Verfassungsschutz und Polizei? ZRP 1994, 267; *Dearing*, Sicherheitspolizei und Strafrechtspflege, FS-*Platzgummer* (1995) 250; *Funk*, Sicherheitspolizeiliche Maßnahmen zur Bekämpfung Organisierter Kriminalität, JRP 1996, 27.

[81] Vgl *Soyer*, Lauschangriffe in Österreich, JRP 1994, 270.

[82] Vgl *Ostendorf*, Organisierte Kriminalität – eine Herausforderung für die Justiz, JZ 1991, 69.

[83] Vgl *Hund*, Der Einsatz technischer Mittel in Wohnungen – Versuch einer verfassungskonformen Lösung, ZRP 1995, 334.

Art von Heimlichkeit im Sprachgebrauch mit dem Unredlichen in Verbindung gebracht wird;[84] Befürworter sehen in diesen Bezeichnungen eine Diskreditierung eines zumindest diskutablen, wenn nicht notwendigen Mittels.[85]

3.1. Begriffserklärung und Abgrenzung

Von einem „*kleinen Lausch- und Spähangriff*" spricht man, wenn ein verdeckter Ermittler alle an ihn gerichteten Äußerungen heimlich Mittels Bild- und Tonaufzeichnungsgeräten festhält und anschließend die Aufnahmen auch der Behörde zugänglich macht.[86] Erfaßt wird somit der Fall, daß die Überwachung in Kooperation mit einem von ihr Betroffenen durchgeführt wird. Dieser Betroffene ist sich daher der Tatsache bewußt, daß er sich in einer Kommunikationssituation mit einem Dritten befindet und kann daher sein Verhalten auf die Überwachung einstellen. Diese basiert jedoch auf einem Irrtum des Überwachten in bezug auf die Absichten seines Gesprächspartners.[87]

Der „*große Lausch- und Spähangriff*" wird durch das kontrollierte Abhören oder Aufzeichnen von Gesprächen oder Sicherheitsbehörden ohne Beisein eines Beamten bestimmt. Es werden dabei per Richtmikrofon, Wanze oder mit anderen Mitteln fremde Gespräche abgehört und aufgezeichnet.[88]

Vom „*ganz großen Lausch- und Spähangriff*" wird gesprochen, wenn sich dieser auf den Einsatz in Wohnungen bezieht und ohne Beisein eines verdeckten Ermittlers erfolgt.[89]

---

[84] Vgl *Aichinger*, Fahndungsmethoden 43.

[85] *Funk*, Sicherheitspolizeiliche Maßnahmen zur Bekämpfung Organisierter Kriminalität, JRP 1996, 34.

[86] Vgl *Schmoller*, Geändertes Erscheinungsbild staatlicher Verbrechensbekämpfung, ÖJZ 1996, 24.

[87] Vgl *Miklau/Pilnacek*, Optische und akustische Überwachungsmaßnahmen zur Bekämpfung schwerer Organisierter Kriminalität („Lauschangriff") – Paradigmenwechsel im Verfahrensrecht? JRP 1997, 293.

[88] Vgl *Aichinger*, Der Lauschangriff für Sicherheits- und Kriminalpolizei, JAP 1996, 119.

[89] Zur Problematik des „Lauschens" in Wohnungen siehe zB für Deutschland: *Hund*, Der Einsatz technischer Mittel in Wohnungen – Versuch einer verfassungskonformen Lösung, ZRP 1995, 334 ff.

3.2. Der sicherheitspolizeiliche Lausch- und Spähangriff

§ 54 (2) Z 3 SPG bestimmt, daß – abgesehen von der Verhinderung bestimmter strafbarer Handlungen noch während ihrer Vorbereitung – die Observation zulässig ist, „wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wäre." Es muß daher bei der Bekämpfung krimineller Verbindungen noch nicht ein konkreter Verdacht gegen einen bestimmten Menschen vorliegen, sondern es genügt ein auf Tatsachen gegründeter Verdacht.[90]

Im Folgenden wird durch § 54 (4) SPG geregelt, daß „die Ermittlung personenbezogener Daten *nur* für die Abwehr gefährlicher Angriffe oder krimineller Verbindungen zulässig" ist. Tatsächlich jedoch ist, nach Betrachtung der Definition eines gefährlichen Angriffs, der Einsatz von Aufzeichnungsgeräten lediglich für Zwecke der Feststellung der Gefahrenquelle, der Vorbeugung wahrscheinlicher gefährlicher Angriffe und der Aufrechterhaltung der öffentlichen Ordnung *nicht* vorgesehen.[91]

Besonders irreführend vor der SPG-Novelle 2000[92] war der Hinweis im § 54 (4) SPG, daß § 120 (1) StGB[93] und das Fernmeldegeheimnis von dieser Bestimmung unberührt bleiben. Strittig war, ob in dieser Bestimmung eine Einschränkung der Ermittlungsbefugnis auf den kleinen Lauschangriff zu sehen sei, oder eine differenzierte Sondervorschrift für den (kleinen Lauschangriff) verdeckter Ermittler.[94]

Vor der gegenständlichen Novelle ergab sich somit folgendes Bild: Während *Funk*[95] die Einschränkung, welche aus dem Verweis des § 54 (4) SPG auf § 120 (1) StGB resultierte, als generelles Verbot des großen Lauschangriffs, also als Verbot des Einsatzes von Tonaufnahme und -*übertragungsgeräten* (hier wird nicht zwischen der Zulässigkeit des Lauschens einerseits und der Zulässigkeit einer Aufzeichnung der Kommunikationsinhalte auf der anderen Seite differenziert) zur akustischen

---

[90] Vgl *Funk*, Sicherheitspolizeiliche Maßnahmen zur Bekämpfung Organisierter Kriminalität, JRP 1996, 31.

[91] Vgl *Soyer*, Lauschangriffe in Österreich, JRP 1994, 271.

[92] BGBl I 85/2000.

[93] Nach dieser Bestimmung wird der Einsatz von Tonaufnahme- und Abhörgeräten zum Zwecke des Zugänglichmachens einer fremden Äußerung, welche weder an den Empfänger gerichtet, noch in der Öffentlichkeit abgegeben wurde, untersagt.

[94] *Soyer*, Lauschangriffe in Österreich, JRP 1994, 271.

[95] *Funk*, Sicherheitspolizeiliche Maßnahmen zur Bekämpfung Organisierter Kriminalität, JRP 1996, 35.

Raumüberwachung für Zwecke der Sicherheitspolizei ansah, unterschied *Soyer*[96] zwischen Ermittlungen nicht-beamteter V-Leute und Organen des öffentlichen Sicherheitsdienstes: Während die Sicherheitsbehörden im Rahmen von § 54 (2) und (3) SPG dazu befugt seien, große und kleine Lauschangriffe mit Bild- und Tonübertragungsgeräten durchzuführen und darüber hinaus im rechtlichen Rahmen des § 54 (4) SPG (zur Abwehr gefährlicher Angriffe oder bandenmäßiger oder Organisierter Kriminalität) sich auch des Instruments des großen Lauschangriffs bedienen könnten, sei der – auch nur kleine – Lauschangriff durch nicht beamtete V-Leute/Spitzel unzulässig und bliebe gem § 120 (1) StGB strafbar. Dabei übersehe er jedoch, so *Aichinger*[97], daß § 120 (1) StGB nur vor dem Abhören einer nicht öffentlichen Äußerung durch einen Unbefugten, zu dessen Kenntnisnahme die Äußerung nicht bestimmt ist, schützt. Verdeckte Ermittler, egal ob privat oder beamtet, seien zur Kenntnisnahme der Äußerungen bestimmt, wodurch V-Leute deshalb nicht von § 120 (1), sondern nur von § 120 (2) StGB erfaßt würden.

Mit der Novelle 2000 des SPG wurde § 54 novelliert, um solchen differenzierenden Auslegungen zu begegnen und die rechtlichen Rahmenbedingungen - sowohl für den sicherheitspolizeilichen Lauschangriff, als auch den sicherheitspolizeilichen Spähangriff – klarzustellen. So wurde die Wendung „§ 120 (1) StGB und das Fernmeldegeheimnis bleiben unberührt“ durch „das Fernmeldegeheimnis bleibt unberührt“ ersetzt und in § 54 (4) eine Ziffer 1 und 2 eingefügt.

Unzulässig ist nunmehr die Ermittlung personenbezogener Daten durch *Tonaufzeichnungsgeräte*, um nichtöffentliche und nicht in Anwesenheit eines Ermittelnden erfolgte Äußerungen aufzuzeichnen (§ 54 Abs 1 Z 1). Die EB[98] halten dazu fest, daß „was in Abs 4 zunächst die *Unzulässigkeit des „großen Lauschangriffs”* anlangt, an die Stelle des Verweises auf § 120 Abs 1 StGB nunmehr eine ausdrückliche Formulierung der damit normierten Kriterien (Nichtöffentlichkeit und Abwesenheit eines Ermittlers) getreten“ ist.

---

[96] *Soyer*, Lauschangriffe in Österreich, JRP 1994, 271 f.

[97] *Aichinger*, Fahndungsmethoden 52.

[98] EBRV 81 BlgNR 21. GP 6

Gerade die Unklarheit in § 54 (4) SPG (alt) sprach dafür, daß der Gesetzgeber bei der Schaffung dieser Bestimmung gar nicht an die Möglichkeit des großen Lauschangriffs gedacht hat[99], was sich nunmehr in der neuen gesetzlichen Regelung zeigt.

Auch was den *großen Spähangriff* angeht, brachte die Novelle des SPG etwas grundsätzlich Neues: Hatte ein Großteil der Lehre einen solchen de lege ferenda für zulässig erachtet[100], so bestimmt § 54 (4) Z 2 nunmehr, daß die Ermittlung personenbezogener Daten „durch *Bildaufzeichnungsgeräte*, um nichtöffentliches und nicht im Wahrnehmungsbereich eines Ermittelnden erfolgtes Verhalten aufzuzeichnen“ (§ 54 Abs 1 Z 2) ebenfalls unzulässig ist.

Die am stärksten in die Rechte Betroffener eingreifenden Ermittlungsinstrumente der verdeckten Ermittlung einerseits und des Einsatzes von Bild- und Tonaufzeichnungsgeräten andererseits sollen auf schwere Fälle der Abwehr krimineller Verbindungen beschränkt werden. Es sollte klargestellt werden, daß das SPG keine Grundlage zur Durchführung eines sogenannten „großen Spähangriffs“ bietet.[101]

Diese Ergänzung sollte also festlegen, daß nicht nur der „große Lauschangriff”, sondern auch der sogenannte „große Spähangriff”, also der isolierte Einsatz von Aufzeichnungsgeräten als Ermittlungsinstrument der Sicherheitspolizei, an die Voraussetzung einer gerichtlichen Genehmigung nach den §§ 149d ff StPO gebunden bleibt.[102]

Da jedoch die eben erläuterten Bestimmungen nur für Bild- und Tonaufzeichnungsgeräte Geltung besitzen, stellt sich die Frage, ob denn das Ermitteln personenbezogener Daten durch Ton*übertragungsgeräte* zulässig ist. Dies wird ebenfalls, unter Berufung auf den eindeutigen Gesetzeswortlaut, von einem Teil der

---

[99] So schon *Funk*, Sicherheitspolizeiliche Maßnahmen zur Bekämpfung Organisierter Kriminalität, JRP 1996, 35.

[100] So zB *Schmoller*, Geändertes Erscheinungsbild staatlicher Verbrechensbekämpfung, ÖJZ 1996, 24; *Funk*, Sicherheitspolizeiliche Maßnahmen zur Bekämpfung Organisierter Kriminalität, JRP 1996, 35; *Soyer*, Lauschangriffe in Österreich, JRP 1994, 272; *Aichinger*, Der Lauschangriff für Sicherheits- und Kriminalpolizei, JAP 1996, 127; *ders*, Fahndungsmethoden 54.

[101] Vgl den Bericht des Ausschusses für Innere Angelegenheiten über die Regierungsvorlage (BlgNR 81 21. GP) BlgNR 223 21. GP 1.

[102] EBRV 81 BlgNR 21. GP 6.

Lehre für zulässig erachtet.[103] Die Gesetzesmaterialien zum SPG 1993[104]unterscheiden aber eindeutig zwischen Bild- und Tonaufzeichnungsgeräten einerseits und Bild- und Tonübertragungsgeräten andererseits. Letztere sind lediglich ein Hilfsmittel direkter Überwachung, deren Einsatz immer dann zulässig ist, wenn die Ermittlung als solche zulässig ist.

Nicht eingeschränkt werden durch diese Bestimmung jedoch Ton- und Bildaufzeichnungen von öffentlichem Verhalten, gleichgültig, ob es in Anwesenheit oder im optischen Wahrnehmungsbereich eines Ermittelnden erfolgt oder nicht.[105]

Eine weitere Neuerung in § 54 SPG stellt der neu eingefügte Absatz 4a dar, welcher bestimmt, daß der Einsatz von Bild- und Tonaufzeichnungsgeräten zur Abwehr einer kriminellen Verbindung nur zulässig ist, wenn die Begehung von mit beträchtlicher Strafe bedrohten Handlungen[106] zu erwarten ist und außerdem durch solche Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit zum Anlaß der Ermittlungen gewahrt wird. Damit wurde ein Pendant zu § 149d (3) StPO geschaffen, welcher den Einsatz strafprozessualer Überwachungsmethoden unter Verwendung technischer Mittel an die Voraussetzungen der Verhältnismäßigkeit zum Zweck der Maßnahme bindet.

Durch diese Bestimmung sollte eine strikte Limitierung des Einsatzes der schwersten Ermittlungsinstrumente die das SPG kennt, nämlich der verdeckten Ermittlung einerseits und des Einsatzes von Bild- und Tonaufzeichnungsgeräten andererseits, normiert werden. Es soll jeweils anhand der konkreten Umstände des Einzelfalls zu beurteilen sein, ob eine allgemeine Gefahr das von § 54 Abs 4a SPG geforderte Gewicht erreicht.[107]

Etwas mißverständlich mutet der Wortlaut des § 54 (4) SPG an, wonach die Sicherheitsbehörden ermächtigt sind, zur Erreichung der im § 54 (1) SPG angeführten Zwecke personenbezogene Daten auch „durch Einsatz von Bild- und Tonaufzeichnungsgeräten zu ermitteln“. Natürlich kann dies auch nur für den kleinen Lausch- bzw Spähangriff gelten, da nur ein solcher nach der Intention des Gesetzgebers

---

[103] So zB *Wiederin,* Sicherheitspolizeirecht Rz 610; mit Einschränkungen *Hauer/Keplinger*, Sicherheitspolizeigesetz[2], § 54 B.10

[104] 148 BlgNR 18. GP 44.

[105] *Hauer/Keplinger*, Sicherheitspolizeigesetz[2], § 54 B.10.

[106] „Mit beträchtlicher Strafe bedroht sind gerichtlich strafbare Handlungen, welche mit mehr als einjähriger Freiheitsstrafe bedroht sind“ (§ 17 SPG).

[107] EBRV 81 BlgNR 21. GP 7.

und in Anbetracht der Bestimmung des § 54 (4) im Sicherheitspolizeirecht überhaupt zulässig ist. Klarheit soll hier eine Neufassung der Bestimmung des § 53 (4) SPG im Zuge einer „SPG-Novelle 2002“[108] bringen: Die betreffende Regelung soll insoweit abgeändert werden, als „die Ermittlung personenbezogener Daten durch Einholen von Auskünften, Beobachten und Einsatz von Bild- und Tonaufzeichnungsgeräten...nur unter den Voraussetzungen des § 54 zulässig “[109] ist.

3.3. Der Lausch- und Spähangriff zur Strafverfolgung

3.3.1. Allgemeines

Bis zur Novelle der Strafprozeßordnung 1996, mit der die Bestimmungen über besondere Ermittlungsmaßnahmen in die StPO eingefügt wurden[110], gab es in Österreich keine Regelung, welche den Lausch- und Spähangriff für zulässig erklärt hätte. Auf die Generalermächtigung des § 24 StPO[111], also den sog „ersten Zugriff der Sicherheitsbehörden“, konnten solche Eingriffe nicht gestützt werden, da dieser nur die Hausdurchsuchung, die vorläufige Verwahrung und die keinen Aufschub gestattenden Vorbereitungshandlungen, sowie das Nachforschen reguliert. Diese Bestimmung stellt eine Eingriffsermächtigungsnorm dar. Aufgrund eines Größenschlusses kann festgehalten werden, daß die Eingriffsintensität des Lausch- und Spähangriffs stärker als jene der Hausdurchsuchung ist, welche nur in den gesetzlich ausdrücklich normierten

---

[108] Ministerialentwurf eines „Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Paßgesetz 1992, das Bundesgesetz über den Schutz vor Straftaten gegen die Sicherheit von Zivilluftfahrzeugen und das Allgemeine bürgerliche Gesetzbuch geändert werden (SPG-Novelle 2002)“, 312/ME 21. GP.

[109] In der Stellungnahme des BMJ zum Entwurf (9/SN-312/ME) geht jenes davon aus, daß die vorgeschlagene Formulierung bedeuten würde, daß „die Erteilung von Auskünften nach den Abs 3, 3a und 3b ebenfalls nur unter den Bedingungen des § 54 Abs 1, also insbesondere der Freiwilligkeit der Mitwirkung, erfolgen müßte“; dieses Ergebnis sei nicht beabsichtigt gewesen.

[110] BGBl I 105/1997.

[111] „Sicherheitsbehörden haben alle Verbrechen und Vergehen mit Ausnahme von Privatanklage- und Antragsdelikten nachzuforschen und die keinen Aufschub gestattenden vorbereitenden Anordnungen zu treffen“.

Fällen (§§ 139 ff StPO) zulässig ist. Weder die Zulässigkeit des Lauschangriffs, noch die des Spähangriffs findet daher in dieser Bestimmung rechtliche Deckung.[112]
Geregelt waren aber schon zu diesem Zeitpunkt die Voraussetzungen für die Überwachung des Fernmeldeverkehrs.[113] Diese Bestimmung ist, nicht zuletzt aufgrund der am 01.01.2002 in Kraft getretenen „Überwachungsverordnung“[114], wieder in den Mittelpunkt der Diskussion um die umstrittene Frage des Bestehens einer Verpflichtung seitens der Telekommunikationsdiensteanbieter, Vermittlungs- und Verbindungsdaten längerfristig speichern und auf Verlangen den Sicherheits- und Strafverfolgungsbehörden aushändigen zu müssen, getreten. Diese Bestimmung soll also später[115] noch genauer untersucht werden, zunächst aber werden – der Vollständigkeit halber für den Lauschangriff und aus für Ermittlungen im Internet relevanten Gründen für den Spähangriff – die Voraussetzungen der Anwendung dieser besonderen Ermittlungsmaßnahmen wie sie die StPO vorsieht, erläutert werden.

3.3.2. Technische Eingriffsmittel

Unter den Begriffen „technische Mittel zur Bild- oder Tonaufnahme“ versteht man jede technische Vorrichtung, wodurch Wahrnehmungen oder Töne über den örtlichen Sicht- oder Klangbereich hinaus verstärkt übertragen werden können. Ferngläser oder ähnliche Mittel, die bloß die unmittelbare Wahrnehmung[116] ermöglichen oder erleichtern, dabei aber keine Übertragungs- oder Aufzeichnungsfunktion besitzen, fallen nicht darunter.
Aus Gründen der Spezialität der §§ 149a bis 149c StPO werden von den gegenständlichen Regelungen auch solche Abhörvorrichtungen nicht erfaßt, die nur zur Überwachung eines Fernmeldeverkehrs angebracht werden.[117]
Ein Bild- oder Tonaufnahmegerät ist eine solche Vorrichtung, die Bilder, Töne oder Tonfolgen so konserviert, daß sie wiederholbar wiedergegeben werden können.[118]

---

[112] Vgl *Aichinger*, Fahndungsmethoden 55.

[113] § 149a StPO idF BGBl 526/1993.

[114] „Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs“ BGBl II 418/2001.

[115] Unten, 5.6.

[116] Vgl *Miklau/Pilnacek*, Optische und akustische Überwachungsmaßnahmen zur Bekämpfung schwerer Organisierter Kriminalität („Lauschangriff“) – Paradigmenwechsel im Verfahrensrecht? JRP 1997, 292.

[117] EBRV 49 BlgNR 20. GP 16.

Der Einsatz solcher Mittel muß auf die Überwachung nichtöffentlichen Verhaltens und nichtöffentlicher Äußerungen von Personen ohne deren Kenntnis darüber gerichtet sein; öffentliche Äußerungen, die für einen größeren, unbestimmten Personenkreis bestimmt sind, werden von den betreffenden Bestimmungen nicht erfaßt.[119] Überall dort, wo wegen der potentiellen Anwesenheit Dritter Privatheit faktisch nicht gewahrt werden kann, liegt kein nichtöffentliches Verhalten vor.[120]

3.3.3. Anwendungsvoraussetzungen des § 149d StPO (Lauschangriff)

Nach § 149d (1) Z 1 StPO ist der Lauschangriff dann zulässig, wenn und solange der Verdacht besteht, daß eine von der Überwachung betroffene Person eine andere entführt, oder sich sonst ihrer bemächtigt hat. Da diese Fälle in rechtlicher Hinsicht in der Regel problemlos erfaßt werden können und besonders rasches Einschreiten erfordern, sind keine weiteren Zulässigkeitsvoraussetzungen vonnöten und ist insbesondere auch keine richterliche Genehmigung vorgesehen. Dabei verfolgt die Überwachung regelmäßig auch repressive Zwecke, die von der Feststellung der Identität des Überwachten, über allgemeine Beweisgewinnungserfordernisse, bis hin zur Beurteilung allfälliger Verbrechensqualifikationen und Strafzumessungsgründe reichen können.[121] Im Unterschied zur Regierungsvorlage ist es die Ansicht des Justizausschusses, daß „bloß die schwerwiegenden und ein sofortiges Einschreiten der Organe des öffentlichen Sicherheitsdienstes gebietenden Fälle einer „Geiselnahme“ im Sinne der Bestimmungen der §§ 100 ff StGB angesprochen werden“.[122]

---

[118] Vgl zu den verschiedenen Techniken etwa *Wahl*, Minispione - Wie sind sie geschaltet, wie werden sie abgewehrt (1987); *Nogala*, Polizei, avancierte Technik und soziale Kontrolle (1989) 49 ff; *Aichinger*, Fahndungsmöglichkeiten 47 ff mwN.

[119] Alles, was mit freiem Auge (öffentlich) wahrnehmbar ist, kann mit Fernglas, Fotoapparat oder Videogerät aufgenommen werden, ohne an die Voraussetzungen des Einsatzes technischer Mittel gebunden zu sein. Hingegen ist der Inhalt eines Gesprächs nicht öffentlich, weshalb auch das Anbringen einer „Wanze“ am Tisch, um das Gespräch abzuhören, nur unter den Voraussetzungen des § 149d StPO zulässig ist (vgl *Leukauf/Steining*er, StGB^3, § 149d Rz 2).

[120] *Miklau/Pilnacek*, Optische und akustische Überwachungsmaßnahmen zur Bekämpfung schwerer Organisierter Kriminalität („Lauschangriff“) – Paradigmenwechsel im Verfahrensrecht? JRP 1997, 292.

[121] EBRV 49 BlgNR 20. GP 17.

[122] JAB 812 BlgNR 20. GP 4.

Der Lauschangriff im Anwendungsfall des § 149d (1) Z 1 StPO bedarf keiner gerichtlichen Anordnung.[123]

§ 149d (1) Z 2 StPO gestattet die Überwachung, wenn sie sich auf Vorgänge und Äußerungen beschränkt, die zur Kenntnisnahme einer von der Überwachung informierten Person bestimmt sind, „oder von dieser unmittelbar wahrgenommen werden können“[124] (*kleiner Lauschangriff* durch einen verdeckten Ermittler oder einer Person, die zur Zusammenarbeit mit der Behörde bereit ist)[125] und sie zur Aufklärung eines Verbrechens erforderlich erscheint. Allerdings werden auch solche (Zwischen-) Äußerungen, die von der Zielperson Dritten gegenüber in Anwesenheit des von der Überwachung Informierten abgegeben werden, als zu deren Kenntnisnahme bestimmt anzusehen sein.[126]

Dabei wird nicht ausschließlich in fremde Kommunikation oder fremdes Verhalten eingedrungen, sondern eine Situation ausgenützt, in der der Überwachte seinem Gesprächspartner etwas mitteilt, was zwar für diesen bestimmt ist, der Überwachende aber als Dritter nicht wissen soll. Damit unterscheidet sich jedoch dieser Fall einer Überwachung kaum von einem Normalfall der Kommunikation: Der Betroffene kann (und muß) sich auf potentielle Indiskretionen des Gesprächspartners einstellen, er hätte diesem mithin mißtrauen können und müssen.[127]

Tatbestandsmerkmal ist auch, daß die Überwachung zur Aufklärung eines Verbrechens *erforderlich* zu sein *scheint*. Durch diese Formulierung sollte die Voraussetzung zum Ausdruck gebracht werden, daß die geplante Überwachungsmaßnahme auf Grund konkreter Anhaltspunkte Aussicht auf Erfolg verspricht und der Untersuchungszweck nicht auf andere, gelindere, Art und Weise erreicht werden kann.[128]

---

[123] § 149e (1) Z 1 Satz 1 StPO.

[124] Eingefügt durch das „Bundesgesetz, mit dem die Strafprozeßordnung 1975 und das Bundesgesetz BGBl I 105/1997 im Bereich besonderer Ermittlungsmaßnahmen geändert werden (Strafprozeßnovelle 2001“ BGBl I 130/2001).

[125] Vgl *Aichinger*, Bundesgesetz zur Einführung besonderer Ermittlungsmaßnahmen in die StPO, JAP 1997/98, 57.

[126] EBRV 49 BlgNR 20. GP 17.

[127] Vgl *Gusy*/*Ziegler*, Menschenrechtsfragen elektronischer Personenüberwachung, ZRP 1996, 193 ff.

[128] Vgl EBRV BlgNR 18. GP 9.

Die Anordnungsbefugnis für den „kleinen Lauschangriff" iSd § 149d (1) Z 2 StPO obliegt der Ratskammer;[129] soll eine Überwachung in ausschließlich der Berufsausübung gewidmeten Räumlichkeiten einer im § 152 (1) Z 4, 5 StPO oder § 31 (1) MedienG aufgeführten Person durchgeführt werden, so ist auch eine Ermächtigung des Rechtsschutzbeauftragten[130] zwingend vorgesehen.[131]

Den seiner Intensität nach stärksten Eingriff in Grund- und Freiheitsrechte stellt die im § 149d Abs 1 Z 3 StPO geregelte Form der Überwachung („*großer Lauschangriff*") dar. Sie soll daher nur zulässig sein, wenn die Aufklärung „eines mit mehr als 10 Jahren Freiheitsstrafe bedrohten Verbrechens, oder des Verbrechens der kriminellen Organisation oder der terroristischen Vereinigung (§§ 278a, 278b StGB) oder die Aufklärung oder Verhinderung von im Rahmen einer solchen Organisation oder Vereinigung"[132] begangenen oder geplanten strafbaren Handlungen

- ansonsten *aussichtslos* oder *wesentlich erschwert* wäre

und

a.) eine überwachte Person des mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder des Verbrechens nach § 278a oder § 278b StGB[133] *dringend verdächtig* ist

oder

b.) Gründe für die Annahme vorliegen, daß eine dringend verdächtige Person mit einer überwachten Person *in Kontakt treten werde*, es sei denn, daß die überwachte Person von der Verbindlichkeit zur Ablegung eines Zeugnisses gesetzlich befreit ist.

Der große Lauschangriff darf nur bei Vorliegen eines sehr hohen Verdachtsgrades, also nur dann, wenn ein hoher Grad an Wahrscheinlichkeit vorliegt daß die überwachte Person Täter eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder eines Verbrechens nach § 278a StGB ist, angeordnet werden.[134]

---

[129] § 149e (1) StPO.

[130] § 149n StPO.

[131] § 149e (2) StPO idF BGBl I 130/2001.

[132] § 149d Abs 1 Z 3 StPO idF BGBl I 134/2002.

[133] § 149d Abs 1 Z 3 lit a StPO idF BGBl I 134/2002.

[134] Vgl Aichinger, Bundesgesetz zur Einführung besonderer Ermittlungsmaßnahmen in die StPO, JAP 1997/98, 58.

Die Aufklärung eines Verbrechens ist dann aussichtslos oder wesentlich erschwert, wenn andere Aufklärungsmittel überhaupt nicht vorhanden sind, oder ihre Erfolgsaussichten nicht ins Gewicht fallen. Eine wesentliche Erschwerung liegt insbesondere dann vor, wenn die Benutzung anderer Aufklärungsmittel einen erheblich größeren Zeitaufwand erfordern und daher zu einer wesentlichen Verfahrensverzögerung führen würde.[135] Eine Überwachung kann auch dann angeordnet werden, wenn ein Verhalten, welches darauf abzielt und geeignet ist, die Bedrohung eines Rechtsgutes durch die Verwirklichung eines Tatbestandes einer gerichtlich strafbaren Handlung vorzubereiten, vorliegt. Von der Überwachung erfaßt werden also auch die von einer kriminellen Organisation geplanten Handlungen, die eine schwere Gefahr für die öffentliche Sicherheit begründen würden, was in der Regel bei Vergehen nicht der Fall sein wird.[136]
Damit soll der Verschwiegenheitskodex organisierter Tätergruppen und deren sonstige Abschirmung vor staatlichen Verfolgungsmaßnahmen durchbrochen werden, um gezielt deren Struktur und Hierarchie anzugreifen, ihre Arbeitsweise zu stören und die Ausführung weiterer Straftaten zu verhindern.[137]
Der Tatverdacht muß sich aber, ähnlich wie bei den Bestimmungen zur Telefonüberwachung, nicht gegen eine namentlich bekannte Person richten. Es ist demnach zulässig, daß die Überwachung auch nicht verdächtige Personen einschließt, wenn aus bestimmten Gründen anzunehmen ist, daß eine dringend verdächtige Person mit einer solchen in Kontakt treten werde.[138]

Die Anordnung des großen Lauschangriffs iSd § 149d (1) Z 3 StPO obliegt der Ratskammer, welche auch ein Eindringen in eine bestimmte Wohnung oder sonstige zum Hauswesen gehörende Räumlichkeiten anordnen kann, soweit dies für die Durchführung der Überwachung unumgänglich ist.[139] Zusätzlich ist eine Ermächtigung des Rechtsschutzbeauftragten vonnöten, wenn eine Überwachung in ausschließlich der

---

[135] Vgl EBRV 49 BlgNR 20. GP 18.

[136] Vgl JAB 812 BlgNR 20. GP.

[137] Vgl *Miklau/Pilnacek*, Optische und akustische Überwachungsmaßnahmen zur Bekämpfung schwerer Organisierter Kriminalität („Lauschangriff") – Paradigmenwechsel im Verfahrensrecht? JRP 1997, 295.

[138] 49 BlgNR 20. GP 18.

[139] § 149e (1) StPO.

Berufsausübung gewidmeten Räumlichkeiten einer im § 152 (1) Z 4, 5 StPO oder § 31 (1) MedienG aufgeführten Person durchgeführt werden soll.[140]
Eine zusätzliche Voraussetzung für die Durchführung sowohl des kleinen, als auch des großen Lauschangriffs normiert § 149d (3) StPO: Eine Überwachung ist nur zulässig, soweit die *Verhältnismäßigkeit* zum Zweck der Maßnahme gewahrt wird.
Soll der große Lauschangriff zur Verhinderung von im Rahmen einer kriminellen Organisation geplanten strafbaren Handlungen angeordnet werden, so ist dies nur zulässig, wenn bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen.

3.3.4. Der „Spähangriff" zur Strafverfolgung

Der Spähangriff (optische Objektüberwachung, Videofalle) ist nach § 149d (2) StPO zum Zweck der Aufklärung einer strafbaren Handlung dann zulässig, wenn er sich auf Vorgänge *außerhalb einer Wohnung* oder sonstiger zum Hauswesen gehöriger Räumlichkeiten beschränkt und ausschließlich zu dem Zweck erfolgt, Gegenstände oder Örtlichkeiten zu beobachten, um das Verhalten von Personen zu erfassen, die mit den Gegenständen in Kontakt kommen oder solche Örtlichkeiten betreten (Z 1) oder wenn er *in* einer *Wohnung* oder sonstigen zum Hauswesen gehörigen *Räumlichkeit* erfolgt und dadurch eine mit *mehr als einjähriger Freiheitsstrafe bedrohte Handlung*, deren Aufklärung ansonsten aussichtslos oder wesentlich erschwert wäre, aufgeklärt werden kann. Zusätzliches Erfordernis stellt die Einwilligung des Inhabers der Räumlichkeiten in die Überwachung dar (Z 2).

Eine optische Objektüberwachung durch Sicherheitsbehörden ist also sowohl nach § 54 (4) SPG (mit Ausnahme des „großen Spähangriffs"), als auch nach der StPO zulässig, je nachdem, ob die Observation zur Strafaufklärung oder zur Gefahrenabwehr - also speziell zur Abwehr gefährlicher Angriffe oder krimineller Verbindungen - erfolgen soll.[141]
Durch die Regelung des § 149d Abs 2 StPO soll klargestellt werden, daß die optische Überwachung außerhalb von Wohnungen auch ohne die materiellen Voraussetzungen

---

[140] § 149e (2) StPO.

[141] Vgl *Aichinger*, Fahndungsmethoden 75.

des § 149d Abs 1 StPO zulässig ist. Durch die Verwendung der Phrase „außerhalb einer Wohnung oder sonstiger zum Hauswesen gehörende Räumlichkeit" sollen jene Räumlichkeiten erfaßt werden, die zwar grundsätzlich auch den Schutz des Hausrechtes genießen, weshalb eine Hausdurchsuchung in ihnen einer richterlicher Anordnung bedürfte, die jedoch – zumindest zu bestimmten Zeiten – öffentlich zugänglich sind (zB Gasthäuser, Wartezimmer von Arztordinationen).[142] Die Einrichtung einer „Videofalle" ist in der *Öffentlichkeit* zur Aufklärung jeder strafbaren Handlung, in *Räumlichkeiten* hingegen nur zur Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung und nur mit Zustimmung des Inhabers der Räumlichkeit zulässig. Damit soll der schon bisher kriminalistisch wertvolle Einsatz von Videogeräten – etwa zur Aufdeckung von Diebstählen in Garderoben – an rechtsstaatliche Bedingungen geknüpft werden.[143] Überwachungskameras in Banken, Bahnhöfen oder Tankstellenshops benötigen, sofern sie für jedermann erkennbar angebracht sind, keiner Anordnung nach diesen Bestimmungen.[144] Soll jedoch das Verhalten konkreter Personen überwacht werden, muß die Zustimmung des Inhabers der betreffenden Räumlichkeiten vorliegen, da das Recht auf Achtung der Geheimsphäre als absolutes Persönlichkeitsrecht Schutz gegen Eingriffe Dritter genießt und geheime Bildaufnahmen im Privatbereich, sowie fortdauernde unerwünschte Überwachungen, eine Verletzung dieser Geheimsphäre darstellen.[145]

Die Entscheidung der Überwachung obliegt im Fall der Videoüberwachung dem Untersuchungsrichter.[146] Auch hier gilt, daß eine Überwachung nur angeordnet werden darf, wenn der angestrebte Erfolg in einem vertretbaren *Verhältnis* zu den voraussichtlich bewirkten Eingriffen in Rechte Dritter steht. Zusätzlich ist im Sinne des Subsidiaritätsprinzips zu prüfen, ob nicht auch mit weniger eingriffsintensiven Mitteln begründete Aussicht auf Erfolg besteht. Insbesondere soll eine Überwachung in durch das Hausrecht geschützten Räumlichkeiten nur dann zulässig sein, wenn vernünftige Gründe für die Annahme sprechen, daß Mitglieder einer kriminellen Organisation an diesem Ort ihre kriminellen Aktivitäten besprechen werden und die zu erwartende

---

[142] Vgl EBRV 49 BlgNR 20. GP 20.

[143] Vgl JAB 812 BlgNR 20. GP 6.

[144] Vgl *Aichinger*, Fahndungsmethoden 76.

[145] Vgl *Miklau/Pilnacek*, Optische und akustische Überwachungsmaßnahmen zur Bekämpfung schwerer Organisierter Kriminalität („Lauschangriff") – Paradigmenwechsel im Verfahrensrecht? JRP 1997, 296.

[146] § 149e (1) StPO.

Verletzung der Geheimsphäre Unbeteiligter, die mit der Überwachung zwangsläufig verbunden ist, in einer vernünftigen Relation zu Bedeutung der Sache steht.[147]
In gleicher Weise wird eine Person, die selbst mit der Straftat wegen der die Überwachung angeordnet wird nichts zu tun hat, nicht allein deshalb umfassend überwacht werden können nur weil zu vermuten ist, daß ein Verdächtiger mit ihr in Kontakt treten werde. Dem Verhältnismäßigkeitsgrundsatz gemäß wird damit zum Ausdruck gebracht, daß die Rechte Dritter nur unter engen sachlichen und zeitlichen Voraussetzungen beeinträchtigt werden dürfen; dies jedoch auch nur dann, wenn die Aufklärung schwerwiegender Verbrechen ansonsten aussichtslos wäre.[148]

3.3.5. Abschließende Bemerkungen zum strafprozessualen Einsatz optischer und akustischer Überwachungsmethoden

Wie in jedem Fall verdeckter Ermittlung nach der Strafprozeßordnung steht auch der Lausch- und Spähangriff in einem Spannungsverhältnis zu § 25 StPO[149]: Den Sicherheitsbehörden, sowie den öffentlichen Beamten und Vertragsbediensteten, ist es untersagt, zur Gewinnung von Verdachtsmomenten, oder auf die Überführung des Verdächtigen, durch Verleitung zur Unternehmung, Fortsetzung oder Vollendung einer strafbaren Handlung hinzuwirken. Nicht nach dieser Bestimmung verboten ist jedoch die Überwachung, die nicht zu dem Zweck erfolgt, dem Verdächtigen ein Geständnis zu entlocken, sondern zur Gewinnung von Informationen, die anschließend die Grundlage für weitere Ermittlungen schaffen könnten.[150] Die bloße Videoüberwachung, die nicht von Scheinkäufen, etc begleitet wird, müßte also – auch wenn die Voraussetzungen des § 149d StPO nicht gegeben sind - erlaubt sein, da sie nicht von § 25 StPO erfaßt wird. Fraglich ist nur, ob durch § 25 StPO die Bestimmung des § 149d StPO eingeschränkt

---

[147] JAB 812 BlgNR 20. GP 6; *Miklau/Pilnacek*, Optische und akustische Überwachungsmaßnahmen zur Bekämpfung schwerer Organisierter Kriminalität („Lauschangriff“) – Paradigmenwechsel im Verfahrensrecht? JRP 1997, 297.

[148] Vgl *Fuchs*, Zum Entwurf eines Bundesgesetzes über besondere Ermittlungsmaßnahmen zur Bekämpfung Organisierter Kriminalität, StrPdGw, Bd 85 (1996) 277.

[149] Siehe dazu auch unten, 37.

[150] Vgl *Aichinger*, Fahndungsmethoden 64.

wird, oder umgekehrt. Die Regeln der materiellen Derogation[151] sind in diesem Fall nicht anwendbar, da an denselben Sachverhalt keine widersprüchlichen Rechtsfolgen geknüpft werden. Es spricht also vieles dafür, daß die Anwendung des § 149d StPO die Regelung des § 25 StPO in keiner Weise verletzt.[152]

So hat jene Regelung nach wie vor, auch angesichts eines geänderten Kriminalitätsfeldes, seine volle Berechtigung, da die rechtsstaatliche Grenze eines verdeckten Einsatzes da zu ziehen ist, wo § 25 StPO erst eingreift: Bei der staatlichen Provokation von Straftaten, die ein Rechtsstaat zum alleinigen Zweck der Sanktionierung der provozierten Tat keinesfalls zulassen sollte.[153] Geschieht dies dennoch, so besteht bei staatlicher Tatprovokation durch einen verdeckten Ermittler ein Strafausschließungsgrund besonderer Art entsprechend dem untauglichen Versuch, der nicht zu bestrafen ist.[154]

Auch läßt schon die Intention des Gesetzgebers, der mit der Einführung der besonderen Ermittlungsmaßnahmen in die StPO auf den Tatbestand der kriminellen Organisation (§ 278a StGB) aufbaute, den Schluß zu, daß solche Ermittlungen als schwerer Grundrechtseingriff nur auf schwerwiegende und außergewöhnliche Ziele ausgerichtet werden sollten, in der Praxis jedoch allzuoft Fälle gewöhnlicher Kriminalität, auch solche trivialen Zuschnitts treffen, für die sie weder bestimmt, noch erforderlich sind.[155]

Dies läßt den plausiblen Schluß zu, daß § 25 StPO zwar weiterhin volle Geltung hat, mit den besonderen Ermittlungsmaßnahmen wie sie § 149d StPO vorsieht jedoch eine Ausnahmeregelung geschaffen wurde, die *nur* unter den streng definierten Voraussetzungen auch verdeckte Ermittlungen zuläßt.

---

[151] „Lex posterior derogat legi priori“ und „lex specialis derogat legi generali“.

[152] Vgl das Beispiel bei *Aichinger*, Fahndungsmethoden 65. § 149d StPO gibt dem verdeckten Ermittler lediglich die Möglichkeit, das Gespräch aufzuzeichnen, sagt aber nichts über die inhaltliche Gestaltung desselben aus.

[153] Vgl *Unterwaditzer*, Zur Frage der „verdeckten Fahndung“, ÖJZ 1992, 255.

[154] Vgl *Fuchs*, Verdeckte Ermittler – anonyme Zeugen, ÖJZ 2001, 497.

[155] Vgl *Miklau/Pilnacek*, Optische und akustische Überwachungsmaßnahmen zur Bekämpfung schwerer Organisierter Kriminalität („Lauschangriff“) – Paradigmenwechsel im Verfahrensrecht? JRP 1997, 296.

3.4. „Lauschen" im Internet?

Zur Durchführung akustischer Überwachungen werden zumeist technische Hilfsmittel, wie beispielsweise „Wanzen", Richtmikrophone oder sonstige Abhörgeräte, die Töne über den natürlichen Klangumfang hinaus verstärken oder übertragen können, verwendet.[156]

Der Begriff des „Lauschens" an sich setzt also voraus, daß – im Unterschied zu verdeckten Ermittlungen im Internet, wo ja zumeist nur Bilder übertragen werden – der Inhalt einer Kommunikation oder Datenübertragung über ein Netzwerk akustisch wahrnehmbar gemacht werden müßte. Dies schließt einen Großteil der Bereiche der Internet-Kriminalität logischerweise aus. Nicht ausgeschlossen ist jedoch, daß entweder *unter Zuhilfenahme des Internet* beispielsweise ein Gespräch abgehört wird, oder aber, daß solche Gespräche überwacht werden, die *über das Internet* zwischen den Kommunikationsteilnehmern stattfinden. Ermöglicht wird eine solche Kommunikation durch telefonähnliche Konferenzschaltungen, die mit spezieller Software problemlos von jedem Homecomputer aus gesteuert werden können.

Als Beispiel sei hier die Software von „Real Networks"[157] angeführt: Die „Mutter" der effektiven digitalen Audio-Kompression (und bis heute für Sprachpräsentation unübertroffen) ist das 1996 eingeführte „Real Audio" Format, ein zeit-, bzw längenbezogenes Verfahren zur maximalen Reproduktion natürlicher Klänge bzw Schallereignisse.

Real Audio wird in Form von „*Streams*" und „*Clips*"[158] im Internet angeboten; solche Dateien können aber auch selbst erzeugt werden, und zwar durch Kompression unter Zuhilfenahme eines sog „Encoders", der auf zahlreichen WWW-Servern[159] zum freien Download angeboten wird. Als Anbieter von Internet-Dienstleistungen kann mit Real Audio ein kontinuierlicher Datenstrom generiert und ins Inter- bzw Intranet eingespeist

---

[156] *Nogala*, Polizei, avancierte Technik und soziale Kontrolle 49, zitiert nach *Aichinger*, Fahndungsmethoden 47.

[157] *http://www.real.com.*

[158] Unter einem „Stream" versteht man ein Audio-Format, das es ermöglicht, schon während der Übertragung abgespielt zu werden. Dadurch wird zB die Übertragung von Radio-Sendungen möglich. Im Unterschied dazu werden bei „Audio Clips" die Dateien komplett übertragen und erst dann gestartet (vgl *http://www.bhak-eisenstadt.at/unterlagen/www-kurs/gloss_s.htm#Streaming-Audio*).

[159] Beispielsweise unter *www.wolf-web.de/download/realplayer.htm; www.br-online.de/hilfe/player.html; www.brainside.de/German/RA_Download.html; www.foto.hgb-leipzig.de/fmp/download.realplayer.html.*

werden. Je nach Kompressionsgrad der zu übertragenden Dateien und der Datenübertragungsrate wird so ein weitgehend authentisches Klangbild erzeugt.[160]

Auf diese Art und Weise ist es also möglich, Gespräche, welche sich in großer Entfernung zur überwachenden Stelle befinden, beispielsweise mit Richtmikrophonen aufzunehmen, mittels der geeigneten Software in ein „Streaming"-Format umzuwandeln und über das Internet zu übertragen bzw im Internet abrufbar zu machen.[161] Ebenso besteht die Möglichkeit, Gespräche zwischen Kommunikationspartnern, welche mit Hilfe solcher Streaming-Audio Übertragungsgeräte im Internet geführt werden, abzufangen, zu übertragen und aufzuzeichnen.

Vor allem in jenen Fällen, die in den Anwendungsbereich des „kleinen Lauschangriffs" fallen, ist es denkbar, einen verdeckten Ermittler, welcher über entsprechendes technisches Wissen verfügt, in kriminelle Kreise einzuschleusen und so eine Übertragungsmöglichkeit für Gesprächsinhalte herzustellen. Dieser Fall einer Überwachung unterscheidet sich auch nicht vom Normalfall einer Kommunikation, da der Betroffene sich auf eine potentielle Indiskretion des Gesprächspartners einstellen und ihr somit mißtrauen muß.[162]

Zugegeben – diese Form einer akustischen Überwachung erscheint vom heutigen Standpunkt der Technik und in Relation des Aufwandes, welcher betrieben werden muß, um die faktischen Möglichkeiten eines solchen „Lauschangriffs" zu gewährleisten, noch einigermaßen konstruiert. Wenn aber neben den technischen Gegebenheiten auch die rechtlichen Voraussetzungen, welche ja bei solchen „transnationalen Überwachungen" keinesfalls immer gegeben sind, für solche Unternehmungen vorliegen, so könnte sich die Übertragung von Gesprächsinhalten über das Internet unter Zuhilfenahme dieser „Stream-Technologien" in nicht allzuferner Zukunft durchaus bewähren.

---

[160] Vgl *Näser*, Audio-Kompression mit Real *Audio*/ Real *Media* und anderen Verfahren, im Internet unter *http://staff-www.uni-marburg.de/~naeser/audio.htm.*

[161] Diese Methode wird vor allem dazu benutzt, um Musikkonzerte quasi „live" auch im Internet zu übertragen.

[162] Vgl *Gusy*/*Ziegler*, Menschenrechtsfragen elektronischer Personenüberwachung, ZRP 1996, 194.

3.5. Der „Web-basierte" Spähangriff

Auf Grundlage derselben „Streaming-Technologie", wie sie schon bei den Fällen des „Lauschens" im Internet beschrieben wurden, ist es auch möglich, unter Zuhilfenahme sog „Web-Cams", wie sie ja schon an vielen Orten der Welt[163] im Einsatz sind, Bilder aufzuzeichnen und zeitgleich im Internet zu übertragen. Eine Web-Cam ist eine Kamera, die mit Hilfe eines Computers in definierten Zeitintervallen digitalisierte Bilder auf einen Server überträgt, welche dann - idR für jedermann abrufbar -, im Internet öffentlich zur Verfügung stehen.[164]

Im konkreten Anwendungsbereich der StPO stellt also eine Überwachung mittels Web-Cams in den Fällen des § 149d (2) Z 1 – dh wenn sie zum Zweck der Aufklärung einer strafbaren Handlung außerhalb einer Wohnung oder sonstiger zum Hauswesen gehörender Räumlichkeiten erfolgt – eine wesentliche Erleichterung der Ermittlungsarbeit der Behörden dar. Das Internet bietet sich gerade zu solchen Zwecken der Datenübertragung an, da weder eine aufwendige Verkabelung des Sende- und Empfangsgerätes miteinander erfolgen muß und auch das Problem der geringen Reichweite von Funksignalen im Falle der „klassischen" kabellosen Datenübertragung umgangen werden kann. Es ist also möglich, beispielsweise in öffentlichen Tiefgaragen oder Parks, von denen man weiß, daß diese des öfteren Schauplätze strafbarer Handlungen darstellen, Kameras zu installieren. Es könnten somit regelmäßig Bilder über einen Server an einen ans Internet angeschlossenen PC des Ermittlers, der sich möglicherweise weit vom Ort der eigentlichen Überwachung entfernt befindet, gesendet werden.

Problematischer stellt sich die Situation im Falle der optischen Objektüberwachung iSd § 149d (2) Z 2 StPO dar: Rechtlich ist sie nur dann zulässig, wenn die Aufklärung einer vorsätzlich begangenen, mit mehr als einem Jahr Freiheitsstrafe bedrohten strafbaren Handlung ansonsten aussichtslos oder wesentlich erschwert wäre. Zwingend ist auch die Einwilligung des Inhabers der zu überwachenden Räumlichkeit vorgeschrieben. Innerhalb einer Wohnung ist es – im Unterschied zu öffentlichen Gebäuden und Anlagen - zweifellos schwieriger, erstens das nötige technische Gerät (Server, etc) so unterzubringen und zu verbergen, daß die zu überwachende Person keinen Verdacht

---

[163] Umfangreiche Linksammlungen zu Standorten von Web-Cams bieten zB die Adressen *http://www.livewebcam.com* oder *www.earthcam.com*.

[164] Vgl *http://a-z.wolf-web.de/w/webcam.htm.*

schöpft und zweitens überhaupt einen Internet-Zugang, der die nötige Übertragungsgeschwindigkeit gewährleistet,[165] vorzufinden.

Hier gilt also, daß die optische Objektüberwachung an öffentlichen Orten zweifelsohne leicht durchführbar ist, der Spähangriff in Wohnungen aber weiterer technischer Neuerungen zu seiner Durchführbarkeit bedarf. Speziell die Idee, etwa die Tätigkeit krimineller Verbindungen über Web-Kameras in privaten Räumlichkeiten überwachen zu können, wäre zwar praktisch durchaus interessant, ist derzeit aber wohl noch schwer realisierbar.

4. Die Problematik der „verdeckten Fahndung“

In Staaten wie den USA schon seit längerem erfolgreich durchgeführt, stellt sich die Frage, ob der Einsatz eines „verdeckten Ermittlers“ auch in Österreich rechtliche Deckung findet. In bezug auf im Internet begangene Delikte, im speziellen im Bereich der Kinderpornographie, wird schon seit längerer Zeit der Einsatz solcher „agent provocateurs“ vehement gefordert, um va die Arbeit der „Meldestelle für Kinderpornographie“[166] im Innenministerium wesentlich zu erleichtern.[167] Wesentliche Erfolge wurden mit dieser Ermittlungsmethode beispielsweise in Großbritannien erreicht, als die „Paedophile Unit“, eine Sondereinheit der britischen Polizei, durch umfassende verdeckte Ermittlungen im Januar 2001 einen landesweiten Ring von Kinderpornographie-Produzenten und –Konsumenten zerschlagen konnte.[168]

---

[165] Die schnellste Möglichkeit einer Verbindung mit dem Internet mit einem veralteten analogen Telefonanschluß liegt bei 56kb/s. Um eine flüssige Übertragung von Bildern zu garantieren, wäre ein ADSL-Anschluß mit bis zu 512kb/s von Vorteil.

[166] *Http://ln-inter1.bmi.gv.at/web/bmiwebp.nsf/AllPages/KP000131000185*.

[167] So ein Statement von Rudolf *Groß* von der Abteilung Gewalt und Sexualdelikte im Innenministerium abgegeben gegenüber der „ORF-Futurezone“ am 14.05.2001, im Internet unter *http://futurezone.orf.at/futurezone.orf?read=detail&id=66729&tmp=27340.*

[168] Vgl die Meldung von Telepolis, das Magazin für Netzkultur vom 18.01.2001, unter *http://www.heise.de/tp/deutsch/inhalt/te/4712/1.html*: „Seit 1999 laufende, verdeckte Ermittlungen führten...zu Hausdurchsuchungen bei 24 Adressen. 13 Verdächtige wurden verhaftet und 27 Computer beschlagnahmt, dazu große Mengen an Fotos, Videos und Magazinen. Es wird angenommen, daß ein

Aber auch im Bereich der Verfolgung von Delikten in Zusammenhang mit Softwarepiraterie[169] werden Ermittlungen immer öfter verdeckt durchgeführt. So wurden beispielsweise Vertrauensmänner der BSA[170] in öffentliche „Warez"[171]-Foren im IRC[172] eingeschleust, welche sich als Tauschpartner für raubkopierte Software ausgaben.[173] So wurde im Dezember des Jahres 2001 im Rahmen der „Operation Buccaneer"[174] in den USA, Kanada, Großbritannien, Australien, Finnland und Norwegen durch etwa 100 Durchsuchungsaktionen, denen umfangreiche verdeckte Ermittlungen vorangegangen waren, der bisher größte Schlag gegen den Vertrieb von raubkopierter Software über das Internet ausgeführt.[175]
Zu prüfen ist nun, ob der sicherheitspolizeiliche und/oder strafprozessuale Einsatz verdeckter Ermittlungsmethoden in Österreich rechtliche Deckung findet.

4.1. verdeckte Ermittlungen im Dienste der Sicherheitspolizei

Eine gesetzliche Grundlage für verdeckte Ermittlungen findet sich im Sicherheitspolizeigesetz: § 54 (1) iVm § 54 (3) SPG bestimmt, daß das Ermitteln personenbezogener Daten durch Einholen von Auskünften nur dann verdeckt erfolgen

---

Großteil des Materials den sexuellen Mißbrauch von Kindern zeigt und daß es sich zum Teil um Material besonders widerlicher Art handelt".

[169] Vgl ORF-Futurezone, „Mit neuen Tools gegen Softwarepiraten", im Internet unter *http://futurezone.orf.at/futurezone.orf?read=detail&id=37687&tmp=27527*.

[170] Business Software Alliance (BSA), eine Vereinigung zur Bekämpfung von Software-Piraterie, im Internet unter *http://www.bsa.com*.

[171] „Warez" ist ein Jargon-Ausdruck für raubkopierte Software.

[172] Der IRC (Internet Relay Chat) ist - neben seiner Hauptfunktion als Chatforum - einer der großen Distributionskanäle für Warez. Im IRC, das im Gegensatz zu webbasierten Chats auf eine jahrelange Tradition zurückblicken kann, tummeln sich in mehreren Servernetzen zigtausend User. In beliebten Warez-Kanälen befinden sich oft hunderte User gleichzeitig.

[173] Siehe dazu *Primig*, Softwarepiraterie 38 ff.

[174] Siehe dazu „Anklage gegen zwei Mitglieder der Warez-Szene", Heise Newsticker vom 24.01.2002, im Internet unter *http://www.heise.de/newsticker/data/anw-24.01.02-001/*.

[175] FBI-Agenten hatten in der Undercover-Aktion über ein Jahr lang Warez- und Cracker-Gruppen infiltriert und so 65 Verdächtige identifiziert. Bei den Durchsuchungen in Firmen, Privatwohnungen und Universitätsräumen in 27 US-Städten beschlagnahmten die Beamten zahlreiche Computer und Unterlagen - unter anderem auch in der Elite-Universität Massachusetts Institute of Technology.

darf, wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wäre. Da die „Kriminelle Verbindung“ als Voraussetzung verdeckter Ermittlungen sehr weit definiert ist,[176] und außerdem zur verdeckten Ermittlung der Verdacht einer solchen kriminellen Verbindung genügt, bietet das SPG einen sehr weiten Anwendungsbereich des geheimen Vorgehens.[177]

War nämlich vor der SPG-Novelle 2000[178] der Einsatz verdeckter Ermittler nur für die Abwehr gefährlicher Angriffe oder die Abwehr bandenmäßiger oder Organisierter Kriminalität vorgesehen,[179] so könnte durch die Neufassung dieser Bestimmung und die Einführung des Terminus „Kriminelle Verbindung“ nun auch in jenem Bereich der (Internet)-Kriminalität ermittelt werden, welcher zuvor nicht die „Kriterien“ organisierter Kriminalität erfüllte.

In Betracht kommen könnte vor allem die Zerschlagung von Distributionswegen für Kinderpornographie, indem sich behördliche Organe oder aber auch private Vertrauensleute[180] in Newsgroups oder Chat-Channels als Interessenten ausgeben. Ebenso könnten in Internet-Foren und Mailinglisten Anfragen bezüglich raubkopierter Software oder rechtsextremistischen Propagandamaterials gestellt werden.

Fraglich ist bei Schein- und Vertrauenskäufen aber, ob die Voraussetzungen einer „Kriminellen Verbindung“ in jedem Fall erfüllt sein werden, oder ob es sich bei derart zu verfolgenden Delikten bloß um solche, die von Einzelpersonen begangen werden, handelt, welche - vielleicht nicht einmal gewerbsmäßig - strafbaren Aktivitäten im Internet nachgehen. In einem solchen Fall, nämlich wenn keine kriminelle Verbindung vorliegt, ist der sicherheitspolizeiliche Einsatz verdeckter Ermittler nur zur

---

[176] Es genügt jede Verbindung von drei Menschen mit dem Vorsatz, fortgesetzt strafbare Handlungen zu begehen, welche mit mehr als einem Jahr Freiheitsstrafe bedroht sind (vgl § 16 (1) Z 2 SPG).

[177] Vgl *Fuchs*, Verdeckte Ermittler – anonyme Zeugen, ÖJZ 2001, 496.

[178] BGBl I 85/2000.

[179] Vgl § 54 (4) SPG alte Fassung.

[180] Privatpersonen, welche mit den Sicherheitsbehörden zusammenarbeiten und diesen Informationen zur Verfügung stellen, sind im SPG nicht vorgesehen; für die Verwertung ihrer Wahrnehmungen gilt nichts anderes als für jene amtlicher verdeckter Ermittler: Wenn sie Zeugen eines deliktischen Geschehens werden oder andere Wahrnehmungen machen, die den Täter einer strafbaren Handlung überführen können, sind sie wie alle Zeugen im Verfahren zu vernehmen. (vgl *Fuchs*, Verdeckte Ermittler – anonyme Zeugen, ÖJZ 2001, 496). Durch die Novelle 2002 zum SPG sollte es den Sicherheitsbehörden ermöglicht werden, sich bei ihren Ermittlungen auch „privater Vertrauensmänner“ zu bedienen.

Gefahrenabwehr vorgesehen; das Vorliegen eines „gefährlichen Angriffs“[181] als zweiter Bereich, in dem ein verdecktes Ermitteln gesetzlich geregelt ist, wird sich andererseits nur sehr schwer nachweisen lassen.

Mit der geplanten Novelle des SPG[182] soll ein neuer § 54 Abs 6 eingeführt werden, nach dem es den Sicherheitsbehörden gestattet werden soll, unter Mitwirkung von Personen, die *nicht Bedienstete einer Sicherheitsbehörde* sind, personenbezogene Daten zu ermitteln. Der Einsatz solcher „privaten Vertauensmänner“ soll jedoch nur unter den Voraussetzungen des § 54 (3) SPG zulässig sein, also nur dann, wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder wesentlich erschwert wäre. Ein Einschreiten eines Organs der Sicherheitsbehörde darf in einem solchen Fall weder möglich, noch erfolgversprechend sein.
Bereits bisher wurde weithin eine solche Vorgangsweise für zulässig erachtet und das Tätigwerden des Privaten der Sicherheitsbehörde zugerechnet, wenn dieser über Auftrag der Behörde eingeschritten ist. Dies vor allem deshalb, da immer wieder Fälle auftreten, in denen der Sicherheitsbehörde kein verdeckter Ermittler zur Verfügung steht, etwa bei Ermittlungen in einer bestimmten ethnischen Gruppe, oder wenn infolge der gebotenen Eile kein Ermittler für ein bestimmtes soziales Umfeld „aufgebaut“ werden kann.[183]
Diese neue Bestimmung kommt zweifellos auch jener „Spezialeinheit“ [184] beim österreichischen Bundeskriminalamt zugute, welche sich auf das Aufspüren illegaler Internet-Inhalte spezialisiert hat: War jene bislang selbst verpflichtet, allen einlangenden Anzeigen selbst nachzugehen und mit dieser Aufgabe oftmals überfordert, so trägt der Einsatz privater Vertauensleute im Rahmen der Vorgaben des SPG sicherlich wesentlich zur Aufklärung Internet-bezogener Straftaten bei.

---

[181] Vgl § 16 (2) (3) SPG.

[182] Vgl den Ministerialentwurf einer „SPG-Novelle 2002“ 312/ME 21. GP.

[183] Vgl die EB zum „ME-SPG 2002“ 26.

[184] Derzeit bearbeiten vier Kriminalbeamte die einlangenden Hinweise bezüglich kinderpornographischem Materials, welches im Internet verbreitet und zugänglich gemacht wird (vgl „Öffentliche Sicherheit“, das Magazin des Innenministeriums Nr. 6/2000, im Internet unter *http://ln-inter11.bmi.gv.at/web/bmiwebp.nsf/b75667aa383dc6ddc1256a9200429f31/c12566f800454cf1c125693e002efac1!OpenDocument*).

4.2. verdeckte Ermittlungen im Dienste der Strafrechtspflege

Im Geltungsbereich der StPO verbietet § 25 den Sicherheitsorganen, sowie allen öffentlichen Beamten und Vertragsbediensteten, „bei strengster Ahndung" auf die Gewinnung von Verdachtsgründen oder die Überführung eines Verdächtigen dadurch hinzuwirken, daß er zu einer strafbaren Handlung verleitet, oder durch insgeheim bestellte Personen zu Geständnissen verlockt wird.

Hinter diesem, seit 1873 geltenden Verbot, steht der Gedanke, daß der Einsatz solcher „agent provocateurs"[185] mit den Prinzipien eines liberalen Rechtsstaates nicht zu vereinbaren ist und der Staat nicht dazu da ist, Verbrechen zu provozieren, sondern allein dazu, solche zu verhindern. Dennoch erlangte der Einsatz verdeckter Fahndungsmethoden vor allem in Zusammenhang mit dem Ansteigen der Suchtgiftkriminalität praktische Bedeutung: „Lockspitzel" sollten dabei den Kontakt zu den Hintermännern des organisierten Drogenhandels herstellen, indem sie als Käufer großer Mengen von Rauschgift auftreten sollten.[186]

Problematisch in solchen Fällen ist jedoch, daß verdeckte Ermittler – „um nicht aufzufallen und nicht Kopf und Kragen zu riskieren"[187] – selbst gezwungen sind, bestimmte Straftaten zu, begehen. Dennoch erscheint es zweckmäßig, vor allem im Hinblick auf eine effiziente Bekämpfung schwerer organisierter Kriminalität, solche Maßnahmen einzusetzen und auch in der StPO zu verankern, um Straftäter zu überführen.[188]

Die oben[189] vorgestellte Regierungsvorlage zur Reform des strafprozessualen Vorverfahrens („Strafprozessreformgesetz") berücksichtigt die Problematik des verdeckten Ermittlers bereits:

---

[185] Im Unterschied zum „agent provocateur" handelt es sich bei „V-Leuten" um Personen, die keine Organe der Sicherheitsbehörden sind. Zuträger, Informanten und Konfidenten stehen außerhalb der Wahrnehmung von staatlichen Funktionen; sie sind selbständige Unternehmer und auf eigene Rechnung und Gefahr tätig (vgl *Funk*, Sicherheitspolizeiliche Maßnahmen zur Bekämpfung Organisierter Kriminalität, JRP 1996, 32).

[186] Vgl *Unterwaditzer*, Zur Frage der „verdeckten Fahndung", ÖJZ 1992, 250.

[187] *Hübner*, Das neue Instrumentarium gegen „OK", RZ 1999, 94.

[188] Vgl *Hauptmann*, Unkonventionelle Gedanken zu einem Strafrechtsänderungsgesetz 2000, in: Strafrechtliche Probleme der Gegenwart (1995) 13.

[189] Kap, 3.2.

§ 129 Z 2 StPORefG bestimmt, daß unter „verdeckter Ermittlung“ der Einsatz von kriminalpolizeilichen Organen oder anderen Personen im Auftrag der Kriminalpolizei, die ihre amtliche Stellung oder ihren Auftrag weder offen legen noch erkennen lassen, zu verstehen ist. Die einschlägigen Regelungen nach deutschem Recht[190] beziehen sich vor allem auf Beamte des Polizeidienstes, welche unter einer sog „Legende“ ermitteln, wobei der Ermittlungsauftrag über einige wenige Ermittlungshandlungen hinausgehen muß um eine Vielzahl von Personen über die wahre Identität des verdeckt ermittelnden Polizeibeamten zu täuschen. Die Definition des § 129 Z 2 StPORefG stellt hingegen darauf ab, daß die amtliche Stellung der eingesetzten Organe oder deren Auftrag für Außenstehende nicht erkennbar ist. Demnach wären auch solche Organe der Kriminalpolizei verdeckte Ermittler, die nur gelegentlich und ohne Legende verdeckt auftreten.[191]

Zulässig soll demnach die „einfache“ verdeckte Ermittlung - dh eine solche, die sich von üblichen Ermittlungen bloß darin unterscheidet, daß der amtliche Zweck nicht offen gelegt wird[192], in jenen Fällen sein, in denen sie zur Aufklärung einer Straftat „erforderlich erscheint“ (§ 131 Abs 1 StPORefG). Eine systematische, über längere Zeit durchgeführte verdeckte Ermittlung ist nur dann zulässig, wenn die Aufklärung einer vorsätzlich begangenen strafbaren Handlung, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, oder die Verhinderung einer im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) geplanten strafbaren Handlung ansonsten wesentlich erschwert wäre (§ 131 Abs 2 StPORefG).

Natürlich ist auch hier wiederum auf die Verhältnismäßigkeit der durchgeführten Maßnahmen zur möglichen Beeinträchtigung verfassungsgesetzlich gewährleisteter Rechte zu achten; neben erheblichen organisatorischen und finanziellen Vorkehrungen bedarf es daher strenger prozessualer Absicherungen, die den Einsatz verdeckter

---

[190] Vgl zur Lehre in Deutschland: *Kleinknecht*/*Meyer-Goßner*, Kommentar zur Strafprozeßordnung[44], § 110a Rz 1 ff.

[191] Vgl EBRV 1165 21. GP 180.

[192] EBRV 1165 21. GP 181.

Ermittler nur dann für zulässig erklären, wenn zur Aufklärung einer Straftat keine anderen erfolgversprechenden Mittel verfügbar sind.[193]

Es ist besonders im Bereich verdeckter Ermittlungen vom österreichischen Gesetzgeber eine Regelung zu fordern, welche die Voraussetzung solcher Fahndungsmethoden auch speziell in bezug auf die Internet-Kriminalität klar regelt. Denn während im Zusammenhang mit der Bekämpfung der organisierten Kriminalität zwar die Problemkreise um „Lauschangriff" und „Rasterfahndung" ausführlich erörtert und schließlich auch gesetzlich festgehalten wurden, erfuhr die Frage sicherheitsbehördlicher bzw strafprozessualer Erhebungen im Internet bisher eine nur spärliche Behandlung.[194]
Tatsache ist jedenfalls, daß in bestimmten Bereichen der Internet-Kriminalität - wie beispielsweise beim Handel mit Softwareraubkopien oder kinderpornographischem Material in Chat-Rooms, Internet-Foren, Mailinglisten oder Newsgroups - nur durch solche Ermittlungen, die verdeckt unter Angabe eines falschen Namens und unter Durchführung von Scheinkäufen erfolgen, auch effizient zur Kriminalitätsbekämpfung beigetragen werden kann. So ist es beispielweise der neuseeländischen Polizei gelungen, bei der Fahndung nach Pädokriminellen in „Chat-Rooms" und Newsgroups ein Programm zu entwickeln, welches der Behörde automatisch das Betreten eines Teilnehmers in eine einschlägige Diskussionsgruppe meldet. Bevor die Beamten auch nur beginnen, den Pädokriminellen in ein „Gespräch" zu verwickeln, wissen sie bereits, aus welchem Staat sich der Teilnehmer eingewählt hat. Mit einem einfachen Programm „schöpfen" die Fahnder dabei die IP-Adresse, von der aus der Observierte ins Web geht, ab. Wenn dieser über eine permanente IP-Adresse verfügt, sich also nicht via Modem

---

[193] Vgl *Dearing*, Kriminalpolizei und Strafprozeßreform. Konzept einer Arbeitsgruppe StPO-Reform des Bundesministeriums für Inneres zu einem sicherheitsbehördlichen Ermittlungsverfahren (Juristische Schriftenreihe Bd 84) (1995) 38.

[194] *Lindau*, Computerwelt Spezial, 1/1996, 3; zitiert nach *Wessely*, Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet, ÖJZ 1996, 612.

ins Internet einwählt, sondern einen Zugang über das Kabelnetz besitzt, ist es einfach[195], den Serverstandort und schließlich den Teilnehmer auszuforschen.[196]

5. Die Überwachung von Datentransfers im Internet

5.1. Allgemeines

Seit die potentielle Eignung des Internet als Hilfsmittel zur Begehung von Straftaten, Verstößen gegen Urheber-, Marken- und Wettbewerbsrechte[197] und generell der Verbreitung illegaler Inhalte erkannt wurde, suchte man nach Möglichkeiten, dies durch die Anwendung bestehender nationaler, oder die Schaffung international gültiger Rechtsakte zu unterbinden und eine Reglementierung des „Internet" oder spezieller Internet-Dienste zu erreichen.[198] Damit im Zusammenhang stehen auch Überwachungs-

---

[195] Die Möglichkeit, aufgrund der vorhandenen IP-Adresse Rückschlüsse auf den Endnutzer zu ziehen, bietet das Programm „Whois", welches auf zahlreichen WWW-Seiten gratis zum Download angeboten wird. Eine derartige Überprüfung kann auf manchen Homepages auch Online vorgenommen werden (zB unter *http://leader.ru/secure/who.html*).

[196] Vgl „Kinderpornographie – Automatisch erwischt", Der Spiegel Online vom 14.02.2002 unter *http://www.spiegel.de/netzwelt/technologie/0,1518,182180,00.html.*

[197] Vgl die zahlreichen Ausführungen zum Domainrecht, zur Haftung für Hyperlinks oder dem illegalen Download urheberrechtlich geschützter Dateien aus dem Internet unter *http://www.internet4jurists.at*, *http://www.it-law.at* oder *http://normative.zusammenhaenge.at*, allesamt mwN zu Literatur und Rechtsprechung auf diesem Gebiet.

[198] Daß es sich beim Internet keinesfalls um einen rechtsfreien Raum handelt, wurde durch die Lehre bereits ausführlich dargestellt (zB bei *Wenning*, Das Internet: Ein rechtsfreier Raum? JurPC 1995, 321; *Thiele*, Straftaten im Cyberspace - Zur Reichweite des österreichischen Internationalen Strafrechts, MR 4/98, 220; zu diesem Begriff siehe weiters *Brandl/Mayer-Schönberger*, Datenschutz und Internet, ecolex 1996, 132; *Spindler*, Deliktsrechtliche Haftung im Internet – nationale und internationale Rechtsprobleme, ZUM 1996, 563; *Jäger/Collardin*, Die Inhaltsverantwortlichkeit von Online-Diensten, CR 1996, 236; *Mayer*, Recht und Cyberspace, NJW 1996, 1789 f; *Sieber*, Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen – Zur Umsetzung von §5 TDG am Beispiel der Newsgroups des Internet, CR 10/1997, 582; *ders*, Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (2) – Neue Herausforderungen des Internet, JZ 10/1996, 494 ff; *Schmölzer*, Internet und Strafrecht, in: Strafrechtliche Probleme der Gegenwart, Schriftenreihe des BMJ (1997) 142).

und Kontrollmaßnahmen von Datentransfers in Computernetzen und deren rechtliche Zulässigkeit und faktische Durchführbarkeit.

In diesem Abschnitt der Arbeit sollen die Aktivitäten des österreichischen Gesetzgebers auf dem Gebiet der Kontrolle von Internet-Inhalten, als auch der Speicherung und Überprüfung von Kommunikation, welche über das Internet – beispielsweise per Electronic Mail – durchgeführt wird, einer näheren Betrachtung unterzogen werden. Dabei werden, ausgehend von einem kurzen Abriß der grundrechtlichen Problematik solcher Überwachungsmaßnahmen, sicherheitspolizeiliche und strafprozessuale Möglichkeiten einer derartigen Kontrolle erörtert und die bereits durchgeführten Anpassungen bestehender Normen an die Eigenheiten des Internet, sowie kürzlich verabschiedete, bzw sich noch in Vorbereitung befindliche, Rechtsakte zu diesem Themenkreis diskutiert.

5.2. Stammdaten, Vermittlungs- und Inhaltsdaten: Definition und Abgrenzung

In § 88 (3) TKG[199] wird festgehalten, daß das „Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen einer im Rahmen der Nutzung eines öffentlichen Telekommunikationsdienstes erfolgten Kommunikation, sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer“ unzulässig ist. Ausnahmen bestehen für die Aufzeichnung und Rückverfolgung von Telefongesprächen durch bestimmte Einrichtungen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung.

Weitere Ausnahmen bestehen auch in der Auskunftspflicht öffentlicher Telekommunikations-Dienstebetreiber gegenüber den Sicherheitsbehörden in den Anwendungsfällen des § 53 (3a) SPG[200], sowie in den Regelungen der Fernmeldeüberwachung der §§ 149a – d StPO[201].

---

[199] Bundesgesetz betreffend die Telekommunikation (Telekommunikationsgesetz - TKG), BGBl I 100/1997 idF 32/2002.

[200] Siehe dazu unten, 5.4.1.

[201] Vgl „Die strafprozessuale Fernmeldeüberwachung“, 5.5.

Einer genaueren Erörterung bedarf die Frage, welche Art von Daten für eine Überwachung der Kommunikation - oder allgemeiner – des Datenaustausches im Internet relevant sind:
Zieht man die Bestimmungen des Telekommunikationsgesetzes heran, so wird dort einerseits zwischen Inhaltsdaten und den „näheren Umständen der Kommunikation“[202], andererseits zwischen Inhalts-, Stamm- und Vermittlungsdaten unterschieden:

Unter „*Stammdaten*“ versteht das Gesetz alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter von Telekommunikationsdiensten oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind, wie beispielsweise Name, Anschrift oder Teilnehmehrnummer des Benutzers.[203] „*Vermittlungsdaten*“ oder „*äußere Gesprächsdaten*“ sind alle personenbezogenen Daten, die sich auf Teilnehmer und Benutzer beziehen und die für den Aufbau einer Verbindung oder für die Verrechnung von Entgelten erforderlich sind. Dazu gehören etwa Art, Datum, Zeitpunkt und Dauer der Verbindung und die übermittelte Datenmenge.[204] Als „*Inhaltsdaten*“ werden die Inhalte übertragener Nachrichten bezeichnet.[205] Diese Inhaltsdaten sind es auch, die in bezug auf eine Überwachung strafbarer Handlungen im Internet oder Netzwerken generell besonders relevant sind: Jede Überwachung eines Gesprächs in einem Chat-Room, jede Nachricht, die in einer (geschlossenen) Newsgroup postiert wird, oder in einer (privaten) Mailinglist aufscheint und nicht zuletzt auch jede E-Mail Nachricht, die - nicht für die Öffentlichkeit bestimmt - an einen Kommunikationspartner versandt wird, genießt besonderen Schutz.

5.3. Das Fernmeldegeheimnis - Schutzumfang und Eingriffsermächtigungen

Die im Zuge des Aufbaus einer Verbindung mit dem Internet entstehenden Informationen, wie auch der Inhalt der Kommunikation selbst, stehen unter dem

---

[202] § 88 (1) TKG.

[203] § 87 (3) Z 4 TKG.

[204] § 87 (3) Z 5 TKG.

[205] § 87 (3) Z 6 TKG.

verfassungsrechtlichen Schutz des Fernmeldegeheimnisses[206], des Schutzes des Privat- und Familienlebens[207], sowie des Grundrechtes auf Datenschutz[208]. Die Problematik va des grundrechtlichen Schutzes von Verbindungsdaten sei im Folgenden - auszugsweise[209] - wiedergegeben.

5.3.1. Art 10a StGG

> „Das Fernmeldegeheimnis darf nicht verletzt werden. Ausnahmen von der Bestimmung des vorstehenden Absatzes sind nur aufgrund eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig." (Art 10a StGG)

Diese Bestimmung schützt die Vertraulichkeit der auf einem bestimmten Kommunikationsweg übermittelten und nicht zur Kenntnisnahme durch Dritte[210] bestimmte Informationen. Die öffentliche Gewalt soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt des über Fernmeldeanlagen abgewickelten, mündlichen oder schriftlichen, Gedanken- und Informationsaustausches zu schaffen, dies unabhängig davon, ob ihr Inhalt Geheimnischarakter hat oder sich in allgemein bekannten Tatsachen erschöpft.[211]. Besonderen Schutz genießen nur solche Daten, die in dem Sinne geheim sind, als sie lediglich für eine oder wenige Personen außerhalb eines, eine geschlossenen Einheit bildenden, Personenkreises bestimmt sind.[212] Daten können einerseits aufgrund ihres Inhalts, oder aufgrund der Tatsache, daß diese Nachrichten in einer bestimmten Kommunikationssphäre übermittelt oder ausgetauscht werden, geheim sein. Für die Geltung des Fernmeldegeheimnisses gilt, daß

---

[206] Art 10a StGG (StGG 21.12.1867 über die allgemeinen Rechte der Staatsbürger, RGBl 1987/142 idF BGBl 8/1974).

[207] Art 8 MRK (BGBl 210/1958).

[208] Vgl die EBRV 1293 BlgNR 18. GP und § 1 DSG 2000 BGBl I 165/1999.

[209] Eine umfassende Erörterung dieses Problemkreises könnte wohl Grundlage mehrerer selbständiger Arbeiten sein.

[210] Vgl *Berka*, Lehrbuch Grundrechte: ein Arbeitsbuch für das juristische Studium mit Hinweisen zur grundrechtlichen Fallbearbeitung (2000) 112.

[211] *Wiederin*, Kommentierung von Art 10a StGG, in: *Korinek*/*Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht. Textsammlung und Kommentar, 4. Lieferung (2000) Rz 3.

[212] Vgl *Wessely*, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht, ÖJZ 1999, 492.

nicht der Inhalt einer Nachricht, sondern deren Bestimmung entscheidend ist;[213] der grundrechtliche Schutz des Fernmeldegeheimnisses ist insofern *abstrakt-formal*, als er sich auf alle mittels Fernmeldetechnik ausgetauschten Daten erstreckt.[214]

Art 10a StGG ist „Jedermannsrecht", sowohl der jeweilige Teilnehmer am Fernmeldeverkehr, als auch jeder Benutzer einer Fernmeldeanlage – mit Ausnahme des jeweiligen Gesprächspartners[215] - sind durch diese Bestimmung geschützt.[216]

Zu klären ist nun, ob auch der *Schutzumfang des Art 10a StGG* sich auf Vermittlungs- und Verbindungsdaten erstreckt, oder ob nur Inhaltsdaten davon erfaßt sind:

Folgt man der Ansicht eines Teiles der Lehre, sowie der Judikatur, so ist *außer Streit zu stellen*, daß auch Vermittlungsdaten dem Schutz des Fernmeldegeheimnisses nach Art 10a StGG unterliegen.[217]

Ansatzpunkte zur Bestimmung des Schutzumfanges können im Begriff des Fernmeldegeheimnisses selbst gesucht werden, welcher in der österreichischen Rechtsordnung schon vor dem Inkrafttreten des Art 10a StGG - nämlich im § 17 FernmeldeG[218] – seinen Niederschlag fand.

Nach Auffassung von *Wiederin*[219] gelte Art 10a StGG jedoch nur für *Inhaltsdaten*, da bei historischer Auslegung sich der Gegenstand des Fernmeldegeheimnisses auf die im Wege des Fernmeldeverkehrs übermittelten Nachrichten und Inhalte beziehe und es den Maßnahmen der rein technischen Überwachung am Eingriffscharakter mangle, da diese

---

[213] So unterliegen beispielsweise im Rundfunk verbreitete Nachrichten auch dann nicht dem Fernmeldegeheimnis, wenn es sich ihrem Inhalt nach um geheime Nachrichten oder Meldungen handelt (vgl *Wessely*, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht, ÖJZ 1999, 492); für Rundfunksendungen besteht somit kein Schutz nach Art 10a StGG (vgl JAB 960 BlgNR 13. GP 2); siehe zu dieser Thematik auch *Korinek*, Die Gewährleistung von Kommunikationsfreiheit im österreichischen Rundfunkrecht, in: *Raschauer* (Hrsg), Grundrechte und Verfassungsgerichtsbarkeit (2000) 197.

[214] Vgl *Wiederin*, Grundrechte, Art 10a StGG Rz 3.

[215] *Brandstetter*, Die Fernmeldeüberwachung öffentlicher Telefonzellen, JBl 1984, 476.

[216] *Wiederin*, Grundrechte, Art 10a StGG Rz 10.

[217] Vgl *Schmölzer*, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr – Anmerkungen zu OGH 6.12.1995, 13 Os 161/95, JBl 1997, 214; *dies*, Cyberstructure: Die „Fangschaltung", Juridikum 1997, 43, 46; *Schmölzer/Mayer-Schönberger*, Das Telekommunikationsgesetz 1997 – Ausgewählte rechtliche Probleme, ÖJZ 1998, 383; Reindl, Telefonüberwachung zweimal neu? JBl 2002, 71; OGH 06.12.1995, 13 Os 161/95, JBl 1997, 260; OGH 18.01.2001, 12 Os 152/00, JBl 2001, 531 (*Burgstaller*) = EvBl 1998/191.

[218] Vgl auch die Nachfolgebestimmung des § 88 TKG.

[219] *Wiederin*, Grundrechte, Art 10a StGG Rz 12.

teilweise völkerrechtlich geboten seien und weil ohne diese ein funktionierender Fernmeldeverkehr nicht möglich sei.[220] Außerdem sei durch die konkrete Fassung des § 119 StGB die Ausforschung äußerer Gesprächsdaten vom Tatbestand nicht erfaßt; diese Beschränkung des *strafrechtlichen Fernmeldegeheimnisschutzes* sei auch grundrechtlich von Relevanz.

Auch nach *Wessely*[221] divergierere nach der Intention des historischen Gesetzgebers der Begriffsinhalt des Fernmeldegeheimnisses nach Art 10 StGG mit jenem des Fernmelde- bzw Telekommunikationsgesetzes[222]: Während sich nämlich das Fernmeldegeheimnis nach dem TKG als besondere Geheimhaltungsverpflichtung darstelle, die *neben* die Amtsverschwiegenheit trete, sei gerade letztere das Ziel des TKG. Gegenstand des Fernmeldegeheimnisses wären demnach bestimmte Nachrichten – genauer: Kommunikations*inhalte* – folglich also Inhaltsdaten. Diese Meinung wird auch durch das Argument unterstrichen, daß der Schutz des Briefgeheimnisses sich auch ausschließlich auf den *Inhalt* verschlossener Briefe bezieht, nicht aber auf die Tatsache der Sendung oder die Identität des Absenders. Wenn also Maßnamen technischer Überwachung keinen Eingriff in das Fernmeldegeheimnis darstellten, so bedeute dies, daß die zu diesen Zwecken erforderlichen Daten (*Vermittlungs- oder Verbindungsdaten*) nicht dem Schutz des Fernmeldegeheimnisses unterliegen.[223]

Als besonders problematisch im Lichte dieser Diskussion stellt sich die Frage, ob die *Fangschaltungsregelung* des § 100 TKG einen Eingriff in den Schutzbereich des Art 10a StGG darstellt, da eine solche zur Durchführung einer richterlichen Genehmigung expressis verbis nicht bedarf.

5.3.1.1. Zum grundrechtlichen Schutz von „Fangschaltungsdaten"

Eine Fangschaltung ist die vom Willen des Anrufenden unabhängige Feststellung der Identität eines anrufenden Anschlusses. Es sollen damit Urheber belästigender Anrufe leichter ausgeforscht werden können.[224] Das Ergebnis der Fangschaltung wird dem

---

[220] An dieser Stelle verweist *Wiederin* auf die Ansicht des Justizausschusses (JAB 960 BlgNR 13. Gp 2).

[221] *Wessely*, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht, ÖJZ 1999, 493.

[222] Dazu sogleich unten, 5.3.1.1.

[223] *Wessely*, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht, ÖJZ 1999, 493.

[224] Vgl *Mayer-Schönberger/Brandl*, Telekommunikationsgesetz und Datenschutz, ecolex 1998, 273.

Teilnehmer mitgeteilt und jener hat die Möglichkeit, selbst darüber zu entscheiden, in welcher Form die Verfolgung des Täters erfolgen soll. Damit wird es ermöglicht, Fälle der Belästigung, die auch ohne ein behördliches Verfahren gelöst werden können, zu berücksichtigen.[225]

Dem *Fernmeldegeheimnis* unterliegen nach den Bestimmungen des Telekommunikationsgesetzes[226] die Inhaltsdaten und die näheren Umstände der Kommunikation, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die *näheren Umstände erfolgloser Verbindungsversuche.*

Während die Überwachung des Fernmeldeverkehrs im Dienste der Strafrechtspflege auf Kenntnisnahme künftiger Inhalts- oder Vermittlungsdaten gerichtet ist, stellt die Fangschaltungsregelung des Telekommunikationsgesetzes eine technische Möglichkeit dar, außerhalb eines Strafverfahrens die Identität eines anrufenden Anschlusses zu erforschen.[227]

Spricht man jetzt auch *Vermittlungsdaten*, die ja den wesentlichen Teil der im Rahmen einer Fangschaltung ermittelten Daten ausmachen, den vollen Schutz des Fernmeldegeheimnisses zu, so würde mit der Regelung des § 100 TKG eben jener grundrechtliche Schutz, den Art 10a StGG auch Vermittlungsdaten gewährt, umgangen werden, da für eine Weitergabe solcher Daten eine *richterliche Genehmigung* notwendig wäre. Die Fangschaltungsregelung des § 100 TKG wäre somit grundrechtswidrig.[228]

Man könnte zunächst, so *Wessely*[229], davon ausgehen, daß die Fangschaltung lediglich Vermittlungsdaten betrifft, sodaß der Schluß naheliege, die formell geringeren Voraussetzungen des Art 8 Abs 2 MRK[230] für einen Eingriff genügen zu lassen. Gerade im Falle der Rufnummernanzeige erscheine diese Zuordnung jedoch zweifelhaft, da sich die übermittelte Rufnummer als Teil der übermittelten Information, sohin als

---

[225] Vgl EBRV 759 BlgNR 20. GP Anm zu § 100 TKG.

[226] § 88 (1) TKG.

[227] Vgl *Schmölzer/Mayer-Schönberger*, Das Telekommunikationsgesetz 1997 – Ausgewählte rechtliche Probleme, ÖJZ 1998, 383.

[228] Kritisiert (*Schmölzer/Mayer-Schönberger*, aaO, 385) wurde auch, daß das TKG keine Vorgaben dahingehend liefert, was unter einem „belästigenden Anruf" zu verstehen ist und wer über das Vorliegen eines solchen entscheidet.

[229] *Wessely*, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht, ÖJZ 1999, 496.

[230] Siehe dazu unten, 5.3.2.

Inhaltsdatum darstelle und hinsichtlich der Eingriffsermächtigung der § 100 TKG der Gesetzesvorbehalt des Art 10a StGG einschlägig wäre. Bietet aber der Eingriffsvorbehalt keine geeignete Grundlage für eine Fangschaltung, so könne diese nur dann als verfassungskonform betrachtet werden, wenn die Beteiligten selbst den Kommunikationsvorgang offenlegen oder aber Dritte[231] in dessen Erfassung einwilligen würden. Tatsächlich aber seien Fangschaltungsmaßnahmen dadurch charakterisiert, daß nur der – die Fangschaltung beantragende – Teilnehmer in eine Datenerfassung einwillige, die anderen jedoch in Unkenntnis des Vorganges gehalten würden und somit in die Preisgabe der eigenen Rufnummer gar nicht einwilligen könnten; Grundrechtskonformität könne dann nur durch eine richterliche Genehmigungspflicht von Fangschaltungen hergestellt werden.[232]

Den gegensätzlichen Standpunkt, nämlich daß Fangschaltungsdaten *nicht* dem Schutzbereich des Art 10a StGG unterliegen, vertritt *Wiederin*[233] und begründet dies wie folgt: Es sprächen bei einer Fangschaltung die besseren Gründe dafür, nicht die technische Seite für entscheidend zu halten, sondern darauf abzustellen, was herkömmlicherweise als Inhalt der zu übertragenden Nachrichten betrachtet wird. Vermittlungsdaten gem § 87 Abs 1 Z 5 TKG würden deshalb nicht dazuzählen, da sie als technische Daten über eine Kommunikation eine „*Metaebene*“ beträfen. Gegen einen Eingriff in Art 10a StGG spräche zudem, daß die mitübertragene Anschlußnummer in eben jenen Konstellationen, in welchen die Fangschaltung notwendig wird, gerade nicht zur Kenntnisnahme durch den Kommunikationspartner bestimmt ist, es also an einer *Vertrauensbeziehung* zwischen den Teilnehmern mangle.

Als wesentlich plausibler stellt sich die Ansicht von *Schmölzer*[234]dar, die vorerst festhält, daß die adäquate *Eingriffsermächtigung* für den Bereich des verfassungsgesetzlich geschützten Fernmeldegeheimnisses de lege lata ausschließlich in den Bestimmungen zur *Überwachung eines Fernmeldeverkehrs* nach §§ 149a ff StPO zu sehen sei und ein Vergleich mit der Regelung des § 100 TKG schon auf der Basis der

---

[231] Vgl zum Problem des „abgehörten Dritten“ ausführlich *Davy*/*Davy*, Staatliche Informationssammlung und Art 8 MRK, JBl 1985, 657 ff.

[232] *Wessely*, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht, ÖJZ 1999, 497.

[233] *Wiederin*, Grundrechte, Art 10a StGG Rz 13.

[234] *Schmölzer*, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr – Anmerkungen zu OGH 6.12.1995, 13 Os 161/95, JBl 1997, 214 f; *dies*, Cyberstructure: Die „Fangschaltung“, Juridikum 1997, 43, 46; *Schmölzer/Mayer-Schönberger*, Das Telekommunikationsgesetz 1997 – Ausgewählte rechtliche Probleme, ÖJZ 1998, 384 ff.

technischen Prämissen insofern unrichtig sei, als die Vorgangsweise bei letzterer sich als völlig anders darstelle: Es handle sich bei einer Fangschaltung lediglich um eine elektronisch gesteuerte *Überprüfung* vorhandenen Datenmaterials und nicht um eine *Überwachung*, die nur Vorgänge erfassen könne, welche gerade ablaufen. Durch die Formulierung des § 88 TKG, die auf „Inhaltsdaten und die näheren Umstände der Kommunikation, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war" abstellt, würden äußere Gesprächsdaten *im weiteren Sinn* vom engen und zweckbezogenen Begriff der Vermittlungsdaten gelöst, in einen weiteren Kontext gestellt und unterlägen explizit dem verfassungsrechtlichen Schutz des Fernmeldegeheimnisses nach Art 10a StGG. Die sachlich nicht gerechtfertigte Differenzierung zwischen Vermittlungsdaten ieS, die Grundrechtsschutz genießen, und solchen iwS, wie zB „Fangschaltungsdaten", sei also durch diese Bestimmung gefallen. Das Problem des Richtervorbehalts, der auch bei der Fangschaltung zu berücksichtigen wäre und unter dem eine Einschränkung des Art 10a StGG steht, sei dadurch jedoch nicht gelöst worden. Die Regelung des Art 100 TKG ist also auch nach dieser Ansicht letztendlich verfassungswidrig.

Mit dem „Strafrechtsänderungsgesetz 2002"[235] wurde eine Anpassung der Strafprozeßordnung an die Bestimmungen und Begriffe des TKG vorgenommen, die angesichts der engen Verknüpfung dieser beiden Gesetze in bezug auf die Fernmeldeüberwachung schon längst überfällig war. So wird in § 149 a Abs 1 Z 1 lit b die Rufdatenrückerfassung, also „die Feststellung, welche Teilnehmeranschlüsse Ursprung oder Ziel einer Telekommunikation sind oder waren" einer ausdrücklichen Regelung unterzogen und von der Voraussetzung einer richterlichen Anordnung abhängig gemacht.[236] Im Gegensatz dazu wurde die Fangschaltungsregelung des § 100 TKG jedoch nicht geändert; eine richterliche Anordnung von Fangschaltungen ist zur Durchführung derselben weiterhin nicht vonnöten.

---

[235] Siehe dazu unten, 5.5.2.2.

[236] Zur Rufdatenrückerfassung vgl unten, 5.5.1.1.

5.3.2. Art 8 MRK

Das Grundrecht des Art 8 Abs 1 MRK verbürgt jedermann den „Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs". Beschränkt wird dieses Recht durch den Gesetzesvorbehalt in Art 8 Abs 2 MRK, wonach der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts nur statthaft ist, wenn dieser Eingriff gesetzlich vorgesehen, notwendig und verhältnismäßig ist.

Dabei schließt die Formulierung „Achtung des Briefverkehrs" die Kommunikation via Telefon[237] und Internet mit ein.[238] MRK und StGG können nebeneinander zur Anwendung gelangen, wobei jedoch der Schutzumfang des Art 8 Abs 1 MRK über jenen des Art 10a StGG hinausgeht, da – neben dem heimlichen Aufzeichnen von Gesprächsinhalten[239] - auch die Aufzeichnung äußerer Gesprächsdaten von ersterem erfaßt wird.[240] Die Bewilligung des Eingriffs durch eine richterliche Anordnung ist gem Art 8 Abs 2 MRK insoweit verfassungsrechtliches Erfordernis, als ohne sie die betreffende Maßnahme nicht als „in einer demokratischen Gesellschaft erforderlich" qualifiziert werden kann.[241] Eine Offenlegung und Auswertung von Vermittlungsdaten ist daher nur zulässig, wenn eine gesetzliche Eingriffsgrundlage im innerstaatlichen Recht besteht, die Maßnahme zudem notwendig und verhältnismäßig ist.[242]

5.3.3. Schlußbemerkung

Der grenzüberschreitende Transfer von Daten macht das Einhalten von Grundrechts- und Datenschutzkonzepten schwierig; hier ist der Staat als „Gewährleister" der

---

[237] EGMR 6.9.1978, Klass, EuGRZ 1975, 278; der EGMR betonte diesbezüglich, daß die Befugnisse zur geheimen Überwachung von Bürgern, wie sie für einen Polizeistaat typisch sind, in einer demokratischen Gesellschaft nur in außergewöhnlichen Situationen zulässig sein können. (siehe dazu die Erläuterungen bei *Davy/Davy*, Aspekte staatlicher Informationssammlung und Art 8 MRK, JBl 1985, 658).

[238] Vgl *Wiederin*, Grundrechte, Art 10a StGG Rz 26.

[239] *Berka*, Grundrechte 112.

[240] EGMR 2.8.1984, Malone, EuGRZ 1985, 17.

[241] *Wiederin*, Grundrechte, Art 10a StGG Rz 26.

[242] Vgl mwN zur Judikatur des EuGH: *Reindl*, Nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren, JBl 1999, 795.

Grundrechte gefragt und muß sich der Tatsache stellen, daß die traditionellen Grundrechte auf moderne Medien oft nur deshalb nicht anwendbar sind, da die diesbezüglichen Bestimmungen in ihrem Wortlaut zu eng formuliert sind. Dem Bürger muß die Möglichkeit gegeben werden, sich gegen Einbrüche in seine Privatsphäre im Zusammenhang mit neuen Technologien zu wehren. Dazu gehört auch die Schaffung von Regelungen, die Abwehrmaßnahmen gegen solche Eingriffe bieten.[243] So wäre zumindest eine begriffliche Ausdehnung zB der Termini „Fernmeldegeheimnis" oder „Fernmeldeverkehr" im Hinblick auf die Erfassung des gesamten Telekommunikationsverkehrs, welcher auch alle Formen der Kommunikation im Internet einschließt, vonnöten.

5.3.4. Beschränkung der Verarbeitung kundenbezogener Daten durch das TKG

Es finden sich aber auch im Telekommunikationsgesetz Bestimmungen, die – neben den Bestimmungen zum Fernmeldegeheimnis und jenen des Datenschutzes im Allgemeinen – einer mißbräuchlichen Verwendung kundenspezifischer Daten seitens des *Providers* vorbeugen sollen:

All jene Daten, welche bei einer Aufnahme der Verbindung mit dem Internet anfallen, werden beim Provider, der ja einen solchen Netzzugang ermöglicht, für einen bestimmten Zeitraum – und seien es nur für einige Augenblicke – gespeichert. Dieser verwaltet nicht nur die *Stammdaten* seiner Kunden, sondern auch Daten darüber, wann, wie oft und wie lange ein Kunde die Verbindung mit dem Internet aufrechterhält, ja sogar erfolglose Verbindungsversuche werden gespeichert (*Vermittlungs-* oder *Verbindungsdaten*). Schließlich verwaltet der Provider auch die Inhalte der übertragenen Nachrichten, also auch *Inhaltsdaten*. Der Provider hat also Kenntnis darüber, wo und wie lange der Kunde sich im Internet aufgehalten hat, an wen er E-Mails versendet hat und welche Nachrichten er aus welchen Newsgroups abgerufen hat. Auch im Falle von verschlüsselten Sendungen ist er in der Lage, die gesamte elektronische Post zu lesen.[244]

---

[243] Vgl *Höne*, Grundrechte im Internet, in: ÖJK (Hrsg), Grundrechte in der Informationsgesellschaft (2001) 88.

[244] Vgl *Zanger*, Telekommunikationsgesetz: Kommentar (2000) § 91 Rz 30.

Grundsätzlich dürfen Stamm-, Vermittlungs- und Inhaltsdaten nur für Zwecke der Besorgung eines Telekommunikationsdienstes ermittelt oder verarbeitet werden (§ 91 Abs 1 TKG). *Vermittlungsdaten* dürfen *überhaupt nicht* gespeichert werden und sind vom Provider nach Beendigung der Verbindung zu löschen oder zu anonymisieren (§ 93 Abs 1 TKG). Ausnahmen bestehen nur, sofern dies für Zwecke der Verrechnung von Entgelten erforderlich ist (§ 93 Abs TKG).

Nur Personen, die auch die Besorgung des Telekommunikationsdienstes selbst vornehmen, dürfen solche Vermittlungsdaten verarbeiten; jene dürfen somit auch nicht an Dritte weitergeben werden, es sei denn, diese führen auch Telekommunikationsdienstleistungen durch und benötigen solche Daten, etwa um eine Verbindung zu einem nichtöffentlichen Server herzustellen oder im Falle des „Outsourcing“ [245] von Dienstleistungen.

Inhaltsdaten dürfen ebenfalls grundsätzlich *nicht gespeichert* werden, außer die Speicherung stellt einen wesentlichen Bestandteil des Telekommunikationsunternehmens dar. Nach Erbringung des Dienstes sind die Daten zu löschen (§ 95 TKG).

5.4. Fernmelde- und Telekommunikationsüberwachung im SPG

Durch den Verweis des § 54 (4) SPG auf das Fernmeldegeheimnis wird klargestellt, daß diese Regelung keine Ermächtigung zur „Telefonüberwachung“ bzw zum „Telefonabhören“ bildet.[246]

Eine sicherheitspolizeiliche Überwachung des Fernmeldeverkehrs, wie sie im Bereich der Strafverfolgung im § 149a StPO verankert ist, ist im SPG nicht vorgesehen, wird aber verschiedentlich als Mittel der vorbeugenden Gefahrenabwehr gefordert.[247]

Im Falle eines kriminalpolizeilichen Auskunftsverlangens im Dienste der Strafrechtspflege ist die Rechtsgrundlage im § 149a StPO iVm den Bestimmungen des Telekommunikationsgesetzes (§ 87 (2), § 96 (7) TKG) zu sehen.[248]

---

[245] Vgl *Mayer-Schönberger/Brandl*, Telekommunikationsgesetz und Datenschutz, ecolex 1998, 273.

[246] *Hauer/Keplinger*, Sicherheitspolizeigesetz[2], § 54 B.11.

[247] *Funk*, Sicherheitspolizeiliche Maßnahmen zur Bekämpfung Organisierter Kriminalität, JRP 1996, 33 f.

[248] *Trawnicek/Lepuschitz*, Sicherheitspolizeigesetz[3], 239.

5.4.1. Befugnisse der Sicherheitsbehörden nach § 53 Abs 3a SPG

Durch die Novelle 1999des SPG[249] wurde Abs 3a in den § 53 SPG, welcher die Berechtigung der Sicherheitsbehörden beinhaltet, von den Betreibern öffentlicher Telekommunikationsdienste[250] unter bestimmten Voraussetzungen Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, eingefügt. Dies war deshalb notwendig geworden, da die Sicherheitsbehörden bis zur Privatisierung der PTV unter Berufung auf Amtshilfe iSd B-VG Auskünfte über Telefonnummern und Stammdaten[251] erhalten konnten. Eine ausreichende Grundlage für derartige Auskünfte außerhalb des Fernmeldegeheimnisses stellte § 53 (3) SPG dar; mit dem Wegfall dieser gesetzlichen Grundlage waren die Sicherheitsbehörden auf den Good-Will der Betreiber angewiesen, wenn sie derartige Auskünfte erlangen wollten. Vor allem in jenen Fällen, die eine unverzügliche Beendigung eines gefährlichen Angriffs erfordern - wie beispielsweise eine telefonische Bombendrohung oder die Ankündigung eines Terroranschlags – wäre eine solche Abhängigkeit jedoch undenkbar.

Durch die neue Bestimmung sollen nunmehr jene Stellen, die über Stamm- oder Vermittlungsdaten iSd TGK verfügen, dazu verpflichtet werden, den Sicherheitsbehörden Auskunft über Name, Adresse oder Teilnehmernummer zu erteilen. Eine solche Auskunft stellt keinen Eingriff in das Fernmeldegeheimnis gem Art 10a StGG dar.[252]

Gemäß Erlaß des BMI[253] steht den Sicherheitsbehörden nach § 53 (3a) SPG der Zugang zu folgenden Informationen offen:

Zur Erfüllung sicherheitspolizeilicher Aufgaben:

---

[249] BGBl I 146/1999.

[250] Vgl § 3 Z 14 TKG: Telekommunikationsdienst stellt „...eine gewerbliche Dienstleistung, die in der Übertragung und/oder Weiterleitung von Signalen auf Telekommunikationsnetzen besteht, einschließlich des Angebotes von Mietleitungen...“ dar.

[251] Vgl § 87 (3) Z 4 TKG.

[252] Vgl EBRV 1479 BlgNR 20. GP 20.

[253] Erlaß des BMI vom 21.12.1999, Zl 61.183/279-II/20/99.

- zu einem der Sicherheitsbehörde bekannten Menschen die Mitteilung seiner Teilnehmernummer(n);
- zu einer der Sicherheitsbehörde bekannten Teilnehmernummer die Mitteilung des Namens und der Anschrift des Inhabers dieses Anschlusses.

Nur zur Erfüllung der *ersten allgemeinen Hilfeleistungspflicht* und zur Abwehr *gefährlicher Angriffe*:

- zu einem zu einer bestimmten Zeit bei einem bestimmten Teilnehmer eingegangenen Rufkontakt die Mitteilung, von welchem Anschluß aus der Anruf erfolgt und welcher Person dieser Anschluß zugeordnet ist.

Für die Begründung der Auskunftspflicht gem § 53 (3a) genügt es, wenn die Sicherheitsbehörden den zu identifizierenden Anschluß durch einen bestimmten Zeitpunkt und die „passive Teilnehmernummer", also die Telefonnummer des Angerufenen, präzisieren. Dies gilt allerdings nur, wenn es sich um die Erfüllung einer der beiden besonders wichtigen sicherheitspolizeilichen Aufgaben der ersten allgemeinen Hilfeleistungspflicht (§ 19 SPG) oder der Abwehr gefährlicher Angriffe (21 SPG), nicht aber wenn es sich bloß um die Aufrechterhaltung der öffentlichen Ordnung (§ 27 SPG) handelt. § 53 (3a) SPG ermöglicht damit auch die nachträgliche Rufdatenerfassung im Dienste der Sicherheitspolizei.[254]
Gem § 53 (3a) letzter Satz ist „die ersuchte Stelle verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen". Diese Bestimmung stieß bei ihrer Einfügung ins SPG vor allem auf Kritik[255] von Seiten der Telekommunkationsdiensteanbieter. Diese wiesen darauf hin, daß die Ermittlung der Vermittlungsdaten einen immensen technischen und finanziellen Aufwand darstelle, der nicht administrierbar sei.[256]
Aber auch von anderer Seite wurde argumentiert, daß die Notwendigkeit der Abwehr beispielsweise eines unmittelbar bevorstehenden Bombenattentates auf eine Schule

---

[254] *Hauer/Keplinger*, Sicherheitspolizeigesetz[2], § 53 B.8.3. f.

[255] Vgl die Stellungnahme der „Telekom Austria" zum Ministerialentwurf der SPG-Novelle 1998 (307/ME 20. GP) 2.

[256] AM *Dearing*, Sicherheitspolizeigesetz (1999) 91, welcher der Ansicht ist, daß „die Erfüllung dieser Übermittlungspflicht...die Betreiber der öffentlichen Telekommunikationsdienste nur mit geringfügigen Kosten belasten (wird,)[...]eine Verpflichtung zur kostenlosen Auskunftserteilung in wirtschaftlicher Hinsicht (somit) zumutbar (ist)".

zwar unbestritten sei, dieser Ausnahmefall allerdings nicht dazu mißbraucht werden dürfe, über Auskunftsbegehren gegenüber Telefonanbietern unverhältnismäßig in Grundrechte aller Bürger einzugreifen. Die Weitergabe nicht nur von Stamm-, sondern vor allem von Vermittlungsdaten sei ein Eingriff in das verfassungsrechtlich geschützte Fernmeldegeheimnis[257]. Außerdem würden die Auskünfte über Vermittlungsdaten nicht nur Namen und Anschrift eines Anschlusses erfassen, sondern – im Falle befürchteter gefährlicher Angriffe – auch Auskünfte über äußere Rufdaten (wer hat, von welchem Anschluß aus, wann und mit welchen Anschlüssen Telefongespräche geführt?). Das allerdings wäre ein gravierender Eingriff in das Privatleben (Art 8 MRK) und das Grundrecht auf Datenschutz (§ 1 Abs 1 DSG 2000), da man dadurch den Aufenthaltsort von Gesprächspartnern ableiten könne.[258]

Daß aber die Überwachung des Internet-Traffic *zur Gefahrenabwehr* ein notwendiges Instrument sein könnte, welches vor allem im Zeitalter modernen Kommunikation via Internet seine Berechtigung hätte, zeigt die Zeitschrift „Der Spiegel“ anhand eines drastischen Beispieles auf[259]:

„Unbemerkt drangen die Dunkelmänner aus dem Fernen Osten in 34 Computernetze des Pentagon ein und sorgten mit falschen Befehlen für Chaos: Ein Tankwagen mit Flugbenzin wurde zum nächsten Marine-Stützpunkt dirigiert. Vergebens wartete eine F-16 Kampfflugzeugstaffel auf neue Raketen; geliefert wurde statt dessen eine Ladung LKW-Lampen. Mehr als robuste Kaufhaus-Computer und erprobter Gratis-Software aus dem Internet brauchten die 35 „Cyber-Soldaten“ nicht, um die Supermacht USA erfolgreich zu attackieren.“

Man könnte einerseits der Einführung einer sicherheitspolizeilichen Telekommunikationsüberwachung entgegenhalten, daß sich Schreckensszenarien in einem solchen Ausmaß in Österreich gar nicht realisieren können und andererseits, daß es an geschulten Sicherheitskräften fehlt, um eine Überwachung in einem erforderlichen Ausmaß durchzuführen. Aber solange es keine gesetzlichen Grundlagen für eine solche Überwachung des Fernmeldeverkehrs gibt, wird auch die Ausbildung von

---

[257] Siehe dazu ausführlich oben, 5.3.

[258] Vgl die „persönliche Stellungnahme des Abgeordneten Dr. Volker *Kier* zum Bericht des Ausschusses für innere Angelegenheiten zur Regierungsvorlage (1479 BlgNR 20. GP), mit dem das Sicherheitspolizeigesetz und weitere Gesetze geändert werden (SPG-Novelle 1999)“.

[259] *Beste*, Terrorismus: Neuralgische Punkte, Der Spiegel 2/2002, 31.

Spezialkräften des Sicherheitsdienstes, welche eine solche Attacke zu verhindern wissen, hintanstehen müssen.
Klarerweise stellt dieses Beispiel nur eine fingierte Situation dar, welche aber aufzeigt, welche Rolle denn eine „vorbeugende Terrorismusbekämpfung“ auf elektronischem Wege in der Zukunft einnehmen könnte.

5.4.2. Zur (speziellen) Rolle des Bundeskriminalamtes im SPG

Nach deutschem Vorbild wurde mit 01.01.2002 die Institution des „*Bundeskriminalamtes*“[260] in die österreichische Rechtsordnung eingeführt.[261] Die EB zur RV führen dazu aus, daß mit der Errichtung des Bundeskriminalamtes eine Einrichtung geschaffen werden sollte, die auf Grund ihrer Organisation und Ausstattung mit speziell ausgebildetem Personal und Sachmitteln besser zur Bekämpfung überregionaler und schwerwiegender Kriminalität und zur Führung der internationalen polizeilichen Kooperation geeignet ist. Die wesentlichen Ziele sind der Abbau bestehender Doppelgleisigkeiten und die Verbesserung der Aufgabenwahrnehmung im Rahmen einer spezialisierten Zentralstelle, die Einrichtung eines „SPOC“ (Single Point of Contact), die Steuerung und Koordinierung der Sicherheitsbehörden und Sicherheitsdienststellen bei der Ausübung der Aufgabe „Kriminalpolizei“, sowie eine Steigerung der Effizienz durch Ressourcenbündelung.[262]
Welche Rolle das österreichische BKA in Zusammenarbeit mit Sicherheitsbehörden anderer europäischer Staaten spielen wird und welche Aufgaben es in Zusammenhang mit der Bekämpfung aller Bereiche von „Computer-Kriminalität“ im Allgemeinen und zur Bekämpfung von unter Zuhilfenahme des Internet geplanten und ausgeführten Verbrechen im Speziellen einnehmen könnte, wird sich im Verlauf der nächsten Jahre zeigen; beachtliche Anfangserfolge konnten jedoch trotz des kurzen Bestehens dieser Institution schon jetzt erzielt werden.

---

[260] Zu den Aufgaben des BKA vgl ausführlich *Aden*, Das Bundeskriminalamt: Intelligence-Zentrale oder Schaltstelle des bundesdeutschen Polizeisystems? Bürgerrechte & Polizei/CILIP 62 (1/1999), im Internet unter *http://www.cilip.de/ausgabe/62/bka.htm*.

[261] „Bundesgesetz, mit dem das Sicherheitspolizeigesetz geändert und ein Bundesgesetz über die Einrichtung und Organisation des Bundeskriminalamtes erlassen wird“ BGBl I 22/2002.

[262] Vgl 806 BlgNR 21. GP 3.

5.5. Die strafprozessuale Fermelde- bzw Telekommunikations-Überwachung

5.5.1. Fernmelde- oder Briefverkehr?

Gegenstand der Prüfung ist nunmehr, ob die für eine Überwachung gegenständlichen Daten dem Fernmeldeverkehr iSd der Bestimmung des § 149a StPO unterliegen, oder ob es sich dabei um eine Art des Briefverkehrs handelt und die Vorschriften über die Beschlagnahme von Briefen (§§ 146 bis 149 StPO) zur Anwendung gelangen.

Im Fernmeldegesetz[263] bestimmte § 2 Z 1 und 2, daß zum Fernmeldeverkehr die Übermittlung von Informationen – wie Zeichen, Signale, Schriften, Bilder oder Schallwellen - die für Menschen oder Maschinen bestimmt sind, mit der Hilfe von Fernmeldeanlagen gehören. Darunter versteht man wiederum alle technischen Anlagen zur Nachrichtenübermittlung, sei es auf dem Leitungs-, Funk- oder optischen Weg, oder Mittels anderer elektromagnetischer Systeme. Das FMG wurde am 01.08.1997 – im Zuge der Umsetzung der Richtlinien zum Liberalisierungspostulat der Telekom-Infrastruktur durch die EU[264] – durch das Telekommunikationsgesetz[265] abgelöst, welches nunmehr zwischen Telekommunikation einerseits und Sprachtelephonie andererseits unterscheidet:
So wird der klassische *Sprachtelefondienst* definiert als „die gewerbliche Bereitstellung für die Öffentlichkeit des direkten Transports und der Vermittlung von Sprache in Echtzeit von und zu den Netzabschlußpunkten von öffentlichen, vermittelten Netzen, wobei jeder Benutzer das an solch einem Netzabschlußpunkt angeschlossene Endgerät zur Kommunikation mit einem anderen Netzabschlußpunkt verwenden kann“[266], während „*Telekommunikation*“ den „technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen,

---

[263] BGBl 908/1993, in Kraft getreten am 01.04.1994.

[264] *Schmölzer/Mayer-Schönberger*, Das Telekommunikationsgesetz 1997 – Ausgewählte rechtliche Probleme, ÖJZ 1998, 378.

[265] Bundesgesetz betreffend die Telekommunikation (Telekommunikationsgesetz - TKG), BGBl I 100/1997 idF 32/2002.

[266] § 3 Z 12 TKG.

Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen“[267] bezeichnet.

Briefe hingegen sind nach hA an einen bestimmten Empfänger gerichtete Sendungen, deren Inhalt vom Absender durch besondere Vorkehrungen vor der Kenntnisnahme durch Dritte geschützt ist und die im Allgemeinen schriftlich fixierte Gedanken, Meinungen und Nachrichten enthalten.[268]

Für die Zuordnung von Kommunikation über das Internet einerseits zum *Brief*-, andererseits jedoch zum *Fernmeldeverkehr* ist es ausschlaggebend, ob die Datenübermittlung – von dem Absenden bis zum Empfang – in irgendeiner Phase in Schriftform mittels Datenträger erfolgt oder nicht.

Dies läßt sich am Beispiel von Electronic Mail am einfachsten verdeutlichen: Der Unterschied zum Telefonverkehr im herkömmlichen Sinne besteht dabei darin, daß bei Telekommunikation mittels E-Mail neben dem abhörbaren Übermittlungsvorgang noch eine schriftliche Fassung der Nachricht existiert; für ausgedruckte Mails werden also die allgemeinen Beschlagnahmeregelungen der §§ 143 ff StPO zur Anwendung gelangen, während ansonsten die spezielle Norm des § 149a StPO relevant ist.[269] Daraus - und aus der Tatsache, daß nicht nur die Post Leitungen für Internet-Verbindungen zur Verfügung stellt[270] - ergibt sich schließlich, daß die Datenübermittlung via Internet dem Fernmeldeverkehr zuzuordnen ist.[271]

Dies soll jedoch nicht darüber hinwegtäuschen, daß für die Beschlagnahme von *Datenträgern* (Disketten, CD-ROMs, Festplatten etc) die allgemeinen Bestimmungen über die Beschlagnahme der §§ 143 ff StPO weiterhin Gültigkeit beanspruchen. Denn wenn Schriftstücke als Einheit von Daten und Papier betrachtet werden,[272] dann muß ähnliches auch für Datenträger gelten. Daß aufgrund der technischen Fortschritte neue

---

[267] § 3 Z 13 TKG.

[268] Vgl *Wiederin*, Grundrechte, Art 10 StGG Rz 12 mwN.

[269] Siehe zur ähnlichen Problematik der rechtlichen Zuordnung von Fernschreiben *Schmölzer*, Prozessuale Zwangsmittel im Fernmeldewesen – Beschlagnahme oder Überwachung (§§ 143 ff, 146, 149a, 149b StPO), RZ 1988, 249 f.

[270] Zur Abgrenzung aufgrund der jeweiligen Transportart vgl VfSlg 2720/1954 (zu Art 10 Abs 1 Z 9 B-VG).

[271] Vgl *Wessely*, Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet, ÖJZ 1996, 614.

[272] Vgl *Schmölzer*, Strafrechtliche Situation der Informationsregulierung, in: *Maier-Rabler/Mayer-Schönberger/Nening-Schöfbänker/Schmölzer*, Netz ohne Eigenschaften (1996) 166; *dies*, Computernetze und Strafrecht – eine internationale Herausforderung, in: FS *Posch* (1996) 340.

Medien zur Datenspeicherung entwickelt wurden, kann an deren Eigenschaft als beschlagnahmte Datenträger nichts ändern. Die einstige Einheit von Schrift und Papier wird dabei lediglich durch die Verbindung von Daten und dem dazugehörigen Träger ersetzt; es ändert sich jedoch nichts daran, daß Daten nur in Verbindung mit einem geeigneten Trägermedium existieren können. In jenen Fällen, in denen ein Datenträger die Funktion des Papiers übernimmt, können auch elektronische Datenträger beschlagnahmt werden.[273]

5.5.1.1. Die „Rufdatenrückerfassung" – ein Anwendungsfall des § 149a StPO?

Bis zur ausdrücklichen Verankerung der rückwirkenden Überprüfung von Vermittlungsdaten im § 149a StPO durch das „Strafrechtsänderungsgesetz 2002" war es strittig, ob eine solche Rufdatenrückerfassung einen Anwendungsfall der Fernmeldeüberwachung darstellt, oder den allgemeinen Beschlagnahmeregelungen der §§ 143 ff StPO unterliegt. Aufgrund der divergierenden Ansicht von Rechtsprechung und Lehre sei auf dieses Problem – trotz der nunmehr vorhandenen klaren Regelung – kurz eingegangen.

§ 149a (1) StPO[274] bestimmt, daß die Überwachung eines Fernmeldeverkehrs einschließlich der Aufnahme und schriftlichen Aufzeichnung seines Inhalts zur Aufklärung einer vorsätzlich begangenen,

> -mit mehr als sechsmonatiger Freiheitsstrafe bedrohten Handlung mit Zustimmung des *Anlageninhabers* (Z 1), *sowie*
>
> -einer mit mehr als einjähriger Freiheitsstrafe bedrohten Straftat, wenn der *Anlageninhaber selbst der Tat dringend verdächtig ist* oder Gründe für die Annahme vorliegen, daß eine der tatdringend verdächtige Person die Anlage benützen oder eine Verbindung mit ihr herstellen werde (Z 2),

zulässig ist.

---

[273] Vgl *Reindl*, Die Nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren („Rufdatenrückerfassung"), JBl 1999, 794.

[274] In der (noch) geltenden Fassung BGBl I 130/2001.

Anlagen eines Medienunternehmens dürfen gem § 149a (2) StPO nur dann überwacht werden, wenn zu erwarten ist, daß dadurch die Aufklärung einer strafbaren Handlung gefördert werden kann, die mit lebenslanger oder einer Freiheitsstrafe bedroht ist, deren Untergrenze nicht weniger als 5 Jahre und deren Obergrenze nicht weniger als 10 Jahre beträgt.
Die Überwachung ist von der Ratskammer mit Beschluß anzuordnen, bei Gefahr im Verzug kann auch der Untersuchungsrichter diese Anordnung treffen (§ 149b StPO).
Teile der schriftlichen Aufzeichnung sind auf Antrag der Staatsanwaltschaft oder des Beschuldigten von Amts wegen zu löschen, sofern diese für ein Strafverfahren nicht von Bedeutung sein können oder als Beweismittel nicht verwendet werden dürfen (§ 149c (7) StPO).

Soll eine Rufdatenrückerfassung unter denselben Voraussetzungen wie die Überwachung von Gesprächsinhalten erfolgen, so wäre also entweder die *Einwilligung des Inhabers* der Telekommunikationsanlage zur Überwachung erforderlich oder es müßte entweder der Inhaber selbst, oder eine den Teilnehmeranschluß benützende Person *dringend einer Straftat verdächtig sein*. In der Praxis ergeben sich durch diese strengen Anordnungsvoraussetzungen für eine Rückerfassung von Vermittlungsdaten nach den Bestimmungen über die Überwachung des Fernmeldeverkehrs grundlegende Schwierigkeiten: Verweigert der Inhaber die Zustimmung, so liegt die Schwierigkeit im Nachweis eines dringenden Tatverdachts, wenn beispielsweise alle von einer öffentlichen Telefonzelle geführten Gespräche in einem bestimmten Zeitraum rückerfaßt werden sollen.
Brauchbare aber etwas holprige und nicht immer nachvollziehbare Lösungsansätze bietet die von der Judikatur vorgenommene *Ausdehnung des Inhaberbegriffs* auf jede eine Telekommunikationsanlage benützende Person:
Auch[275] in seiner jüngsten Entscheidung[276] zum Thema hat der OGH darauf hingewiesen, daß eine Rufdatenrückerfassung nur innerhalb der durch die §§ 149a bis 149c StPO gezogenen Grenzen[277] zulässig ist. Das Höchstgericht stellte fest, daß der

[275] Vgl schon OGH 06.12.1995, 13 Os 161/95, JBl 1997, 260.

[276] OGH 18.01.2001, 12 Os 152/00, JBl 2001, 531 (*Burgstaller*) = EvBl 1998/191.

[277] Vgl dazu *Schmölzer*, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr – Anmerkungen zu OGH 6.12.1995, 13 Os 161/95, JBl 1997, 214 f; *dies*, Cyberstructure: Die „Fangschaltung“, Juridikum 1997, 43, 46, sowie die Ausführungen oben, 5.3.

Begriff der Überwachung des Fernmeldeverkehrs im § 149a StPO lediglich dahingehend umschrieben werde, daß darunter auch die Aufnahme des im Telekommunikationswege geführten Gesprächs, sowie die schriftliche Aufzeichnung des Gesprächsinhalts falle. Demgegenüber erläutere § 88 Abs 3 TKG einerseits das „Überwachen" als Mithören, Abhören, Aufzeichnen und Abfangen, sowie andererseits die „sonstige Überwachung" einer im Rahmen der Nutzung eines Telekommunikationsdienstes erfolgten Kommunikation; unter einer „*sonstigen Überwachung*" sei auch die *Rückverfolgung von Telefongesprächen* zu verstehen. Diese gesetzliche Definition des § 88 Abs 3 TKG stelle somit auch den Umfang der in den §§ 149a ff StPO vorgesehenen, auf die Möglichkeiten des Fernmeldeverkehrs abstellenden, Überwachungsmaßnahmen klar.

Die Beschlagnahmeregelungen der §§ 143 ff StPO seien nicht anwendbar, da für Vermittlungsdaten aufgrund des verfassungsgesetzlich gewährleisteten Fernmeldegeheimnisses besondere Schutzbestimmungen gelten. Es seien nur die Bestimmungen über die Überwachung des Fernmeldeverkehrs, unter besonderer Berücksichtigung der Voraussetzung der richterlichen Anordnung, maßgeblich.

Das Problem in der Anwendung der Bestimmung des § 149a StPO auf den konkreten Sachverhalt[278] bestand jedoch in der fehlenden *Einwilligung* des Telekom-Dienstleisters in die Rufdatenrückerfassung. Eine Anwendung des § 149a (1) Z 1 StPO schied somit aus. Aber auch die Z 2 leg cit war nicht anwendbar, da der Telekommunikationsdienstleiser *nicht selbst dringend verdächtig* war, die Tat begangen zu haben und auch keine Gründe für die Annahme vorlagen, daß eine der Tat dringend verdächtige Person die Anlage *benützt*, oder eine *Verbindung mit ihr hergestellt* hat. In bezug auf das Erfordernis der Einwilligung des Inhabers der Telekommunikationsanlage zu den beabsichtigten Überwachungsmaßnahme kam der OGH zu dem Schluß, daß Inhaber einer Fernmeldeanlage iSd § 149a StPO jeder „Teilnehmer" iSd § 87 (3) Z 3 TKG sei und hinsichtlich öffentlicher Telefonzellen,

[278] Im gegenständlichen Fall ging es um die Rufdatenrückerfassung betreffend Datum, Uhrzeit, Dauer des Anrufes, gewählte Nummer und Teilnehmer bezüglich sämtlicher Telefongespräche, welche innerhalb eines Zeitraumes von ca 70 Minuten von den öffentlichen Telefonzellen des Bahnhofes Innsbruck und dessen unmittelbarer Umgebung mit welchen Teilnehmern auch immer geführt wurden.

welche einer Überwachung unterzogen werden sollen, *daher jeder bekannte Benützer als deren Inhaber anzusehen ist.*[279]

Dabei ist jedoch jener Fall, daß der Inhaber der Telefonanlage selbst das Opfer einer Straftat ist und somit seine Zustimmung zur Rufdatenrückerfassung nicht erteilen kann, ungeregelt geblieben. Eine Lösung läßt sich darin erblicken, daß angenommen wird, nicht nur der Anrufer stelle eine Verbindung zu einer Fernmeldeanlage iSd § 149a (1) Z 2 lit b StPO her, sondern auch derjenige, der von ihr aus angerufen wird.[280]

Die Ansicht des OGH, eine rückwirkende Erfassung von Vermittlungsdaten stelle einen Anwendungsfall des § 149a StPO dar, wurde von der Lehre keineswegs geteilt:

So wurde beispielsweise argumentiert[281], daß die §§ 149a ff StPO in ihrer Gesamtheit auf den Aussagewert ihrer Formulierungen hin zu untersuchen seien: Abgesehen vom Fall der Zustimmung des Anlageninhabers zu einer Rufdatenrückerfassung tauchen dabei immer wieder „zukunftsweisende" Passagen auf: So setze schon § 149a Abs 1 lit b StPO voraus, „daß eine der Tat dringend verdächtige Person die Anlage benützen werde"; daran, daß sie dies bereits getan hat, sei bei der Wahl des Futurums nicht gedacht worden. Zudem würden die im Zusammenhang mit den §§ 149a ff StPO verwendeten Begriffe der „Überwachung eines Fernmeldeverkehrs" einschließlich der „Aufnahme und schriftlichen Aufzeichnung seines Inhalts" und des „Übertragens der relevanten Teile in Schriftform" darauf hinweisen, daß es sich hiebei eher um eine elektronisch gesteuerte Durchsuchung vorhandenen Datenmaterials iS einer Überprüfung handelt; überwacht könne nur ein Vorgang werden, der gerade abläuft und nicht einer, der bereits passiert ist.

Einschränkend wurde allerdings vorgebracht[282], daß die §§ 139 bis 145 StPO als allgemeine Regeln für die Beschlagnahme von Papieren keine Rücksicht auf die Art der

---

[279] Strengere Maßstäbe an den Begriff des „Inhabers einer Fernmeldeanlage" setzt *Brandstetter* (Die Fernmeldeüberwachung öffentlicher Telefonzellen, JBl 1984, 477 f), wonach für die Inhaberschaft an einer Fernmeldeanlage ein rein faktisches Kriterium maßgeblich sei: Inhaber sei derjenige, der die tatsächliche Verfügungsmacht über die Fernmeldeanlage besitzt, in der Regel also jene Person, welche bestimmen kann, wer die Fernmeldeanlage wann benützen darf.

[280] Vgl *Burgstaller*, Anm zu OGH 18.01.2001, 12 Os 152/00, JBl 2001, 536.

[281] *Schmölzer*, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr – Anmerkungen zu OGH 6.12.1995, 13 Os 161/95, JBl 1997, 214

[282] *Reindl*, Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren („Rufdatenrückerfassung"), JBl 1999, 794 f, 797.

von der Maßnahme betroffenen Daten nehmen würden, Vermittlungsdaten aber als Bestandteil des verfassungsgesetzlich gewährleisteten Fernmeldegeheimnisses besonderem Schutz unterlägen, welcher durch die Anwendung der Beschlagnahmeregelungen auf die Rufdatenrückerfassung nicht umgangen werden dürfe. Eine solche sei daher nur dann zulässig, wenn einerseits ein richterlicher Befehl vorliegt, sie zur Aufklärung einer mit mehr als einem Jahr bedrohten Straftat notwendig und - in Hinblick auf die Rechte der von der Maßnahme betroffenen, aber sonst am Strafverfahren nicht beteiligten Personen – diese auch verhältnismäßig ist.

5.5.2. Reform des § 149a StPO

Die Diskussionen darüber, ob die Überwachung des Datenverkehrs im Internet im Allgemeinen oder die rückwirkende Überprüfung von Vermittlungsdaten im Speziellen einen Anwendungsfall der Fernmeldeüberwachung iSd § 149a StPO darstellt, sowie der generelle Ruf nach einer einheitlichen Regelung diesbezüglich, mündeten letztendlich in zwei voneinander getrennte Reformvorhaben des Gesetzgebers, welche (unter anderem) auch eine Novellierung der Bestimmungen der Telefonüberwachung zum Inhalt haben: Einerseits dem Entwurf eines umfassenden „Strafprozessreformgesetz“[283], andererseits, aufbauend auf dem „Entwurf einer Strafprozessnovelle 2001“, dem „Strafrechtsänderungsgesetz 2002“[284].

Gerade im Hinblick darauf, daß zwar mit der Überwachungsverordnung[285] die technischen Details einer Telekommunikationsüberwachung (ansatzweise) festgehalten wurden, die Bestimmungen des formellen Rechts zur Fernmeldeüberwachung in der StPO jedoch nunmehr seit beinahe zehn Jahren unverändert Gültigkeit haben, scheint eine solche Reform nicht nur nötig, sondern ist eine solche unabdingbar.

---

[283] Zum Zeitpunkt des Verfassens dieser Arbeit als „Regierungsvorlage betreffend Bundesgesetz, mit dem die Strafprozessordnung 1975 neu gestaltet wird (Strafprozessreformgesetz)“, 1165 BlgNR 21. GP vorliegend; vgl dazu ausführlich oben, 2.2.

[284] „ Bundesgesetz, mit dem das Strafgesetzbuch, die Strafprozeßordnung 1975, das Strafvollzugsgesetz, das Suchtmittelgesetz, das Gerichtsorganisationsgesetz, das Waffengesetz 1996, Fremdengesetz 1997 und das Telekommunikationsgesetz geändert werden (Strafrechtsänderungsgesetz 2002)“, BGBl I 134/2002.

[285] Siehe dazu unten, 5.6.

5.5.2.1. Der Ministerialentwurf einer „Strafprozessnovelle 2001"

Im Sommer 2001 wurde ein Ministerialentwurf einer Strafrechtsnovelle[286] veröffentlicht, der einige interessante Ansatzpunkte zur Reform der Bestimmungen über die Fernmeldeüberwachung aufwies. Das Vorhaben wurde jedoch wegen ungeklärter Fragen im Zusammenhang mit der zum Zeitpunkt der Erarbeitung des Ministerialentwurfs noch nicht erlassenen „Überwachungsverordnung" zurückgestellt.[287]

Da dieser Entwurf - und die kritischen Stimmen in der Lehre dazu[288] - jedoch wesentliche „Vorarbeit" zur Novellierung der Bestimmung des § 149a StPO iS des „Strafrechtsänderungsgesetz 2002" geleistet hat, sollen die wichtigsten Punkte dieses Reformvorhabens kurz vorgestellt werden.

Im Sinne des Entwurfs und des damit geänderten § 149a (1) StPO wird unter „*Überwachung einer Telekommunikation*"

(a) die Feststellung, welche *Teilnehmeranschlüsse* Ursprung oder Ziel einer Telekommunikation, einschließlich *erfolgloser Verbindungsversuche*, sind oder waren, und
(b) das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen des Inhalts von Nachrichten, die durch Telekommunikation übermittelt oder empfangen werden

verstanden.

Nach den EB zum Entwurf[289] bezeichnet der Begriff „Telekommunikation" den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen. Es soll im Bereich der Überwachung der Telekommunikation künftig nicht mehr auf Begriffe wie „Aufnahmen" oder

---

[286]Ministerialentwurf einer „Strafprozeßnovelle 2001", 240/ME 20. GP; BMJ 578.020/5-II 3/2001. Im Folgenden: „ME-StPO 2001".

[287] Vgl die EB zum Ministerialentwurf eines „Strafrechtsänderungsgesetz 2002" (308/ME 21. GP), BMJ 318.015/5-II 1/2002, 34. Im Folgenden: „ME-StRÄG 2002"

[288] Va *Reindl*, Telefonüberwachung zweimal neu? JBl 2002, 69.

[289] Vgl die EB zum ME-StPO 2001, 10.

„schriftliche Aufzeichnungen", sondern auf das im § 149a (1) Z 2 des Entwurfs definierte „Ergebnis einer Telekommunikation" abgestellt werden. Nicht nur jedes durch die Überwachung gewonnene Stamm- oder Inhaltsdatum soll von davon umfaßt werden, sondern auch rufbegleitende Daten - also solche Daten, die auch im Fall einer Inhaltsüberwachung, insbesondere im Bereich der Überwachung von Mobilfunknetzen, anfallen. Auch der Datenträger als solches fällt unter den Begriff des „Ergebnisses der Überwachung".[290]

Die Bestimmungen der StPO in bezug auf die Überwachung des Fernmeldeverkehrs sollen auf sämtliche Formen der Telekommunikation iSd § 3 Z 13 TKG ausgeweitet werden.[291]

Der erste Anwendungsfall einer Überwachung besteht nach dem Ministerialentwurf in der Feststellung der Vermittlungs- und Verbindungsdaten. Die Bezugnahme auf „Telekommunikation iSd § 3 Z 13 TKG" führt unweigerlich dazu, daß auch Internetverbindungen oder GPRS von einer Überwachungsmaßnahme erfaßt sein sollen. Unter diese Bestimmung fällt beispielsweise, *wer* sich *wann* und *wie lange* mit dem Internet im Allgemeinen, oder mit einer Web-Page oder einem News-Server im speziellen verbunden, oder sich in eine FTP-Seite eingewählt hat.

Für die Erteilung der Anordnung der Überwachung ist es nach dem Entwurf weiters nötig (§ 149a Abs 2), daß dadurch die Aufklärung einer

- vorsätzlich begangenen, mit *mehr als sechsmonatiger Freiheitsstrafe* bedrohten strafbaren Handlung gefördert werden kann und der *Inhaber des Teilnehmeranschlusses* der Überwachung ausdrücklich *zustimmt*, *oder*

- die Überwachung zur Aufklärung einer *vorsätzlich begangenen*, mit *mehr als einjähriger Freiheitsstrafe* bedrohten strafbaren Handlung erforderlich erscheint, der *Inhaber des Teilnehmeranschlusses* selbst *dringend verdächtig* ist, die Tat begangen zu haben, oder Gründe für die Annahme vorliegen, daß eine der Tat *dringend verdächtige Person* den Teilnehmeranschluß benützt hat oder benützen werde oder eine Verbindung mit ihm hergestellt hat oder herstellen werde.

---

[290] Vgl die EB zum ME-StPO 2001, 12.

[291] Vgl die EB zum ME-StPO 2001, 11.

Durch die erfolgte Differenzierung sollte die Überwachung von Inhaltsdaten auch sprachlich deutlich von der Überwachung und Ermittlung von Verbindungsdaten abgegrenzt werden. Auch sollte damit der Judikatur[292] entsprochen werden, wonach die Durchführung einer hinsichtlich einer bestimmten Telefonanlage angeordneten Rufdatenrückerfassung von den Regelungen zur Überwachung des Fernmeldeverkehrs iSd §§ 149a bis 149c StPO umfaßt wird.[293] Nach der Vorstellung dieses Entwurfs sollte die Rufdatenrückerfassung somit auf der Grundlage des § 149a StPO unter denselben Voraussetzungen wie eine Überwachung von Gesprächsinhalten erfolgen.
Kritisiert wurde in diesem Zusammenhang vor allem, daß auch in jenen Fällen, in denen nur Verbindungs- nicht aber Inhaltsdaten überwacht werden sollen, am Vorliegen eines „*dringenden Tatverdachts*“ angeknüpft wird. Die bloße Erhebung von Verbindungsdaten stelle einen wesentlich geringeren grundrechtlichen Eingriff dar, als das Erfassen von Inhaltsdaten. Man solle demnach eine Rufdatenerhebung schon dann zulassen, wenn der *konkret begründete Verdacht* einer Straftat vorliegt, die Datenerhebung zur Aufklärung der Tat *notwendig* und sie überdies *verhältnismäßig* ist; zudem sollten die vorgeschlagenen Voraussetzungen auch für die Rufdatenerhebung in Echtzeit gelten, wenn die strengeren Voraussetzungen für die Ermittlung von Inhaltsdaten iSd § 149a StPO vorliegen.[294]

Gerade die Eigenheit des Entwurfs, nämlich die Überwachung auch auf das Internet als solches auszudehnen, hat verständlicherweise wiederum auch zu Mißmut auf Seiten der Telekommunikationsdienstesbetreiber geführt. Die Aussage jedoch, daß dieser Entwurf „unter dem Deckmantel einer StPO Novelle die viel diskutierte Überwachungsverordnung vorwegzunehmen versucht und nicht nur eine begriffliche Anpassung an die Bestimmungen des TKG angestrebt wird, sondern es sich vielmehr um weitreichende neue Bestimmungen, die vor allem die Telekombetreiber vor vollendete Tatsachen stellen sollen, (handelt)“[295] ist jedoch schlichtweg als falsch einzustufen. Selbst unter dem Aspekt, daß die Überwachungsverordnung zum Zeitpunkt des Erscheinens des Entwurfs eines Strafprozeßreformgesetzes 2001, auf den sich die

---

[292] Siehe dazu ausführlich oben, 5.5.1.1.

[293] Vgl die EB zum ME-StPO 2001, 11.

[294] Vgl *Reindl*, Telefonüberwachung zweimal neu? JBl 2002, 71.

[295] Vgl *Pracher*, Stellungnahme zum Entwurf einer Strafprozeßnovelle 2001 aus der Sicht eines Telekombetreibers, im Internet unter *http://www.it-law.at/papers/pracher-stpo.pdf*.

Kritik bezieht, noch nicht in ihrer Endfassung vorlag, so war Gegenstand der Diskussion um den Inhalt der Überwachungsverordnung stets die technische Realisierung solcher Überwachungsmaßnahmen zu regeln, nicht aber deren rechtliche Anwendungsvoraussetzungen festzuhalten.[296] Die Verordnung schafft - im Einklang mit der gesetzlichen Grundlage - nur die technischen Voraussetzungen für eine sich aus den berührten Bereichen (TKG und StPO) ergebende Materie, und definiert die für eine Überwachung erforderlichen Standards.[297] Die beiden Materialen inhaltlich zu vergleichen und Parallelen ziehen zu wollen kann zu keinem Ergebnis führen.
Die übrigen Bestimmungen des Entwurfs zu erörtern würde den Rahmen dieser Arbeit sprengen. Zusammenfassend läßt sich aber sagen, daß es sich hierbei um eine durchaus taugliche Grundlage handelt, Regelungen für Fragen, die sich in bezug auf die Überwachung von Inhalts- und Vermittlungsdaten heutzutage stellen, auch in die StPO einzugliedern.

5.5.2.2. Das „Strafrechtsänderungsgesetz 2002“

Wesentliche Neuerungen im Vergleich zum „Ministerialentwurf einer Strafprozessnovelle 2001“ bringt die aktuelle Regierungsvorlage eines „Strafrechtsänderungsgesetz 2002“[298] im Bereich der Überwachung des Telekommunikationsverkehrs vor allem in bezug auf die Rufdatenrückerfassung:

---

[296] Siehe dazu va die „Schriftliche Anfragen des Abgeordneten *Pilz*, Freundinnen und Freunde an die Bundesministerin für Verkehr, Innovation und Technologie (2090/J 21. GP), den Bundesminister für Inneres (2091/J 21. GP), den Bundesminister für Justiz (2089/J 21. GP) betreffend Überwachungsverordnung“ vom 07.03.2001, und die betreffenden Anfragebeantwortungen (2076/AB 21. GP, 2061/AB 21. GP und 2058/AB 21. GP).

[297] „Anfragebeantwortung durch den Bundesminister für Inneres Dr. Ernst *Strasser* zur schriftlichen parlamentarische Anfrage betreffend Überwachungsverordnung“, 2061/AB 21. GP vom 02.05.2001, Antwort zu den Fragen 18 und 19.

[298] „Bundesgesetz, mit dem das Strafgesetzbuch, die Strafprozeßordnung 1975, das Strafvollzugsgesetz, das Suchtmittelgesetz, das Gerichtsorganisationsgesetz, das Waffengesetz 1996, Fremdengesetz 1997 und das Telekommunikationsgesetz geändert werden (Strafrechtsänderungsgesetz 2002)“, BGBl I 134/2002.

Die Bewilligung einer solchen wurde mit der aktuellen Regelung vom Vorliegen eines „dringenden Tatverdachts“ gelöst und ist nunmehr unter weniger strengen Voraussetzungen durchführbar:[299]

Die *Feststellung des räumlichen Bereiches*, in dem sich ein durch einen bestimmten Teilnehmeranschluß gehörendes Endgerät befindet (§ 149a (1) lit a StPO idF StRÄG 2002), wie auch die Feststellung, welche *Teilnehmeranschlüsse* Ursprung oder Ziel einer Telekommunikation sind oder waren[300] (§ 149a (1) lit b StPO idF StRÄG 2002) ist nunmehr auch in jenen Fällen möglich, in denen zu erwarten ist, daß

- dadurch die Aufklärung einer *vorsätzlich begangenen*, mit *mehr als einjähriger Freiheitsstrafe* bedrohten strafbaren Handlung gefördert werden kann (§ 149a (2) Z 2 StPO idF StRÄG 2002)

und

- durch die Überwachung *Daten des Verdächtigen ermittelt werden können* (§ 149a (2) Z 2 StPO idF StRÄG 2002).

Als erschwerend im Vergleich zur Regelung des Ministerialentwurfs einer „Strafprozessnovelle 2001“ stellen sich jedoch die Voraussetzungen dar, unter denen eine *Inhaltsüberwachung* von Nachrichten angeordnet werden kann: Diese ist nur dann ohne Zustimmung des Inhabers des Teilnehmeranschlusses zulässig, wenn

- die Überwachung zur Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung erforderlich erscheint

und

a) der *Inhaber* des Teilnehmeranschlusses *selbst dringend verdächtig* ist, die Tat begangen zu haben (§ 149a (2) Z 3 lit a StPO idF StRÄG 2002),

---

[299] Vgl dazu die EB zum ME-StRÄG 2002, 35: „In Entsprechung dieser Vorschläge soll eine Rufdatenrückerfassung nicht mehr an das Erfordernis eines dringenden Tatverdachts gebunden sein und durch den Untersuchungsrichter – bei Vorliegen der übrigen Voraussetzungen, insbesondere der Verhältnismäßigkeit (Abs 4) – angeordnet werden können[...]“.

[300] Vgl dazu auch den Beschluß des BGH vom 21.2.2001, 2 BGs 42/2001, worin ausdrücklich festgehalten wird, daß die Strafverfolgungsbehörden im Rahmen einer nach den §§ 100a, 100b dStPO angeordneten Überwachung und Aufzeichnung der Telekommunikation mit einem Mobilfunktelefon von dem Netzbetreiber die Bereitstellung von Informationen darüber verlangen können, in welcher Funkzelle sich das Telefon befindet, selbst wenn mit diesem nicht telefoniert wird.

oder

b) Gründe für die Annahme vorliegen, daß eine der Tat *dringend verdächtige Person* den Teilnehmeranschluß *benützen* oder eine Verbindung mit ihm herstellen werde (§ 149a (2) Z 3 lit b StPO idF StRÄG 2002).

Ebenfalls eingearbeitet wurde eine Regelung zum Erfordernis der *Verhältnismäßigkeit* der Überwachungsmaßnahme, welche im wesentlichen dem bisherigen § 149d (3) StPO entspricht: Eine Überwachung ist nur zulässig, soweit die Verhältnismäßigkeit zum Zweck der Maßnahme gewahrt wird. Dabei ist insbesondere darauf Bedacht zu nehmen, daß der angestrebte Erfolg in einem vertretbaren Verhältnis zu den voraussichtlich bewirkten Eingriffen in die Rechte unbeteiligter Dritter steht, und zu prüfen, ob nicht auch mit weniger eingreifenden Maßnahmen begründete Aussicht auf Erfolg besteht (§ 149a (4) StPO idF StRÄG 2002). Anordnungen zur Bekanntgabe einer (unbestimmten Anzahl) von Anschlüssen, die in einem bestimmten räumlichen Bereich aktiv oder passiv eine Verbindung aufgenommen oder aufzunehmen versucht haben, werden vor diesem Grundsatz kaum bestehen können.[301]

Auch der Justizausschuß[302] hält fest, daß auch bei diesen Ermittlungsmaßnahmen eine – bei jedem Grundrechtseingriff gebotene – Prüfung der Verhältnismäßigkeit vorzunehmen ist. Diese hat in Fällen eines Eingriffes in das Fernmeldegeheimnis und in die Privatsphäre alle Umstände des Einzelfalls konkret zu berücksichtigen. Dabei sind das Gewicht der Straftat und die Aussicht auf deren Aufklärung durch den Grundrechtseingriff der Bedeutung dieses Eingriffs und dessen Umfang, dh der Zahl der von der Überwachung der Telekommunikation betroffenen gegenüberzustellen. Auch die Erfolgsaussichten weniger einschneidender Maßnahmen sind zu prüfen.

Die Überwachung darf nur für einen solchen Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist. Eine neuerliche Anordnung ist nur zulässig, soweit aufgrund bestimmter Tatsachen anzunehmen ist, daß die Überwachung nun Erfolg haben werde (§ 149b (3) StPO idF StRÄG 2002).

Zusammenfassend läßt sich zu dem Entwurf sagen, daß durch die Unterscheidung zwischen Vermittlungs- und Inhaltsdaten, sowie der bloßen Standortfeststellung eines Endgeräts, ein wesentlicher Schritt unternommen wurde, die seit 1993 unverändert bestehende Bestimmung des § 149a StPO in erster Linie an das

---

[301] EB zum ME-StRÄG 2002, 36.

[302] JAB 1213 BlgNR 21. GP 2.

Telekommunikationsgesetz, letztlich aber auch an die Regelungen der Überwachungsverordnung anzupassen.

Kritisch angemerkt muß aber dennoch werden, daß es zwar einerseits der Rechtssicherheit dienlich ist, eine Rufdatenrückerfassung unter weniger strengen Voraussetzungen, insbesondere auch ohne der Zustimmung des Inhabers eines Teilnehmeranschlusses, durchführen zu können, als eine Überwachung von Inhaltsdaten; andererseits könnte jedoch eine Erleichterung der Anwendungsvoraussetzungen zur Erfassung von Verbindungsdaten leicht dazu mißbraucht werden, um jene Maßnahmen durchzuführen, die letztlich in einer Kontrolle der *Inhalte einer Verbindung* (der Kommunikation) münden können: Wenn nicht nur *gespeicherte* Verbindungsdaten rückerfaßt werden, sondern auch Vermittlungsdaten in Echtzeit quasi „live" beobachtet und aufgezeichnet werden (vgl § 149a Abs 1 Z 1 lit b StPO idF StRÄG 2002: „...die Feststellung, welche Teilnehmeranschlüsse Ursprung oder Ziel einer Telekommunikation...*sind* oder waren"), so ergibt sich damit möglicherweise automatisch auch eine Überwachung des Inhalts: Wenn beispielsweise beobachtet werden soll, wer sich in einen Chat-Kanal, der dafür bekannt ist, Umschlagplatz für kinderpornographisches Material zu sein, einloggt, dann ist es ein leichtes, auch den Inhalt der Diskussion mitzuverfolgen.

Noch heikler stellt sich die Lage im Falle des Überwachens von Kontakten *mit* Newsgroups und Internet-Foren dar: Während bei der gewöhnlichen Sprachtelephonie Inhaltsdaten seitens des Telekommunikationsdiensteanbieters oft (noch)[303] gar nicht oder nur wenige Tage aufbewahrt werden, so sind Nachrichten auf News- oder WWW Servern meist über Jahre hinweg gespeichert. Eine Kontrolle, wann sich wer und für wie lange in solchen Foren aufhielt, könnte ebenfalls schlußendlich - und zwar einfach per Mausklick - in eine umfassende Inhaltkontrolle im Sinne des Lesens der gespeicherten Nachricht münden. Sollte also, was sich eigentlich als unzweifelhaft darstellt, eine Überwachung der Telekommunikation auch alle per Internet übertragenen Daten umfassen, so sind gesonderte Regelungen seitens des Gesetzgebers nicht nur wünschenswert, sondern auch dringend notwendig.

Trotz intensiver Recherchen - unter anderem im Datenschutzrat[304] – konnte nicht eruiert werden, wie der Personenkreis der „Betreiber, die an der Überwachung mitzuwirken

---

[303] Siehe zu den Bestimmungen der Überwachungsverordnung unten, 5.6.

[304] Http://www.argedaten.at.

haben“, definiert ist. Vorgebracht wurde unter anderem, jeder Betreiber möge im Rahmen eines Verfahrens nach dem AuskunftspflichtG[305] feststellen lassen, ob die gegenständlichen Bestimmungen auch ihn beträfen. Es würde aber natürlich eine Verzögerung des Ermittlungsverfahrens daraus resultieren, daß erst im Anlaßfall geprüft wird, ob eine Verpflichtung eines bestimmten Betreibers zur Durchführung von Überwachungsmaßnahmen besteht. Eher wahrscheinlich ist die Annahme, die betreffende Formulierung sei deshalb so allgemein gehalten, um jederzeit nicht nur Infrastruktur-Betreiber, wie die klassischen Telekom-Firmen, zu Überwachungsmaßnahmen heranziehen zu können, sondern jede Form von Internetbetreibern. In diesem Punkt bleibe die Regierungsvorlage also mit Absicht unklar.[306]

5.5.2.3. Das „Strafprozessreformgesetz“

Eine umfassende Änderung, nicht nur der Bestimmungen über die Überwachung des Fernmeldeverkehrs, sondern auch des gesamten strafprozessualen Vorverfahrens beinhaltet die Regierungsvorlage eines „Strafprozeßreformgesetzes“[307]. In den §§ 134, 135 des Regelwerkes wird die „Beschlagnahme von Briefen, Auskunft über Standort- und Vermittlungsdaten sowie Überwachung von Nachrichten“ einer gesetzlichen Regelung unterzogen. Dabei wird zwischen der *Überwachung von Standort- und Vermittlungsdaten* einerseits und der *Überwachung von Nachrichten* andererseits unterschieden.

§ 134 Z 2 StPORefG gibt Aufschluß darüber, daß unter „Auskunft über Standort- und Vermittlungsdaten“ die Erteilung einer Auskunft über

a) die näheren Umstände der Übertragung von Nachrichten durch Telekommunikation oder durch ein Computersystem, insbesondere über die *Person des Adressaten oder Absenders* einer Nachricht, seines *Standortes*, die für Verrechnungszwecke erforderlichen Daten und die *Adresse*

---

[305] BGBl 287/1987 idF BGBl I 158/1998.

[306] Vgl das „Votum Seperatum zum Entwurf eines Strafrechtsänderungsgesetzes 2002“ der „ARGE-Daten“ vom 03.05.2002, 2 f, im Internet unter *ftp://ftp.argedaten.at/sic/VSSTPO.pdf*.

[307] „Regierungsvorlage betreffend das Bundesgesetz, mit dem die Strafprozessordnung 1975 neu gestaltet wird (Strafprozessreformgesetz)“, 1165 BlgNR 21. GP. im Folgenden: „StPORefG“; siehe dazu auch oben, 2.2.

der technischen Einrichtung oder des Computersystems, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder ist, und

b) den *räumlichen Bereich*, in dem sich ein zur Übermittlung und zum Empfang von Nachrichten durch Telekommunikation bestimmtes *Endgerät* befindet oder befunden hat,

zu verstehen ist.

Die EB zur RV[308] führen dazu aus, daß mit „Auskunft über Standort- und Vermittlungsdaten" jene Anordnungen definiert werden sollen, durch die Diensteanbieter verpflichtet werden können, bestimmte Daten den Strafverfolgungsbehörden bekannt zu geben. Die Definition erfaßt im Bereich der Telekommunikation insbesondere die *nachträgliche Rufdatenerfassung* und die *Standortfeststellung*, wie sie auch der Regierungsvorlage eines Strafrechtsänderungsgesetzes 2002 vorgeschlagen wird.
Schließlich sollen durch § 134 Z 2 lit a Z 2 StPORefG auch die von Art 17 der Cyber-Crime-Convention angesprochenen Daten erfaßt werden, die von Dateninhabern wie Diensteanbietern bereits verarbeitet und gespeichert wurden. Dabei soll jedoch lediglich eine eindeutige Befugnis geschaffen werden, welche die Sicherung und Weitergabe existierender und rechtmäßig gespeicherter Daten im Zusammenhang mit strafrechtlichen Ermittlungen zu verlangen gestattet.[309]

Im Gegensatz dazu stellt die „*Überwachung von Nachrichten*" das Ermitteln des Inhalts von Nachrichten, die durch Telekommunikation oder durch ein *Computersystem übermittelt oder empfangen werden*, dar (§ 134 Z 3 StPORefG).
Diese Definition der Überwachung von Nachrichten stellt nicht mehr ausschließlich auf die Übertragung von Nachrichten durch Telekommunikation ab, sondern berücksichtigt auch andere Übertragungstechniken. Es sollen demnach auch bestimmte, mittels eines Computersystems übertragene Kommunikationsformen erfaßt werden, welche die Übertragung der Kommunikation über Telekommunikationsnetzwerke vor deren Empfang durch ein anderes Computersystem einschließen können.[310]

---

[308] EBRV 1165 BlgNR 21. GP 187.

[309] EBRV 1165 BlgNR 21. GP 187.

[310] EBRV 1165 BlgNR 21. GP 187.

Die Auskunftserteilung über *Standort- und Vermittlungsdaten* ist nur dann zulässig (§ 135 (2) StPORefG),

1. wenn und solange der *dringende Verdacht* besteht, daß eine von der Überwachung betroffene Person eine andere *entführt* oder sich sonst ihrer *bemächtigt* hat, und sich die Auskunft auf Daten, Signale und Nachrichten beschränkt, von denen anzunehmen ist, daß sie zur Zeit der Freiheitsentziehung *durch vom Beschuldigten benützte technische Einrichtungen* oder *Computersysteme* und *Endgeräte* übermittelt, empfangen oder gesendet werden,
2. wenn zu erwarten ist, daß dadurch die Aufklärung einer *vorsätzlich begangenen*, mit mehr als *sechsmonatiger Freiheitsstrafe* bedrohten strafbaren Handlung gefördert werden kann und der *Inhaber* der technischen Einrichtung oder des Computersystems, die oder das Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft *ausdrücklich zustimmt*,
3. wenn dies zur Aufklärung einer *vorsätzlich begangenen*, mit *mehr als einjähriger Frei*heitsstrafe bedrohten strafbaren Handlung erforderlich erscheint und auf Grund bestimmter Tatsachen anzunehmen ist, daß dadurch *Daten des Beschuldigten ermittelt werden können*.

Die Ermittlung von Standort- und Verbindungsdaten soll dann gestattet sein, wenn sich der Verdacht gegen den *Inhaber* der technischen Einrichtung richtet, dieser aktiv oder passiv an der Übertragung einer Kommunikation durch Telekommunikation oder im elektronischen Weg *beteiligt ist oder war* oder der Inhaber der Auskunft *zustimmt* (etwa zur Ausforschung des Urhebers einer gefährlichen Drohung, die dem Betroffenen per E-Mail übermittelt wurde). Die in dieser Bestimmung geregelten Fälle knüpfen an die Bestimmung der Überwachung einer Telekommunikation nach § 149a Abs. 2 Z 1 und 2 idF StRÄG 2002 an.[311]

Die Ermittlung von *Nachrichten* soll gem § 135 (3) StPORefG nur

1. in den Fällen des Abs 2 Z 1,
2. in den Fällen des Abs 2 Z 2, sofern der *Inhaber* der technischen Einrichtung oder des Computersystems der Überwachung *zustimmt*,
3. wenn dies zur Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten strafbaren Handlungen *ansonsten wesentlich erschwert wäre* und der *Inhaber* der technischen Einrichtung oder des Computersystems, die oder das Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, *dringend verdächtig* ist, die Tat begangen zu haben oder zu planen,

[311] Vgl die EBRV 1165 BlgNR 21. GP 188 f.

4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, daß dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann,

zulässig sein.

Diese Bestimmung zu den Voraussetzungen der Überwachung des *Inhalts* von Nachrichten sei jedoch an dieser Stelle nur der Vollständigkeit halber angeführt, da sie sich am Wortlaut des § 149a Abs 2 Z 3 StPO idF des Ministerialentwurfs des StRÄG 2002[312] orientiert, eine Überarbeitung und Anpassung an die Regierungsvorlage somit noch erfolgen müßte.

5.6. Die „Überwachungsverordnung"

Um zu normieren, ob und für welchen Zeitraum Inhalts- und Verbindungsdaten gespeichert werden *müssen* und Klarheit darüber zu schaffen, inwieweit „Betreiber" iSd § 14 TKG die technischen Voraussetzungen für eine Überwachung des Fernmeldeverkehrs nach den Bestimmungen der StPO bereitzustellen haben, wurde auf Grundlage des § 89 (3) TKG[313] die „*Überwachungsverordnung*"[314] geschaffen, welche am 01.01.2002 in Kraft getreten ist.
Diese nur sechs Paragraphen beinhaltende Verordnung hat im Vorfeld ihres In-Kraft-Tretens für etlichen Unmut auf Seiten der Datenschützer, aber auch auf Seiten der (privaten) Anbieter von Telekommunikationsdiensten gesorgt. Kernpunkt der Verordnung, § 3, bestimmt, daß

> „Betreiber in ihren Anlagen die Funktionen *bereitzuhalten* (*haben*), die in der Lage sind, über aktive Mitwirkung des Betreibers im Einzelfall die *Überwachung und Aufzeichnung der Telekommunikation* zu gewährleisten, die von dem zu überwachenden Teilnehmeranschluß

---

[312] 308/ME 21. GP.

[313] „Durch Verordnung kann der Bundesminister für Wissenschaft und Verkehr im Einvernehmen mit den Bundesministern für Inneres und für Justiz, dem jeweiligen Stand der Technik entsprechend, die näheren Bestimmungen für die Gestaltung der technischen Einrichtungen zur Gewährleistung der Überwachung eines Fernmeldeverkehrs nach den Bestimmungen der StPO festsetzen".

[314] BGBl II 418/2001.

> ausgeht oder für diesen bestimmt ist oder zu Datenspeichern geleitet wird, die dem Teilnehmeranschluß zugeordnet sind, oder die aus solchen Datenspeichern abgerufen wird."

Problematischer in Hinblick auf die praktische Durchführbarkeit liest sich § 3 (2) ÜVO, nach dem

> „Betreiber in ihren Anlagen die Funktionen bereitzuhalten (haben), die in der Lage sind, die *Inhaltsdaten* sowie die sonstigen mit der Überwachung der Telekommunikation *in Zusammenhang stehenden* erforderlichen Informationen zur Verfügung zu stellen."

Es sind also all die technischen Voraussetzungen, welche für eine Überwachung des Fernmeldeverkehrs vonnöten sind, ständig *bereitzuhalten* und nicht etwa erst im Falle einer richterlichen Anordnung der Überwachung einzurichten. Eine solche Anordnung ist erst zur Aufzeichnung und in weiterer Folge zur Herausgabe der Daten an die Behörde vonnöten.
Verständlicherweise gipfelten die Diskussionen um die Erlassung der ÜVO in heftigen Protesten vor allem der Mobilfunkbetreiber gegen die verordnete Umrüstung der Netze auf Abhörtauglichkeit.[315] Auch der „Verband Alternativer Netzbetreiber" (VAT) kritisierte in seiner Stellungnahme[316], daß „die unklare Formulierungsweise der Verordnung nicht klar und deutlich erkennen läßt, daß es in jedem Einzelfall der Netzbetreiber sein muß, der eine auf richterliche Anordnung zu erfolgende Überwachung einrichtet, für den Zeitraum der Anordnung monitort und nach Ablauf wieder entfernt".

Ermöglicht sollen die von der Verordnung festgelegten Vorgänge zur Datenspeicherung und -Überwachung gem § 4 ÜVO durch eine technische Schnittstelle, basierend auf dem sogenannten „ETSI-Standard" in der Fassung ES 201 671 Version 2.1.1, werden.

---

[315] Die Umsetzung dieser Norm des „European Telecom Standards Institute" (ETSI) würde – so die Meinung der Telekommunikationsdienstebetreiber - nicht nur einen Großumbau der Vermittlungsstellen mit sich bringen, sondern auch zusätzliche Hochsicherheitszonen notwendig machen, da jede Schnittstelle gleichzeitig eine Schwachstelle im Netz und somit einen Angriffspunkt für Eindringlinge aller Art darstelle (vgl dazu „Hunderte Millionen für die Überwachung", ORF-Futurezone vom 22.08.01 unter *http://futurezone.orf.at/futurezone.orf?read=detail&id=76861*).

[316] VAT-Stellungnahme im Rahmen der Begutachtung zum Entwurf einer Überwachungsverordnung (ÜVO) – GZ 100048/IV-JD/00.

Als Zeitraum, in dem eine solche technische Schnittstelle eingerichtet werden muß, bestimmt § 6 (2) ÜVO, daß Betreiber von Telekommunikationseinrichtungen, mittels derer zum Zeitpunkt des In-Kraft-Tretens dieser Verordnung bereits Telekommunikationsdienste erbracht wurden, die Verpflichtungen gemäß §§ 3 und 4 ÜVO unverzüglich, spätestens jedoch sechs Monate nach In-Kraft-Treten der Verordnung zu erfüllen haben. Der „ETSI-Standard" soll mit 01.01.2005 überall realisiert worden sein (§ 6 (3) ÜVO).

5.6.1. „ETSI" – Die Standardisierung der Telekom-Überwachung[317]

Mit Hilfe der Einführung des EU-Abhörstandards „ETSI ES 201 671"[318] sollen alle Formen der Telekommunikation lückenlos überwachbar werden. Verantwortlich für die Erarbeitung des technischen Standards, der die technischen Gegebenheiten dafür beschreibt, daß Kommunikation, sei es nun im Bereich der Sprachtelephonie oder aber des Internet, „abhörbar" wird, ist die sog Sektion „*Lawful Interception*" (SEC LI)[319] des „*European Telecom Standards Institute*" (ETSI). Zu diesem Zweck wird von drei verschiedenen Arbeitsgruppen ein technischer Standard laufend, parallel zu den Entwicklungen auf technischem Gebiet, weiterentwickelt, um Schnittstellen zur Überwachung sämtlicher digitalen Netze - von ISDN über UMTS bis hin zum Internet - überhaupt erst zu ermöglichen. Techniker und Manager jener Firmen, die das Abhörequipment für diese standardisierten Schnittstellen liefern, wirken in diesen Arbeitsgruppen ebenso mit, wie Behördenvertreter, welche über enge Verbindungen zu deutschen, britischen und holländischen Nachrichtendiensten verfügen. Den

---

[317] Die nun folgenden Ausführungen stützen sich im großen und ganzen auf die hervorragend recherchierte und detailliert ausgeführte 4-teiligen Artikelreihe „Die ETSI-Dossiers" von Erich *Möchel*, abgedruckt (Teil 1 bis 4) jeweils in c't 7/2001, 58; c't 9/2001, 54; c't 17/2001, 78; c't 4/2002, 80. Online erschienen diese Artikel teilweise auch - in bezug auf den „Enfopol"-Schwerpunkt des Online-Magazins „Telepolis" - unter *http://www.heise.de/tp/deutsch/special/enfo/default.html*.

[318] Die aktuelle Version wird durch das Dokument „Handover interface for the lawful interception of telecommunications traffic" des „ETSI Technical Committee Security (SEC)" (ETSI ES 201 671 V1.1.1 (1999-07)) beschrieben. Siehe zu den technischen Details *Möchel*, Abhörstandards für digitale Netze vor der Verabschiedung, Heise-Newsticker vom 13.08.2001 unter *http://www.heise.de/tp/deutsch/special/enfo/9306/1.html*, sowie „Die ETSI-Dossiers" (FN 794).

[319] Http://portal.etsi.org/portal_common/home.asp?TbId=503.

Netzbetreibern sollen dadurch zusätzliche, teure Systeme zur Überwachung verkauft werden, was auch der Grund dafür ist, daß die „SEC LI“ gemeinsam mit Polizei und Behördenvertretern an der Standardisierung mitwirkt.
Relativ einfach gibt sich die Arbeit zur Überwachung von herkömmlicher Telephonie oder Internet-Modem Verbindungen, während die Welt der Datagramme und des dezentralen Paketverkehrs im Internet auf andere und komplexere Weise funktioniert als das, prinzipiell nur aus anrufender und angerufener Partei bestehende, Telephoniemodell. Der aktuelle „ETSI-Standard“, welcher der österreichischen, wie auch der deutschen Überwachungsverordnung zugrunde liegt, ermöglicht derzeit nur eine Internet-bezogene Überwachung im Bereich der Modem-Benutzer über einen der Norm entsprechenden „Switch“ am jeweiligen Wählamt. Dennoch arbeitet man fieberhaft bereits an Methoden, den gesamten Internet-Verkehr überwachbar zu machen, und zwar vollständig, in Echtzeit und ohne eine Einbuße an der Verbindungsqualität, dh für den Überwachten unbemerkbar, hervorzurufen. So wird beispielsweise das „Gegenstück“ zum Standard „201.671“, der technische Report (TR 101 331), welcher ein Pflichtenheft der Polizei und anderen Behörden für Netzwerk-Betreiber darstellt, gerade um das Abfangen von E-Mails und die Überwachung des IP-Verkehrs erweitert.

Probleme ergeben sich aber bei der Umsetzung des Überwachungsstandards „ETSI ES 201 671“ nicht nur im technischen Sinne, sondern auch in bezug auf die rechtlichen Rahmenbedingungen:
Noch fehlt den in den Rang eines europäischen Standards erhobenen Definitionen zum Abhören von Telekommunikationsnetzen die politische Legitimation durch die EU. In der aktuellen Version sind aber bereits auf technischer Ebene alle notwendigen Schnittstellen zum Abhören durch Strafverfolgungsbehörden und Geheimdienste festgelegt. Seit der Verabschiedung des aktuellen Schnittstellen-Standards am 31. August 2001 stellte die Arbeitsgruppe „Lawful Interception“ die rechtlichen Vorgaben dieses Standards auf EU-Ebene her. Kompetenzen aus dieser unter Behördenaufsicht stehenden Arbeitsgruppe werden nun immer mehr in zivil besetzte Techniker-Gremien verlagert; seitens der Netzbetreiber und Ausrüster war sogar überlegt worden, „SEC LI“ überhaupt aufzulösen.[320] Der Entwicklungsprozeß dieses Überwachungsstandards lief

[320] *Möchel*, ENFOPOL: EU-Abhörstandards für die Telekommunikationsnetze, Telepolis, das Magazin für Netzkultur vom 11.02.2002 unter *http://www.heise.de/tp/deutsch/special/enfo/11818/1.html.*

also in der Reihenfolge ab, daß sich „Ausrüster (Alcatel, Ericsson, Nokia et al) mit Polizei und Telekom-Regulatoren in den ETSI-Arbeitsgruppen hingesetzt und zusammen die technische Überwachung der digitalen Netze ausgetüftelt haben“.[321]

Übersehen wurde jedoch schlichtweg, daß das technische Anforderungspapier hierfür schlichtweg fehlte. Dieses Dokument, auch bekannt als die „*International User Requirements*“ (IUR)[322], wurde praktisch in letzter Minute Mitte August 2001 nachgereicht. *Nachdem* also bereits mit dem ETSI-Abhörstandard bezüglich der Überwachung neuerer Technologien wie GPRS, UMTS und Kabelmodems vollendete Tatsachen geschaffen wurden, gingen Polizei und Telekommunikationsdiensteanbieter erst daran, ihre Vorgaben zu formulieren, jedoch ohne gültigen Auftrag durch die EU. Die „International User Requirements“ wurden auf politischer Ebene von teils identischen Beteiligten in der „Police Cooperation Working Group“ des EU-Rats erst nachträglich erstellt.[323]

Ebenso wie sich der technische Überwachungsstandard laufend ändert, werden auch die rechtlichen Rahmenbedingungen, in deren Zentrum die „IUR“ als Bindglied stehen, laufend erweitert, und zwar durch die sog „*Enfopol-Papiere*“. So jagte seit dem Beginn der 90-er Jahre ein „Enfopol“-Dokument, welches meist in der Form eines EU-Ratsbeschlusses verfaßt wurde, oftmals aber über den Status eines Entwurfs nicht hinausging, das andere, ohne jedoch jemals in der Öffentlichkeit vorgestellt, geschweige denn umgesetzt worden zu sein.

An dieser Stelle wird jedoch nicht näher auf diese Dokumente, welche die Telekom-Überwachung auf EU-Ebene zu legalisieren suchen, eingegangen.

---

[321] So ein Vorstandsmitglied eines österreichischen Handy-Netzbetreibers im Gespräch mit dem ORF, im Internet unter *http://futurezone.orf.at/futurezone.orf?read=detail&id=109853.*

[322] Die „Requirements” vom 17.01.1995, „Council Resolution on the lawful interception of Telecommunications”. Erstmals veröffentlicht in: ABl. C 329 v 04.11.1996, 1. Das Dokument ist auch unter den Namen „ENFOPOL 95“, „ENFOPOL 150“ oder „International User Requirements (IUR)“ bekannt.

[323] Vgl „Überwachung ohne Auftrag der EU“, Qintessenz.Org - Verein zur Wiederherstellung der Menschenrechte im Informationszeitalter, im Internet unter *http://www.quintessenz.at/archiv/msg01849.html.*

5.6.2. Zum Vergleich: Die deutsche „TKUEV“

Als – vor allem für Internet-Provider und Anbieter mobiler Telefonnetze - höchst unbefriedigendes Ergebnis langer Diskussionen präsentiert sich also nun in Österreich eine Verordnung, welche es in einigen wenigen Bestimmungen für sich beansprucht, eine taugliche Grundlage für die (technische) Einrichtung umfassender Telekom-Überwachungsmaßnahmen zu sein. Zwar nicht unumstritten, aber dennoch weitaus ausgereifter erweist sich hingegen die „Telekommunikations-Überwachungsverordnung“[324], die am 22.01.2002 in Deutschland erlassen wurde: Allein in Hinblick auf die Begriffsbestimmungen des „Betreibers“[325] einer Telekommunikationsanlage und der genauen Erläuterung, welche Art von Daten einer Überwachung unterliegen[326], scheint diese Verordnung - im Vergleich mit der ÜVO - wesentlich ausgegorener. Aufgrund der dem österreichischen TKG entsprechenden Bestimmung[327] des § 87 (3) dTKG[328] erlassen, enthält das 27 Paragraphen umfassende Regelwerk auch umfassende Normen über die Anforderungen an technische Einrichtungen[329], die Beschaffenheit der bereitzustellenden Daten[330] und schließlich eine Bestimmung,[331] welche die Grundlage für die Schaffung einer „Technischen Richtlinie“ - zu erlassen von der „Regulierungsbehörde für Telekommunikation und Post“ unter Beteiligung der Verpflichteten, der Hersteller der technischen Einrichtungen, der berechtigten Stellen sowie der Hersteller der Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen - war. In dieser Richtlinie sollten die

---

[324] „Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung - TKÜV)“ dBGBl I 5/2002.

[325] § 2 (2) TKUEV.

[326] § 4 Z 15 TKUEV.

[327] In § 87 (3) dTKG wird das Bundesministerium für Post und Telekommunikation ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, die Erfüllung der Verpflichtungen nach § 87 (1) und (2) dTKG näher zu regeln. Dabei kann der Kreis der Verpflichteten und das zu fordernde Maß an Schutzvorkehrungen entsprechend der wirtschaftlichen Bedeutung der jeweiligen Telekommunikationsanlage festgelegt werden.

[328] BGBl I 1120/1996.

[329] § 6 TKUEV.

[330] § 7 TKUEV.

[331] § 11 TKUEV.

technischen Einzelheiten und Anforderungen, die zur physischen Einrichtung solcher Überwachungsanlagen nötig sind, näher erläutert werden.

Die technischen Umstellungen an den Telekommunikationsanlagen in Deutschland sollen bis 01.01.2005 erfolgreich abgeschlossen sein,[332] spezielle Ausnahmen bestehen aber für „Betreiber kleiner Telekommunikationsanlagen".[333]

Obwohl ebenfalls nicht kritiklos akzeptiert[334], stellt die TKUEV in Deutschland ohne Zweifel eine weitaus vollständigere Version dessen, was sich in Österreich unter dem Titel „Überwachungsverordnung" herausnimmt, die technischen Grundlagen für die effektive Umsetzung der Bestimmungen zur Fernmeldeüberwachung der Strafprozeßordnung zu gestalten, dar.

5.6.3. Umfang und Grenzen der Überwachung nach der ÜVO

Kritisiert wurde, neben den Bestimmungen zur Kostentragung[335], auf die in diesem Rahmen jedoch nicht näher eingegangen werden kann, daß der Begriff des „Betreibers" iSd § 2 Z 1 ÜVO nicht hinreichend klar definiert sei.

Aus der Legaldefinition gehe nicht eindeutig hervor, ob als Betreiber zum Beispiel auch Internet Service Provider bzw Verbindungsnetzbetreiber angesehen werden könnten. Betrachtet man den eigentlichen Wortlaut des § 14 TKG, auf den ja die ÜVO zur Bestimmung des Kreises der Verpflichteten verweist, so fallen darunter nur Anbieter mobiler Sprachtelefoniedienste bzw öffentlicher Mobilfunkdienste.

---

[332] § 26 TKUEV.

[333] § 21 TKUEV.

[334] ES existiert bereits seit dem 04.12.2001, also nahezu eineinhalb Monate vor Erlassung der TKUEV, ein „Entwurf für eine erste Verordnung zur Änderung der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation". Diese wurde vom Bundeskabinett am 12.06.2002 beschlossen (vgl dazu *http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=57&tdid=1704*).

[335] So hatten die Mobilfunker heftig gegen die verordnete Umrüstung der Netze auf Abhörtauglichkeit protestiert. Allein der Telekom würde die Umstellung auf den Abhörstandard ETSI ES 201 671 mindestens 500 Millionen ATS kosten. (Vgl dazu ausführlicher „Hunderte Millionen für die Überwachung", ORF-Futurezone vom 22.08.2001, im Internet unter *http://futurezone.orf.at/futurezone.orf?read=detail&id=76861*).

Meist wird die Ansicht vertreten, die ÜVO finde keine Anwendung auf Kommunikation im und unter Zuhilfenahme des Internet [336] und in der Stellungnahme der ARGE Daten zum Entwurf der ÜberwachungsVO[337] wird die Geltung der Bestimmungen nur für den Bereich der Sprachtelephonie anerkannt:

Die Überwachungsverordnung solle sich auf die Regelung der Überwachung der Telefongespräche beschränken; „Internet-Mailüberwachung muß als Einstiegsdroge in die flächendeckende Überwachung abgelehnt werden. Die Überwachung sollte ausschließlich der Aufklärung von Verbrechen vorbehalten sein. Andere Überwachungsgründe, etwa aus steuerlichen Gründen, sollten ausdrücklich ausgeschlossen werden".[338]

Nach Ansicht des Datenschützers Erich *Möchel*[339] *muß* die Überwachungsverordnung - zumindest teilweise - auch das Internet mit einschließen, nämlich dort, wo über Modem das Telefonnetz angewählt wird. Alle jene Daten, welche sich in solchem Telefonnetz befinden, seien es Daten der Sprachtelephonie oder aber jene des Internet-Traffic, würden nämlich im „Switch", also am Wählamt, gebündelt und gespeichert. Es ließe sich somit keine exakte Trennung vornehmen; bei jeder Überprüfung von Daten betreffend die Sprachtelephonie würden automatisch auch Internetverbindungen, welche mittels Modem getätigt wurden, mitüberprüft werden.

Dem ist zuzustimmen, ermöglicht es der im Rahmen der ÜVO umzusetzende ETSI-Standard „ES 201 671" eben noch nicht, den *gesamten* Inhalt jeder Internet-Kommunikation, gleichgültig um welche Art der Internet-Verbindung es sich handelt, während ihrer gesamten Dauer zu erfassen. Dennoch ist nach der eigentlichen Intention derjenigen Dokumente, auf denen die ÜVO fußt, zu fragen und diese zielen auf die

---

[336] Die Geltung dieser Verordnung auch für Internet-Provider wurde seitens des BM für Verkehr, Innovation und Technologie mit dem nicht sonderlich aussagekräftigen Argument verneint, „um keine Möglichkeit für deren Überwachung zu schaffen. Der uneingeschränkte Zugang auf die Festplatte sei nicht möglich, denn das wäre Hacking, und somit eine kriminelle Handlung." (Vgl die Parlamentskorrespondenz/02/17.01.2002/Nr 21, im Internet unter *http://www.parlinkom.gv.at/pd/pk/2002/PK0021.html*).

[337] „Stellungnahme der ARGE DATEN zur Abhörverordnung des Verkehrsministeriums" vom 23.02.2001, im Internet unter *http://www.ad.or.at/news/20010223.html.*

[338] Alles Lauschen....Telekom-ÜberwachungsVerordnung: K(l)eine Kulturgeschichte zur Überwachung, ARGE-Daten News vom 23.11.2001 unter *http://www.argedaten.at/news/20011123.html*.

Ermöglichung der Überwachung des *gesamten Datenverkehrs* ab. Man muß sich, um diese Aussage stützen zu können, lediglich die im Rahmen der Europäischen Union bzw des Europarats erlassenen oder vorgeschlagenen Ratsbeschlüsse, „Drafts“ oder „Discussion Papers“ vor Augen halten: Die ÜVO ist doch in Wirklichkeit nur deshalb geschaffen worden, um den ETSI-Standard zur Überwachung der Telekommunikation auch in Österreich rechtlich zu verankern. Und wenn man die Dokumente, die diesen Standard beschreiben betrachtet,[340] liegt es auf der Hand, das durch deren Umsetzung auch die „Enfopol“ Papiere – verdeckt unter dem Schutzmantel „Überwachungsverordnung“ - Eingang in die österreichische Rechtsordnung finden sollen. Denn sowohl das Dokument „Enfopol 98“, wie auch die aktuelle Resolution „Enfopol 55“ schreiben vor, daß „*all kinds of telecommunications may be subject to interception and/or data searches in relation to enquiries*”. Die Überwachungsverordnung darf also nicht als eigenständiges Regelwerk betrachtet werden; vielmehr ist sie nur das Ergebnis eines legistischen Entwicklungsprozesses, welcher auf EU-Ebene schon mit den „International User Requirements“[341] im Jahre 1994 seine Anfänge genommen hat und seine ersten Ergebnisse nun in Österreich bzw Deutschland auch auf nationaler Ebene in der Form von länderübergreifend aufeinander abgestimmten Regelungen präsentiert. Und im Verlauf der technischen Entwicklungen und der Erarbeitung eines ETSI-Standards, der in nächster Zeit jegliche Form von Internet-Überwachung technisch ermöglichen soll, werden auch die Regelungen der ÜVO entsprechend angepaßt werden müssen.

---

[339] „Big Brother hat ein neues Spielzeug“, ein Interview mit dem Datenschützer Ernst *Möchel*, in: Die Oberösterreichischen Nachrichten Online vom 09.02.2002, im Internet unter *http://www.nachrichten.at/wochenende/wochenende.asp?id=261417&ressort=Wochenende*.

[340] So nehmen sowohl die „Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies” (ETSI Technical Report 331 vom Dezember 1996), als auch das aktuelle Dokument “Handover interface for the lawful interception of telecommunications traffic“ (ETSI ES 201 671 V1.1.1 1999-07) Bezug auf die Enfopol. Dies erklärt sich dadurch, daß diese ursprünglich Bestandteil der „Enfopol-Papiere“ hätten sein sollen, später aber doch ausgegliedert und der Sektion „Lawful Intercpetion (SEC LI)“ zur Ausarbeitung übertragen wurden.

[341] Die „Requirements” vom 17.01.1995, „Council Resolution on the lawful interception of Telecommunications”. Erstmals veröffentlicht in: ABl. C 329 v 04.11.1996 S 1. Das Dokument ist auch unter den Namen „ENFOPOL 95“, „ENFOPOL 150“ oder „International User Requirements (IUR)“ bekannt.

Zusammenfassend bleibt also festzuhalten, daß die Verordnung „in ihrer Struktur zwar in Ordnung, in ihrer Detaillierung und ihrem Problemlösungskonzept jedoch mangelhaft ist, vor allem, weil alle bisher aus der Praxis bekannten Rahmenbedingungen und Erfahrungen der privaten Betreiber unberücksichtigt geblieben sind.“[342] Im Ergebnis wird diese Verordnung die Rechtssicherheit der Normunterworfenen (der TK-Dienstleister) erheblich reduzieren und etliche werden in „vorauseilendem Gehorsam teure, durch dieses Papier nicht klar genug geforderte Überwachungsinvestitionen tätigen und bei allen wird reichlich Verwirrung herrschen“.[343]

5.7. Überwachungsmaßnahmen im Militärbefugnisgesetz

Mit dem geplanten Reorganisationsbegleitgesetz[344] soll das Militärbefugnisgesetz[345] insofern geändert werden, als in § 22 ein neuer Abs 2a eingefügt werden soll, der wie folgt lautet:

- „Militärische Organe und Dienststellen...dürfen von den Betreibern öffentlicher Telekommunikationsdienste jene Auskünfte über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses verlangen, die diese Organe und Dienststellen als wesentliche Voraussetzung zur Erfüllung von Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr benötigen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.“

Die Befugnis zur Auswertung solcher Daten kommt militärischen Organen und Dienststellen, die mit Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr betraut sind, also beispielweise dem Heeresnachrichtenamt, zu (vgl § 22 Abs 1 MBG).

---

[342] VAT-Stellungnahme im Rahmen der Begutachtung zum Entwurf einer Überwachungsverordnung (ÜVO) – GZ 100048/IV-JD/00, 10.

[343] „Stellungnahme der ARGE DATEN zur Abhörverordnung des Verkehrsministeriums“ vom 23.02.2001, im Internet unter *http://www.ad.or.at/news/20010223.html.*

[344] „Bundesgesetz, mit dem das Wehrgesetz 2001, das Heeresdisziplinargesetz 1994, das Heeresgebührengesetz 2001, das Auslandseinsatzgesetz 2001, das Munitionslagergesetz, das Militär-Auszeichnungsgesetz, das Militärbefugnisgesetz und das Sperrgebietsgesetz 2002 geändert werden sowie das Tapferkeitsmedaillen-Zulagengesetz 1962 aufgehoben wird (Reorganisationsbegleitgesetz – REORGBG)“, 1119 BlgNR 21. GP.

[345] BGBl I 86/2000.

Es liegt hier der Verdacht nahe, daß sich der österreichische Gesetzgeber bei der Schaffung dieser Bestimmung einmal mehr an der Rechtssituation der Bundesrepublik Deutschland angelehnt hat, wo in der „Ersten Verordnung zur Änderung der Telekommunikations-Überwachungsverordnung“[346] eine Änderung der TKUEV[347] dahingehend normiert werden soll, als die „strategische Fernmeldekontrolle“ leitungsgebundener Telekommunikationsbeziehungen durch den *Bundesnachrichtendienst* jede Telekommunikation erfassen soll, die „von der zu überwachenden Rufnummer oder anderen Kennung ausgeht,...für die zu überwachende Rufnummer oder anderen Kennung bestimmt ist, oder in eine Speichereinrichtung, die der zu überwachenden Rufnummer oder anderen Kennung zugeordnet ist, eingestellt oder aus dieser abgerufen wird....“[348]

Die Kritiker der geplanten Bestimmung des § 22 Abs 2a MBG machten vor allem geltend, daß die sehr allgemein gehaltene Formulierung es militärischen Organen erlaube, künftig jederzeit personenbezogene Daten abzufragen. Es würden somit dem Militär umfassendere Zugriffsrechte gewährt als der Exekutive, die nur zur Abwehr gefährlicher Angriffe oder zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht Zugang zu derartigen Daten erhält. Eine Überprüfung der Angemessenheit derartiger Datenzugriffe würde dadurch de facto unmöglich gemacht.[349] Mit Bedacht sei die allgemeine Formulierung „militärische Organe“ gewählt worden, wodurch „jeder beliebige Wachmann im Dienst“ Zugriff auf Telekomdaten hätte, was einen „unverschämten Freibrief, der durch keinerlei Gefahren- oder Bedrohungsszenarien gerechtfertigt ist“, darstelle.[350]

---

[346] Kabinettbeschluss vom 12.06.2002, im Internet unter *http://www.bmwi.de/textonly/Homepage/download/telekommunikation_post/TKUEVAend1.pdf.*

[347] Vgl oben, 5.6.2.

[348] Siehe die näheren Ausführungen zum Beschluss unter: *http://www.bmwi.de/textonly/Homepage/download/telekommunikation_post/TKUEVAendBegr11.pdf.*

[349] Vgl die Stellungnahme des „Vereins für Internet-Benutzer Österreichs (VIBE!AT)“ vom 18.06.2002 unter *http://www.vibe.at/aktionen/200206/mil_18jun2002.html.*

[350] Vgl „Lauschgeil durchs Land“, ARGE-Daten News vom 17.06.2002 unter *http://www.argedaten.at/news/20020617.html*; siehe weiters: „HNA-Lobbyisten im Parlament“, Quintessenz-Newsticker vom 17.06.2002 unter *http://www.quintessenz.at/cgi-bin/index?funktion=view&id=000100002063.*

Die Überwälzung der Kosten für die Auskunftserteilung auf die betroffenen Dienstleister stelle eine bedenkliche Verlagerung der Aufwendungen für die Landesverteidigung hin zu privatwirtschaftlich geführten Unternehmen dar. Darüber hinaus erschwere diese Kostenverlagerung auch eine demokratische Kontrolle des Umfanges der jährlichen Datenzugriffe, da die diesbezüglich gemachten Angaben nicht anhand der Gesamtkosten auf Plausibilität geprüft werden könnten.[351]

5.8. Zur praktischen Relevanz der (neuen) Regelungen

Um die Notwendigkeit einer einheitlichen Regelung der Überwachung von Telekommunikation und Telekommunikationsinhalten zu verdeutlichen, muß man sich nur die Statistik der letzten Jahre darüber ansehen, wieviele Überwachungen des Fernmeldeverkehrs in Österreich angeordnet bzw durchgeführt wurden. Laut Sicherheitsbericht des BMI waren im Jahr 1999 1.228 Eingriffe in das „Telekommunikationsgeheimnis“ zu verzeichnen, 1998 waren es 804, davor (1997) nur 444.[352] Im August des Jahres 2001 erwartete sich die Telekom Austria bis Jahresende an die 2.000 bewilligte Überwachungsanträge.[353]

Alle diese Zahlen sind unter dem Aspekt zu sehen, daß über einen längeren Zeitraum alle bei jedem dieser Anschlüsse ein- und ausgehenden Anrufe überwacht und alle kontaktierten Nummern registriert und überprüft wurden. Die Angaben über die Gesamtzahl der genehmigten Anträge beruhen auf der Überlegung, daß jedem Antrag zumindest ein Telefonanschluß entspricht. Als Anträge auf Telefonüberwachung werden im Folgenden jene Überwachungen gezählt, die sich auf die Aufnahme und schriftliche Aufzeichnung des Inhalts eines Fernmeldeverkehrs beziehen. Die statistischen Erhebungen stellen dabei nicht auf die Zahl der Anträge, sondern auf die Zahl der tatsächlich überwachten Anschlüsse ab. Die Statistik betrifft genehmigte und

---

[351] Vgl die Stellungnahme des „Vereins für Internet-Benutzer Österreichs (VIBE!AT)“ vom 18.06.2002 unter *http://www.vibe.at/aktionen/200206/mil_18jun2002.html*.

[352] Quelle: „Justizministerium gegen Telekoms“, ORF-Futurezone vom 30.08.2001 unter http://futurezone.orf.at/futurezone.orf?read=detail&id=78331.

[353] Vgl „Überwachungs-Rekordjahr 2001“, ORF-Futurezone vom 31.08.2001 unter *http://futurezone.orf.at/futurezone.orf?read=detail&id=78431*.

durchgeführte Anträge auf Rufdatenrückerfassung oder Telefonüberwachung für das Jahr 2000.[354]

Rufdatenrückerfassungen und Inhaltsüberwachung (Zahl der Anschlüsse)

	OLG Wien	OLG Graz	OLG Linz	OLG Innsbruck	Österreich gesamt
Rufdatenrück-erfassung genehmigt	520	212	128	121	**981**
Rufdatenrück-erfassung durchgeführt	516	212	125	121	**974**
Telefonüber-wachungen genehmigt	132	25	145	41	**343**
Telefonüber-wachungen durchgeführt	131	25	139	41	**336**

Freilich sperren sich Internet-Provider und Telekommunikations-Diensteanbieter dagegen, Vermittlungsdaten, geschweige denn Inhaltsdaten, so lange aufzubewahren, daß eine Auswertung auch nach Verstreichen eines längeren Zeitraumes noch immer durchgeführt werden könnte:

Besonderes Aufsehen erregte im Februar 2002 die Kärntner Gendarmerie mit der Aufforderung an die heimischen Mobilfunkbetreiber, den Behörden seien rund 200.000 Vermittlungsdaten sofort zur Auswertung auszuhändigen:

Anlaß für dieses Vorgehen waren drei Einbrüche in Kärnten im Dezember und Januar 2002, bei denen Tresore „geknackt" wurden, die Täter dabei jedoch versehentlich ein Mobiltelefon am Tatort zurückgelassen hatten. Die Kärntner Polizei verlangte daraufhin von den Mobilfunkbetreibern, die Verbindungsdaten aller Handygespräche zu erhalten, die innerhalb von vierundzwanzig Stunden an den drei Tagen der Einbrüche geführt wurden. Zwar gab es keine inhaltliche Überwachung, zumal dies erst nach der Implementierung des ETSI-Standards gemäß der ÜVO technisch durchführbar wäre,

[354] Quelle der Statistik: „Anfragebeantwortung durch den Bundesminister für Justiz Dr. Dieter *Böhmdorfer* zur schriftlichen parlamentarische Anfrage betreffend Überwachungsverordnung" (2090/J 21. GP vom 07.03.2001) 2058/AB 21. GP vom 02.05.2001.

dennoch reichen aber die Rufdaten bereits aus, um Bewegungsprofile einzelner Personen zu erstellen.[355] Es sollte also festgestellt werden, wer, wann, von wo aus und mit wem telephoniert hat. Weil - bis auf das Handy - jede Spur von den Tätern fehlte, beantragte die Gendarmerie über die Staatsanwaltschaft beim Landesgericht Klagenfurt eine nachträgliche Auswertung der Rufnummern im Sendebereich der drei Tatorte.[356] Sowohl die Telekom, als auch die Mobilfunkanbieter „One" und „tele.ring" kamen der Aufforderung nach, der Exekutive die „erforderlichen" Daten zur Verfügung zu stellen. Einzig der Telekommunikationsdienstleister „max.mobil"[357] weigerte sich, dem richterlichen Beschluß nachzukommen[358] und hat statt dessen am 06.02.2002 eine Klage gegen die Überwachungsverordnung, im speziellen gegen die (fehlenden) Kostentragungsbestimmungen, beim Verfassungsgerichtshof eingebracht.[359]

Aus meiner Sicht problematisch ist, daß zwar durch das „StrÄG 2002" die Problematik der Telekommunikationsüberwachung stärker thematisiert wurde, die Differenzierung zwischen der *Echtzeit-Erhebung von Verbindungsdaten* und dem *Abfangen von Inhaltsdaten* auf der einen und die Speicherung und *rückwirkende Erfassung von Vermittlungs- und Inhaltsdaten* auf der anderen Seite nicht in einer Form ins österreichische Recht übertragen wurde, die keine Abgrenzungsschwierigkeiten mehr offen läßt. Statt dessen wurde mit der Fassung des § 149a Abs 1 Z 1 lit b StPO idF StRÄG 2002, wonach unter „Überwachung der Telekommunikation" die „Feststellung, welche Teilnehmeranschlüsse Ursprung oder Ziel einer Telekommunikation *sind* oder

---

[355] Vgl *Zarzer*, Panzerknackern auf der Spur, Telepolis, Das Magazin für Netzkultur vom 09.02.2002 unter http://www.heise.de/tp/deutsch/inhalt/te/11802/1.html.

[356] Vgl die Online-Nachrichten auf Kärnten@ORF.at vom 07.02.2002 unter *http://kaernten.orf.at/oesterreich.orf?read=detail&channel=9&id=182307*.

[357] Nunmehr: „t-mobile".

[358] Im Oktober des Jahres 2001 spitzte sich der Streit zwischen max.mobil und dem Innenministerium zu. „Die Firma max.mobil weigert sich stets bei der Überwachung des Fernmeldeverkehrs im erforderlichen Ausmaß mitzuwirken", hieß es damals in einem offiziellen Statement des BMI (vgl „max.mobil und Innenministerium im Clinch", ORF-Futurezone vom 08.10.2001 unter *http://futurezone.orf.at/futurezone.orf?read=detail&id=86091*). Siehe dazu auch die „Anfrage des Abgeordneten *Pilz*, Freundinnen und Freunde an den Bundesminister für Inneres betreffend Bekämpfung des Datenschutzes mit allen Mitteln", 2906/J 21. GP vom 10.10.2001.

[359] Eine Entscheidung diesbezüglich ist bis dato (September 2002) noch ausständig.

waren...“ zu verstehen ist, eine Regelung geschaffen, welche eben *nicht* zwischen der *Auswertung bereits gespeicherter* und der *Überwachung von gerade stattfindender* Kommunikation unterscheidet und letztere in bestimmten Fällen auch ohne Zustimmung des Inhabers eines Endgeräts für zulässig erklärt. Man könnte nun dahingehend argumentieren, daß es ohnehin einerlei sei, bereits erfolgten, oder aber aktuell geschehenden Datentransfer zu überwachen, schließlich geht es ja nur um Verbindungs- nicht aber um Inhaltsdaten.
Jedoch könnte eine Erleichterung der Anwendungsvoraussetzungen zur *Echtzeit-Erfassung von Verbindungsdaten* leicht dazu mißbraucht werden, um jene Maßnahmen durchzuführen, die letztlich in einer Kontrolle der *Inhalte einer Verbindung* (der Kommunikation) münden: Es ergibt sich dann nämlich in den Fällen der „bloßen“ Erfassung von Verbindungsdaten möglicherweise *automatisch* auch eine Überwachung des Inhalts: Ein Beispiel hiefür ist die Überwachung von „Chat-Rooms“ im IRC: Wenn beobachtet werden soll, wer sich in einen Kanal, der dafür bekannt ist, Umschlagplatz für kinderpornographisches Material zu sein, einloggt, dann ist es ein leichtes, auch den Inhalt der Diskussion mitzuverfolgen, da ja der Ermittler in einem solchen Fall nicht nur registriert, *wann* und *welche* Person den virtuellen Raum betritt, sondern auch *worüber* sie sich mit anderen Personen unterhält. In einem solchen Fall geht die Überwachung von Verbindungsdaten mit jener des Inhalts Hand in Hand.

Zusammenfassend läßt sich aber dennoch festhalten, daß die österreichische Rechtsordnung, durch spezielle Auslegung bereits bestehender Normen oder die Schaffung neuer Rechtsvorschriften im Verlauf der letzten Jahre, bereits über etliche Regelungen verfügt, die sowohl die Telekommunikation im gesamten, als auch das Internet im speziellen einer Überwachung zugänglich machen. Freilich, diese „neuen“ Regelungen mögen noch unausgegoren und vor allem deren technische Umsetzung noch nicht bis ins letzte Detail durchdacht sein, dennoch zeichnen sich – aufgrund der aktiven Mitwirkung von Strafverfolgungsbehörden, Telekommunikationsdiensteanbietern und Datenschützern – in naher Zukunft Kompromisse ab, die den Forderungen all dieser betroffenen Parteien Rechnung tragen und auch dem Anwender – hoffentlich nicht unberechtigt - die Angst vor der „totalen Überwachung“ der Telekommunikation nehmen werden.
Notwendig ist dies allemal, nicht zuletzt aufgrund der Ausarbeitung diverser Regelungen zur Bekämpfung von Internet-Kriminalität auf europäischer Ebene, zu

deren innerstaatlicher Umsetzung sich auch Österreich verpflichtet hat oder in Zukunft verpflichten wird.

.

Aichinger: Der Lauschangriff für Sicherheits- und Kriminalpolizei, JAP 2/1996, 119.

ders: Neue Fahndungsmethoden zur Bekämpfung organisierter Kriminalität, Wien 1997.

ders: Bundesgesetz zur Einführung besonderer Ermittlungsmaßnahmen in die StPO, JAP 1997/98, 56.

Bär: EDV-Beweissicherung im Strafverfahrensrecht, CR 1998, 434.

Berka: Lehrbuch Grundrechte: ein Arbeitsbuch für das juristische Studium mit Hinweisen zur grundrechtlichen Fallbearbeitung, Wien 2000.

Bertel/Schwaighofer: Österreichisches Strafrecht, Besonderer Teil I; §§ 75 bis 168 StGB[6], Wien 2000.

dies: Österreichisches Strafrecht, Besonderer Teil II; §§ 169 bis 321 StGB[4], Wien 1999.

Brandl/Mayer-Schönberger: Datenschutz und Internet, ecolex 1998, 132.

Brandstetter: Die Fernmeldeüberwachung öffentlicher Telefonzellen, JBl 1984, 475.

Brandstetter/Schmid: Kommentar zum Mediengesetz: auf Grundlage des Kommentars zum Mediengesetz von Hartmann und Rieder[2], Wien 1999.

Burgstaller: Anmerkung zu OGH 18.01.2001, 12 Os 152/00, JBl 2001, 536.

Davy/Davy: Staatliche Informationssammlung und Art 8 MRK, JBl 1985, 656.

Dearing: Sicherheitspolizei und Strafrechtspflege – Versuch einer Bestimmung des Verhältnisses zweier benachbarter Rechtsgebiete, in: *Fuchs*/*Brandstetter* (Hrsg), FS Winfried *Platzgummer*, Wien-New York 1995, 246.

ders et al: Kriminalpolizei und Strafprozessreform. Konzept einer Arbeitsgruppe StPO-Reform des Bundesministeriums für Inneres zu einem sicherheitsbehördlichen Ermittlungsverfahren (Juristische Schriftenreihe Bd 84), Wien 1995.

ders: Sicherheitspolizeigesetz, Wien 1999.

Determann: Kommunikationsfreiheit im Internet – Freiheitsrechte und gesetzliche Beschränkungen, Baden-Baden 1999.

Edelbacher: Das Tor zum Osten, Der Kriminalbeamte 10/1993, 8.

Ellinger: Die Reform des strafprozessualen Vorverfahrens, Wien 1993.

ders: Der „Lauschangriff" - Begriff und Manipulation, in: Der Kriminalbeamte 4/1994, 13.

Foregger/**Fabrizy**: Strafgesetzbuch: StGB samt den wichtigen Nebengesetzen; Kurzkommentar; mit einer Einführung und Erläuterungen unter Berücksichtigung der Rechtsprechung des Obersten Gerichtshofes und des Schrifttums[7], Wien 1999.

Fuchs: Zum Entwurf eines Bundesgesetzes über besondere Ermittlungsmaßnahmen zur Bekämpfung organisierter Kriminalität, in: Strafrechtliche Probleme der Gegenwart, Bd 85 der Schriftenreihe des BMJ, Wien 1996, 263.

ders: Österreichisches Strafrecht, Allgemeiner Teil I[4], Wien 2000.

ders: Verdeckte Ermittler – anonyme Zeugen, ÖJZ 2001, 495.

Funk: Das neue Sicherheitspolizeirecht – Kodifikation und Reform einer klassischen Verwaltungsmaterie, JBl 1994, 137.

ders: Sicherheitspolizeiliche Maßnahmen zur Bekämpfung organisierter Kriminalität, JRP 1996, 26.

ders: Zur Reform des strafrechtlichen Vorverfahrens, Verfassungsrechtliche Aspekte und Beziehungen zum Sicherheitspolizeirecht, in: Entwicklungslinien im Straf- und Strafprozeßrecht, Bd 82 der Schriftenreihe des BMJ, Wien 1996, 81.

Hager: Gedanken zur Reformfreude des Strafgesetzgebers, JBl 1994, 710.

Hanusch: Kommentar zum Mediengesetz, Wien 1998.

Hauenschild: Das Zusammenwirken der Strafverfolgungsbehörden – verfassungsrechtliche Fragen zum Entwurf der Strafprozeßreform, RZ 2000, 186.

Hauer/Keplinger: Sicherheitspolizeigesetz samt „Lauschangriff", „Rasterfahndung" und Polizeikooperationsgesetz, Wien 1997.

dies: Sicherheitspolizeigesetz: Kommentar[2], Wien 2001.

Hauptmann: Unkonventionelle Gedanken zu einem Strafrechtsänderungsgesetz 2000, in: Strafrechtliche Probleme der Gegenwart, Bd 84 der Schriftenreihe des BMJ, Wien 1995, 125.

Hinterhofer: Strafrecht Besonderer Teil II[3], Wien 2002.

Hobert: Datenschutz und Datensicherheit im Internet: Interdependence und Korrelation von rechtlichen Grundlagen und technischen Möglichkeiten, Frankfurt 1998.

Höne: Grundrechte im Internet, in: ÖJK (Hrsg), Grundrechte in der Informationsgesellschaft, Wien 2001, 79.

Höpfel/Ratz: Wiener Kommentar zum Strafgesetzbuch[2] 16. Lieferung §§ 274-287, bearbeitet von *Steininger*, Wien 2000.

dies: Wiener Kommentar zum StGB[2] 21. Lieferung: § 61 bearbeitet von *Höpfel*, §§ 62-67 bearbeitet von *Kathrein*, Wien 2000.

Hund: Der Einsatz technischer Mittel in Wohnungen – Versuch einer verfassungskonformen Lösung, ZRP 1995, 334.

Jaburek/Schmölzer: Computer-Kriminalität (EDV und Recht, Band 2), Wien 1985.

Keplinger: Handbuch zum Sicherheitspolizeigesetz, Eisenstadt 1993.

Kienapfel: Bildung einer kriminellen Organisation (278a Abs 1 StGB), JBl 1995, 615.

Kienapfel/Höpfel: Grundriß des österreichischen Strafrechts, AT[9], Wien 2001.

Kienapfel/Schmoller: Grundriß des österreichischen Strafrechts, BT III – Delikte gegen sonstige Individual-, und Gemeinschaftswerte[8], Wien 1999.

Kind: Bekämpfung der Kriminalität im Internet – Vortrag aufgrund der Tagung des BKA Wiesbaden am 15./16.02.2000, im Internet unter *http://www.bka.de/aktuell/agenda98/agenda.html.*

***Leukauf/Steininge*r**: Kommentar zum Strafgesetzbuch[3], Wien 1992.

Mayerhofer: Das österreichische Strafrecht, erster Teil: Strafgesetzbuch[5], Wien 2000.

Mayer-Schönberger: Das Immaterialgüterrecht in der Informationsgesellschaft – Ein Essay, ÖBl 2000, 51.

Mayer-Schönberger/Brandl: Telekommunikationsgesetz und Datenschutz, ecolex 1998, 272.

Michel/Wessely: Strafrecht, Allgemeiner Teil, Wien 1999.

Miklau/Pilnacek: Optische und akustische Überwachungsmaßnahmen zur Bekämpfung schwerer organisierter Kriminalität („Lauschangriff") – Paradigmenwechsel im Verfahrensrecht? JRP 5/1997, 286.

Möchel: Lachnummer ISP Austria, Telepolis, das Magazin für Netzkultur vom 21.2.1999 unter *http://www.telepolis.de/tp/deutsch/inhalt/te/1924/1.html.*

ders: Die ETSI Dossiers – Europäische Standards für das Abhören digitaler Netze, c't 7/2001, 58.

ders: Die ETSI-Dossiers, Teil 2– Der Griff der Geheimdienste nach dem Internet, c't 9/2001, 54.

ders: Die ETSI-Dossiers, Teil 3 – Abhörstandards für digitale Netze vor der Verabschiedung, c't 17/2001, 78.

ders: Die ETSI Dossiers, Teil 4 - Lauscher am Netz, c't 4/2002, 80.

ders: ENFOPOL: EU-Abhörstandards für die Telekommunikationsnetze, Telepolis, das Magazin für Netzkultur vom 11.02.2002 unter *http://www.heise.de/tp/deutsch/special/enfo/11818/1.html.*

Näser: Audio-Kompression mit Real *Audio*/Real *Media* und anderen Verfahren, im Internet unter *http://staff-www.uni-marburg.de/~naeser/audio.htm.*

Nening-Schöfbänker: Potentiell strafrechtlich relevante Vorkommnisse im Internet und der österreichischen „Netz-Landschaft", in *Maier-Rabler/Mayer-Schönberger/Nening-Schöfbänker/Schmölzer:* Netz ohne Eigenschaften Wien 1996, 14.

Noll: Sicherheitspolizeigesetz (SPG), Wien 1988.

Pleischl: Reform des strafprozessualen Vorverfahrens aus der Sicht der Justiz, in: Kritik und Fortschritt im Rechtsstaat, 21. Tagung der ÖJK 1994, 13.

Pleischl/Soyer: Strafgesetzbuch und Jugendgerichtsgesetz, Wien 1997.

Plöckinger: Zur Zuständigkeit österreichischer Gerichte bei Straftaten im Internet, ÖJZ 2001, 798

ders: Anmerkung zu OLG Wien 10.09.2001, 24 Bs 242/01, MR 2001, 282.

Pracher: Stellungnahme zum Entwurf einer Strafprozeßnovelle 2001 aus der Sicht eines Telekombetreibers, im Internet unter *http://www.it-law.at/papers/pracher-stpo.pdf*.

Primig: Software-Piraterie im Internet, Diplomarbeit, Graz 1999.

Rami: Anmerkung zu OLG Wien 09.03.2001, 21 Ns 42/01, MR 2001, 155.

Reindl: Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren, JBl 1999, 791.

dies: Telefonüberwachung zweimal neu? JBl 2002, 69.

Schmoller: Geändertes Erscheinungsbild staatlicher Verbrechensbekämpfung, ÖJZ 1996, 21.

Schmölzer: Prozessuale Zwangsmittel im Fernmeldewesen – Beschlagnahme oder Überwachung (§§ 143 ff, 146, 149a, 149b StPO), RZ 1988, 247.

dies: Die unbefugte Verwendung einer fremden Bankomatkarte, EDVuR 1990, 30.

dies: Strafrechtliche Situation der Informationsregulierung, in: *Maier-Rabler/Mayer-Schönberger/Nening-Schöfbänker/Schmölzer*, Netz ohne Eigenschaften, Wien 1996, 97.

dies: Computernetze und Strafrecht – eine internationale Herausforderung, in: FS *Posch*, Wien 1996, 321.

dies: Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr – Anmerkungen zu OGH 6.12.1995, 13 Os 161/95, JBl 1997, 211.

dies: Cyberstructure: Die „Fangschaltung“, Juridikum 1997, 43.

dies: Internet und Strafrecht, in: Strafrechtliche Probleme der Gegenwart, Bd 91 der Schriftenreihe des BMJ, Wien 1997, 129.

Schmölzer/Mayer-Schönberger: Das Telekommunikationsgesetz 1997 – Ausgewählte rechtliche Probleme, ÖJZ 1998, 378.

Schulzki-Haddouti: EU-Parlament verabschiedet Enfopol-Überwachungspläne, Telepolis, das Magazin für Netzkultur vom 10.05.1999 unter *http://www.heise.de/tp/deutsch/special/enfo/6404/1.html*

dies: Europäisches Rechtshilfeübereinkommen kurz vor der Verabschiedung, Telepolis, das Magazin für Netzkultur vom 26.05.2000 unter *http://www.heise.de/tp/deutsch/special/enfo/6807/1.html*.

dies: Vom Ende der Anonymität - Die Globalisierung der Überwachung^2, Hannover 2001.

dies: Desaster Inpol-neu - Das neue Polizei-Informationssystem: viel zu teuer, viel zu langsam, c't 24/2001, 108.

dies: Europäisches Parlament gegen Speicherung von Verbindungsdaten, Telepolis, das Magazin für Netzkultur vom 19.04.2002 unter *http://www.heise.de/tp/deutsch/inhalt/te/12355/1.html.*

dies: Bundesrat segnet Vorratsspeicherung ab, Telepolis, das Magazin für Netzkultur vom 31.05.2002 *unter http://www.heise.de/tp/deutsch//inhalt/te/12642/1.html.*

Sieber: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (1) Neue Herausforderungen des Internet, JZ 1996, 431, im Internet unter *http://www.jura.uni-muenchen.de/sieber/article/STVIPDT/Svi01.htm.*

ders: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (2) Neue Herausforderungen des Internet, JZ 1996, 494, im Internet unter *http://www.jura.uni-muenchen.de/sieber/article/STVIPDT/Svi02.htm.*

ders: Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I); Zur Umsetzung von §5 TDG am Beispiel der Newsgroups des Internet, CR 1997, 581.

ders: Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II); Zur Umsetzung von § 5 TDG am Beispiel der Newsgroups des Internet, CR 1997, 656.

ders: Verantwortlichkeit im Internet – Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen, zugleich eine Kommentierung von § 5 TDG und § 5 MDStV, München 1999.

ders: Staatliche Regulierung, Strafverfolgung und Selbstregulierung: Für ein neues Bündnis zur Bekämpfung rechtswidriger Inhalte im Internet - Bericht erstellt für die Bertelsmann-Stiftung, in: *Waltermann*/*Machill* (Hrsg), Verantwortung im Internet: Selbstregulierung und Jugendschutz, Gütersloh 2000, 345–432, im Internet unter:
http://www.jura.uni-muenchen.de/sieber/article/bertelsmann/bertelsmann_deutsch.pdf.

ders: Die Bekämpfung von Hass im Internet: Technische, rechtliche und strategische Grundlagen für ein Präventionskonzept – Zugleich eine rechtspolitische Bewertung von BGH NJW 2001, 624, ZRP 2001, 97, im Internet unter *http://www.jura.uni-wuerzburg.de/sieber/article/article_online_deutsch.htm*.

Soyer: Lauschangriffe in Österreich, JRP 1994, 270.

Spindler: Deliktsrechtliche Haftung im Internet – nationale und internationale Rechtsprobleme, ZUM 1996, 533.

Trawnicek/Lepuschitz: Das neue österreichische Sicherheitspolizeigesetz[3], Wien 2000.

ders: Strafrecht Allgemeiner Teil I[2], Wien 1994.

Unterwaditzer: Zur Frage der „verdeckten Fahndung", ÖJZ 1992, 250.

Walter/Mayer: Grundriß des österreichischen Bundesverfassungsrechts[9], Wien 2000.

Weiß: Zur straf- und medienrechtlichen Haftung für Ehrenbeleidigungen, MR 1990, 10.

Welp: Erkenntnisse aus präventiv-polizeilichem Lauscheingriff, NStZ 1995, 601.

Wessely, *Wolfgang*: Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet, ÖJZ 1996, 612.

ders: Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491.

Wiederin: Einführung in das Sicherheitspolizeirecht, Wien 1998.

ders: Kommentierung von Art 10a StGG, in: *Korinek*/*Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht. Textsammlung und Kommentar, 4. Lieferung, Wien 2001.

Zanger: Telekommunikationsgesetz: Kommentar, Wien 2000.

Zankl: Der Entwurf zum E-Commerce-Gesetz, NZ 2001, 325.

ders: E-Commerce-Gesetz, Kommentar und Handbuch, Wien 2002.

ders: Online-Handbuch für E-Commerce und Internetrecht, im Internet unter *http://www.e-zentrum.at/handbuch/buch-cont.htm*.

Zarzer: Österreich übernimmt Lauschangriff und Rasterfahndung ins Dauerrecht, Telepolis, das Magazin für Netzkultur vom 13.10.2001 unter *http://www.heise.de/tp/deutsch/inhalt/te/9806/1.html*

dies: Panzerknackern auf der Spur, Telepolis, das Magazin für Netzkultur vom 09.02.2002 unter *http://www.heise.de/tp/deutsch/inhalt/te/11802/1.html*.