

Malaika-D. Nolde
Schiersteiner Str. 28
65187 Wiesbaden

Abbestr. 21
30519 Hannover

m.nolde@CriminalLaw.de
Matrikel-Nr. 2153861 (EULISP VI)

Abschlußarbeit
im Rahmen des
Ergänzungsstudiengangs Rechtsinformatik

Universität Hannover / University of Strathclyde Glasgow
Sommersemester 2002 / Wintersemester 2002/03

Ermittlungsmaßnahmen im Internet
- Polizeiliche Tätigkeit im Vorfeld von Anfangsverdacht
und konkreter Gefahr -

*They that can give up essential liberty
to obtain a little temporary safety
deserve neither liberty nor safety.*

Benjamin Franklin, Historical Review of Pennsylvania, 1759

If privacy is outlawed, only outlaws will have privacy.

Phil Zimmermann, Why do you need PGP?, 1991

Gliederung

Einführung	1
I. Internet als Panopticon	1
II. Rechtsinformatik als methodischer Zugang	2
1) Voraussetzungen der Informationstechnologie	3
2) Anwendungen der Informationstechnologie	3
3) Folgen der Informationstechnologie	3
III. Gang der Darstellung	4
IV. Eingrenzung des Themas	5
A. Technische Möglichkeiten und Grenzen der Internetermittlung	6
I. WWW	6
II. File-Transfer-Protocol (FTP)	7
III. Internet Relay Chat (IRC)	8
IV. Usenet / Newsgroups	9
V. Möglichkeiten des Zugangsschutzes	11
VI. Identitätsbestimmung anhand des Datenschattens	12
B. Tätigkeits- und Interessenschwerpunkt der Ermittler	15
I. PKS	16
II. Periodischer Sicherheitsbericht	16
III. Fallzahlen der ZaRD, 1999 – 2001	17
IV. Problematik der Deliktsfokussierung	18
V. Zusammenfassung zum Lagebild	20
1) § 184 III StGB – „harte“ Pornographie	21
2) §§ 86, 86 a, 130 StGB – Staatsschutz	21
3) Arznei- und Betäubungsmittelgesetz	22
C. Eingriffsqualität der Internet-Recherche	22
I. Recherchedienste	22

1) Bayern	22
2) BKA	23
II. Vorgehensweise der Ermittler	23
1) Surfen nach der „Jedermann-Methode“	23
2) Einsatz von Überwachungstools	24
III. Grundrechtsschutz im Internet – Schutzbereich und Eingriff	26
1) Art. 5 I GG	26
a) Schutzbereich	26
b) Eingriff	26
2) Art. 8 I GG	27
3) Art. 10 I GG	29
a) Schutzbereich	29
b) Eingriff	31
4) Art. 2 I i.V.m. 1 I GG	31
a) Schutzbereich des informationellen Selbstbestimmungsrechts	31
aa) Sphärentheorie	31
bb) Abkehr von der Sphärentheorie – Recht auf informationelle Selbstbestimmung	32
b) Eingriff	33
aa) Einwilligung	33
(1) Testkäufer und virtuelles Hausrecht	34
(2) Übertragbarkeit auf das ISR	35
bb) Zwischenergebnis nach der sog. Eingriffstheorie	38
cc) Ziel des Volkszählungsurteils und status quo der Zielerreichung	39
dd) Lösungen auf der Ebene des Eingriffsbegriffs	42
(1) Zugänglichkeit der Daten	42
(2) Erfordernis konkreter Grundrechtsgefährdung	43

(3) Eingrenzung über den Begriff der Erhebung	43
(4) Eingrenzungskriterium der Überschaubarkeit	45
c) Eingriffsqualität der einzelnen Maßnahmen	45
aa) WWW	46
bb) FTP	46
cc) IRC	47
dd) Eingriffsqualität des Einsatzes von Ermittlungstools	49
5) Art. 13 I GG	51
a) Schutzbereich	51
b) Eingriff	52
6) Art. 3 I GG	53
IV. Zusammenfassung zur Eingriffsqualität	53
D. Aufgabenzuweisungsnorm	53
I. Gefahrenabwehr oder Strafverfolgung – tertium non datur?	53
II. Funktion einer Aufgabenzuweisungsnorm	55
III. Aufgabenbereich der Bayerischen Polizeibehörde	55
1) Strafverfolgung	56
2) Klassische Gefahrenabwehr	56
3) Entstehung einer dritten polizeilichen Aufgabenkategorie	57
a) Vorbereitung auf die Gefahrenabwehr	58
b) „Vorbeugende Bekämpfung von Straftaten“	59
aa) Verhütung von Straftaten	60
(1) Prävention durch Repression ?	60
(2) Präventivwirkung der Internetstreife	61
bb) Strafverfolgungsvorsorge	65
4) Rechtmäßigkeit der Erweiterung des Gefahrenabwehrbegriffs	67
a) Wortlaut von Musterentwurf und Landespolizeigesetzen	68

b) Gesetzgebungskompetenz der Länder	69
aa) Art. 70, 72, 74 I Nr. 1 GG	69
bb) Problematik der konkurrierenden Gesetzgebung	71
(1) Anhaltspunkte in der StPO	71
(2) Konsequenzen einer Regelung im Polizeirecht	73
(a) Sachleitungsbefugnis der StA	73
(b) Grenzenloses Vorfeld	74
(c) Verabschiedung des Anfangsverdachts	75
(d) Beschränkungen in d. Befugnisnormen	75
5) Zusammenfassung	76
IV. Aufgabenzuweisungsnorm der BKA-Streife	77
1) Regelung im BKAG	77
2) Gesetzgebungskompetenz	79
V. Vorfeldtätigkeit und Trennungsgebot	79
1) Wesen des Trennungsgebots	80
2) Trennungsgebot de lege lata	80
3) Verbindlichkeit des Trennungsgebots	80
a) Polizeibrief als Verfassungsbestandteil	81
b) Trennungsgebot als Folge des Rechtsstaatsprinzips	81
4) Folge für die Vorfeldermittlung	82
5) Zwischenergebnis	83
E. Ermächtigungsgrundlagen der Maßnahmen mit Eingriffsqualität	83
I. Bayern	84
II. BKA	84
F. Vorgehen zur Identifizierung des Verantwortlichen	86
I. § 89 VI TKG	86
II. § 7 II BKAG	88

G. Rechtmäßigkeit vor dem Hintergrund möglicher grenzüberschreitender Ermittlung	89
I. Prinzip der formellen Territorialität	89
II. Eingriff in die Gebietshoheit eines fremden Staates	91
III. Einordnung der Internetstreife	91
1) Streifengang	91
2) Anfrage beim Zugangs-Provider	93
IV. Probleme der Rechtshilfe und angestrebte Lösung	94
H. Zusammenfassung und Schlußbetrachtung	95
I. Zusammenfassung	95
II. Schlußbetrachtung	96

Literaturverzeichnis

Ahlf / Daub / Lersch / Störzer

Bundeskriminalamtgesetz

Stuttgart 2000

Appel, Hummel, Hippe (Hrsg.)

Die Neue Sicherheit – Vom Notstand zur Sozialen Kontrolle

Köln 1988

Artzt

Doppelfunktionales Handeln des Polizeivollzugsdienstes

Kriminalistik 1998, S. 353 ff.

Bär

Strafrechtliche Kontrolle in Datennetzen

MMR 1998, S. 463 ff.

Bär

Auskunftsanspruch über Telekommunikationsdaten nach den neuen §§ 100 g, 100 h StPO

MMR 2002, S. 358 ff.

Bär

Aktuelle Rechtsfragen bei strafprozessualen Eingriffen in die Telekommunikation

MMR 2000, S. 472 ff.

Bär

Auf dem Weg zur „Internet-Polizei“?

in: Bäumler (Hrsg.), „Polizei und Datenschutz“, S. 167 ff.

Bäumler

Eine sichere Informationsgesellschaft ?

DuD 2001, S. 348 ff.

Bäumler

Öffentliche Sicherheit und Datenschutz

<<http://www.datenschutzzentrum.de/material/themen/divers/lverwg30.htm>>

Bäumler (Hrsg.)

„Polizei und Datenschutz“ – Neupositionierung im Zeichen der Informationsgesellschaft
Neuwied – Kriftel – Berlin, 1999

Bäumler (Hrsg.)

E-Privacy

Braunschweig/Wiesbaden 2000

Bizer

Verschlüsselung und staatlicher Datenzugriff

in: Büllsbach (Hrsg.), Datenschutz im Telekommunikationsrecht, S. 245 ff.

Bleyenbergl

Das Internet als Panopticon

<<http://www.uni-muenster.de/PeaCon/zurawski/panopticum/interpan.htm>>

Bock

Kriminologie

2. Auflage, München 2000

Breuer

Anwendbarkeit des deutschen Strafrechts auf exterritorial handelnde Internet-Benutzer

MMR 1998, S. 141 ff.

Büllsbach (Hrsg.)

Datenschutz im Telekommunikationsrecht

Köln 1997

Bundeskriminalamt (Hrsg.)

Festschrift für Horst Herold zum 75. Geburtstag

Wiesbaden 1998

Christensen

Taschenkontrolle im Supermarkt und Hausverbot – BGHZ 124, 39

JuS 1996, S. 873 ff.

Denninger

Die Trennung von Verfassungsschutz und Polizei und das Grundrecht auf informationelle
Selbstbestimmung

ZRP 1981, S. 231 ff.

Derksen

Perspektiven für eine wirksame Bekämpfung von Rechtsradikalismus und Rassismus im Internet
ZFIS 1999, S. 150 ff.

Deutsch

Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei
Heidelberg 1992

Dix

Internationale Aspekte
in: Bäumler (Hrsg.), E-Privacy, S. 93 ff.

Duttge

Was bleibt noch von der Wissenschaftsfreiheit? - Zur Hypertrophie des Datenschutzes
NJW 1998, S. 1615 ff.

Eckhardt

Neue Regelungen der TK-Überwachung
DuD 2001, S. 197 ff.

Erfurth

Verdeckte Ermittlungen: Problemlösung durch das OrgKG ?
Frankfurt am Main 1997

Feltes (Hrsg.)

Das Modell New York: Kriminalprävention durch Zero Tolerance
<http://www.felix-verlag.de/download/Band_12.doc>

Fiehl

Erfahrungen bei der Recherche in den Datennetzen
der kriminalist 1999, S. 2 ff.

Fiehl

Bekämpfungssituation aus der Sicht der Polizei
<http://www.bka.de/aktuell/agenda98/vtr98/vtr_fieh198.html>

Floerecke

Kriminalprävention durch Polizei?
Kriminologisches Journal 1983, S. 167 ff.

Foucault

Überwachen und Strafen

3. Auflage, Frankfurt am Main 1979

Germann

Gefahrenabwehr und Strafverfolgung im Internet

Berlin 2000

Göppinger

Kriminologie

5. Auflage, München 1997

Götte

Spurensuche im Internet

Deutsche Polizei 11/1998, S. 6 ff.

Graf

Internet: Straftaten und Strafverfolgung

DRiZ 1999, S. 281 ff.

Graf

Befugnisse und Grenzen der Ermittlungsbehörden

Deutsches Polizeiblatt (DPolBl) 4/2001, S. 6 ff.

Graf

Möglichkeiten zur Verbesserung der Zusammenarbeit zwischen Internet-Service-Providern und
Strafverfolgungsbehörden

<http://www.bka.de/aktuell/agenda98/vortrag_graf.doc>

Gruhler

Das Ende der „totalen“ Freiheit im Internet

Marburg 1998

Gusy

Polizeirecht

4. Auflage, Tübingen 2000

Gusy

Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten

ZRP 1987, S. 45 ff.

Hanack

Hausfriedensbruch durch Testkäufer – LG Frankfurt NJW 1963, 1022
JuS 1964, S. 352 ff.

Heinzmann / Ochsenbein

Strafrechtliche Aspekte des Internet
Kriminalistik 1998, S. 513 ff., S. 599 ff.

Hilbrans

Erfassungskonflikte im Cyberspace
Datenschutz Nachrichten 2/2001, S. 16 ff.

Hilgendorf

Die Neuen Medien und das Strafrecht
ZStW 2001, S. 650 ff.

Hoeren / Sieber (Hrsg.)

Handbuch Multimedia Recht
München, Losebl., Stand: Dezember 2001

Hoffmann-Riem

Informationelle Selbstbestimmung in der Informationsgesellschaft
- Auf dem Weg zu einem neuen Konzept des Datenschutzes -
AöR 123 (1998), S. 513 ff.

Holznapel / Enaux / Nienhaus

Grundzüge des Telekommunikationsrechts
2. Auflage, München 2001

Huber

Ermittlung und Strafverfolgung bei Internetattacken
DSWR 2000, S. 63 ff.

Hund

Überwachungsstaat auf dem Vormarsch – Rechtsstaat auf dem Rückzug
NJW 1992, S. 2118 ff.

Hund

Polizeiliches Effektivitätsdenken contra Rechtsstaat
ZRP 1991, S. 463 ff.

Ipsen

Völkerrecht

4. Auflage, München 1999

Janovsky

Internet und Verbrechen

Kriminalistik 1998, S. 500 ff.

Kant

Internet-Streifen

Bürgerrechte und Polizei / Cilip 1/2002, S. 29 ff.

Keller / Griesbaum

Das Phänomen der vorbeugenden Bekämpfung von Straftaten

NStZ 1990, S. 416 ff.

Kilian

Warum Rechtsinformatik?

CR 2001, S. 132 ff.

Knemeyer

Polizei- und Ordnungsrecht

8. Auflage, München 2000

Kniesel

Versammlungs- und Demonstrationsfreiheit

NJW 2000, S. 2857 ff.

Kniesel

Neue Polizeigesetze contra StPO

ZRP 1987, S. 377 ff.

Kniesel / Vahle

Zur Novellierung des nordrhein-westfälischen Polizeirechts

DÖV 1990, S. 646 ff.

Köhler / Arndt

Recht des Internet

3. Auflage, Heidelberg 2001

Köhntopp / Köhntopp

Datenspuren im Internet

CR 2000, S. 248 ff.

als pdf unter: <<http://123.koehntopp.de/kris/artikel/datenspuren/>>

Köhntopp, Marit / Pfitzmann

Gibt es einen sinnvollen Kompromiß zwischen der Verhinderung von Cyber-Crime und Datenschutz?

Datenschutz Nachrichten 2/2001, S. 21 ff.

Kollmann

Islamistischer Terrorismus – eine Herausforderung für die internationale Staatengemeinschaft (Bericht zur Herbsttagung des Bundeskriminalamtes)

<<http://www.bdk.de/magazin/januar-2002.php3>>

Krader

Kampf gegen die Internetkriminalität

DuD 2001, S. 344 ff.

Kröger / Gimmy

Handbuch zum Internetrecht

2. Auflage, Heidelberg 2002

Kudlich

Strafprozessuale Probleme des Internet

JA 2000, S. 227 ff.

Kugelman

Die „Cyber-Crime“ Konvention des Europarates

DuD 2001, S. 215 ff.

Lammer

Verdeckte Ermittlungen im Strafprozeß

Berlin 1992

Legge

New York - weder Modell noch Fortschritt ?

in: Feltes (Hrsg.), Das Modell New York: Kriminalprävention durch Zero Tolerance,

S. 116 ff. (133)

Lindig

Die neuen „ereignis- und verdachtsunabhängigen“ Befugnisse im Polizeirecht

<<http://www.jurawelt.com/aufsaeetze/oer/3573?stylite=1>>

Lisken

Polizei und Verfassungsschutz

NJW 1982, S. 1481 ff.

Lisken / Denninger

Handbuch des Polizeirechts

3. Auflage, München 2001

Lloyd

Information Technology Law

3. Auflage, London / Edinburgh / Dublin 2000

Lloyd

Legal Aspects of the Information Society

London / Edinburgh / Dublin 2000

Loewenheim / Koch

Praxis des Online – Rechts

München 2002

Lorch

Ermittlungen im Internet

Kriminalistik 2001, S. 328 ff.

Lorch

PERKEO

<http://www.bka.de/aktuell/agenda98/vtr99/vtr_lorch.html>

Marr

Anlaßabhängige Ermittlungen der Polizei im Internet

der kriminalist 2001, S. 227 ff.

Marberth-Kubicki

Internet und Strafrecht

<<http://www.ag-strafrecht.de/aufsatzkubik.htm>>

McCandless

Warez World

in: Medosch/Röttgers (Hrsg.), Netzpiraten, S. 35 ff.

Medosch/Röttgers (Hrsg.)

Netzpiraten – Die Kultur des elektronischen Verbrechens

Hannover 2001

Merten, Karlheinz / Merten, Heike

Vorbeugende Verbrechensbekämpfung

ZRP 1991, S. 213 ff.

Merten

Zulässigkeit der langfristigen Video-Überwachung

NJW 1992, S. 354 ff.

Meseke

Ermittlungen im Internet – Positionen und Dissonanzen

Kriminalistik 2000, S. 245 ff.

Meseke

Ermittlung und Fahndung im Internet

in: BKA (Hrsg.), Festschrift für Herold, S. 505 ff.

Meseke

INTERNET und Kriminalität

<http://www.bka.de/aktuell/agenda98/vtr98/vtr_meseke98.html>

Meseke

Präsentation: „Lagedarstellung der Internet-Kriminalität“

<http://www.bka.de/aktuell/agenda98/vortrag_meseke99.zip>

v. Münch / Kunig (Hrsg.)

Grundgesetz – Kommentar

Bd. 1 (Präambel bis Art. 20)

5. Auflage, München 2000

Bd. 3 (Art. 70 bis 146)

3. Auflage, München 1996

Nitz

Einsatzbedingte Straftaten Verdeckter Ermittler
Hamburg 1997

Nogala

Der Frosch im heißen Wasser
in: Schulzki-Haddouti (Hrsg.): Das Ende der Anonymität, S. 149 ff.

Ochsenbein

Strafrechtliche Aspekte des Internet
Kriminalistik 1998, (S. 513 ff., S. 599 ff.), S. 685 ff.

Paulus

Pädo-Kriminelle im Datennetz
Kriminalistik 2000, S. 390 ff.

Pieroth / Schlink

Grundrechte – Staatsrecht II
13. Auflage, Heidelberg 1997

Rachor

Vorbeugende Straftatenbekämpfung und Kriminalakten
Baden-Baden 1989

Riepl

Informationelle Selbstbestimmung im Strafverfahren
Tübingen 1998

Roßnagel / Scholz

Datenschutz durch Anonymität und Pseudonymität
MMR 2000, S. 721 ff.

Rötzer

Das Recht auf Anonymität
in: Bäumler (Hrsg.), E-Privacy, S. 27 ff.

Rogall

Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht
Tübingen 1992

Roggan

Über das Verschwimmen von Grenzen zwischen Polizei- und Strafprozeßrecht

<<http://www.jura.uni-bremen.de/grenzen.pdf>>

Rublack

Terrorismusbekämpfungsgesetz: Neue Befugnisse für die Sicherheitsbehörden

DuD 2002, S. 202 ff.

Sachs

GG, 2. Auflage

München 1999

Sakowski

Virtuelles Hausrecht

<<http://www.sakowski.de/onl-r/onl-r65.html>>

Schetsche

Internetkriminalität: Daten und Diskurse, Strukturen und Konsequenzen

<<http://www1.uni-bremen.de/~mschet/interkrim.html>>

Schlink

Das nachrichtendienstliche Mittel

NJW 1980, S. 552 ff.

Schoreit

Gefahrenabwehr – vorbeugende Verbrechensbekämpfung - Legalitätsprinzip

DRiZ 1991, S. 320 ff.

Schulzki-Haddouti (Hrsg.)

Vom Ende der Anonymität – Die Globalisierung der Überwachung

2. Auflage, Hannover 2001

Schulzki-Haddouti

Von Kinderpornographie zur Globalisierung der Polizeiarbeit

<<http://www.heise.de/tp/deutsch/inhalt/te/2951/1.html>>

Schulzki-Haddouti

Maschinenstürmer im Bundesinnenministerium

<<http://www.heise.de/tp/deutsch/inhalt/te/1547/1.html>>

Schuster

Die Grenzen polizeilicher Ermittlung
in: Bäumler (Hrsg.), E-Privacy, S. 77 ff.

Schwan

Die Abgrenzung des Anwendungsbereiches der Regeln des Straf- und
Ordnungswidrigkeitenverfolgungsrechtes von dem des Rechtes der Gefahrenabwehr
Verwaltungsarchiv 1979, S. 109 ff.

Schwan

Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte
Verwaltungsarchiv 1975, S. 120 ff.

Seidl-Hohenveldern / Stein

Völkerrecht
10. Auflage, Köln 2000

Sieber

Internationales Strafrecht im Internet
NJW 1999, S. 2065 ff.

Siebrecht

Die polizeiliche Datenverarbeitung im Kompetenzstreit zwischen Polizei- und Prozeßrecht
JZ 1996, S. 711 ff.

Soiné

Datenverarbeitung für Zwecke künftiger Strafverfahren
CR 1998, S. 257 ff.

Soiné

Fahndung via Internet
NStZ 1997, S. 166 ff. (und 321 ff.)

Soiné

Strafverfolgung, Polizei und Internet
Polizeispiegel 2001, S: 167 ff. und 199 ff.

Spatscheck / Alvermann

Internet-Ermittlungen im Steuerstraßprozeß
wistra 1999, S. 333 ff.

Stadler

Anlaßunabhängige Überwachung des Internet

<<http://www.afs-rechtsanwaelte.de/internetstreife.htm>>

Steiger / Adler

Auf Streife

Deutsches Polizeiblatt (DPolBl) 4/2001, S. 23 ff.

Tinnefeld

Persönlichkeitsrecht und Modalitäten der Datenerhebung im Bundesdatenschutzgesetz

NJW 1993, S. 1117 ff.

Vassilaki

Strafverfolgung der grenzüberschreitenden Internet-Kriminalität

CR 1999, S. 574 ff.

Vowinkel

Kinderpornographie: Polizei vernachlässigt Fahndung im Internet

<<http://www.welt.de/daten/2001/12/30/1230vm305032.htx?print=1>>

Wabnitz / Janovsky

Handbuch des Wirtschafts- und Steuerstrafrechts

München 2000

Weichert

Cyber-Crime-Bekämpfung und Datenschutz

Datenschutz Nachrichten 2/2001, S. 5 ff.

Weßlau

Gefährdungen des Datenschutzes durch den Einsatz neuer Medien im Strafprozeß

ZStW 2001, S. 681 ff.

Weßlau

Vorfeldermittlungen – Probleme der Legalisierung „vorbeugender Verbrechensbekämpfung“ aus strafprozessualer Sicht

Berlin 1989

Wiedemann

Tatwerkzeug Internet

Kriminalistik 2000, S. 229 ff.

Wiese

Unfreiwillige Spuren im Netz

In: Bäumler (Hrsg.), E-Privacy, S. 9 ff.

Wilson / Kelling

The police and neighborhood safety: Broken windows

in: Feltes (Hrsg.), Das Modell New York: Kriminalprävention durch Zero Tolerance, S. 50 ff.

Wuermeling / Felixberger

Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz

CR 1997, S. 230 ff.

Zimmermann

Polizeiliche Gefahrenabwehr und das Internet

NJW 1999, S. 3145 ff.

Zöller

Verdachtslose Recherchen und Ermittlungen im Internet

GA 2000, S. 563 ff.

Ohne Verfasserangabe

Internet und Kinderpornographie – Wie das BKA und das Bayer. LKA dem Mißbrauch begegnen

Die Polizei 1999, S. 265 ff.

< **Stand aller angegebenen URL: 27.12.2002** >

Einführung

I. Internet als Panopticon

Polizeiliche Tätigkeit verschiebt sich zunehmend in das *Vorfeld* der klassischen Gefahrenabwehr und Strafverfolgung. Diese Entwicklung ist ein Hauptkonfliktpunkt in der aktuellen Debatte um „Freiheit oder Sicherheit“.

Anlaß zu Diskussionen bietet auch die Frage, in welchem Maße das ursprünglich auf Selbstregulierung angelegte *Internet* zum Objekt staatlicher Überwachung werden soll.

Die anlaßunabhängige Ermittlung im Internet wird damit aus zwei Richtungen zum spannungsgeladenen Thema.

Die Befürworter von umfangreichen Ermittlungsmaßnahmen im Netz sehen den Staat in der Pflicht, ein „Grundrecht auf Sicherheit“ seiner Bürger zu gewährleisten. Die Gesellschaft müsse vor den Gefahren des Internets geschützt werden. Als Hauptargument zur Legitimierung nahezu jeglicher Überwachung dient vor allem das Aufkommen an Kinderpornographie im Netz. Datenschutz sei Tatenschutz.

Die Datenschutz-Verfechter hingegen sehen sich in Orwells „1984“ versetzt. Unsere Gesellschaft gleiche mittlerweile dem vom Juristen und Philosophen Jeremy Bentham entworfenen Panopticon – jener Vollzugsanstalt, deren ringförmige Bauweise die lückenlose Überwachung der Gefangenen ermöglicht.

Die Insassen eines Panopticons wissen zu keinem Zeitpunkt, ob sie augenblicklich tatsächlich beobachtet werden. Das bloße Entdeckungsrisiko soll ausreichen, um sie zu normkonformem Verhalten zu veranlassen¹. – Eine solche Präventivkraft messen die Ermittler auch ihren Überwachungsaktivitäten im Internet bei.

¹ Foucault, Überwachen und Strafen, S. 259

Die mögliche Kehrseite eines gehemnten, angepaßten Verhaltens aber beschreibt das Bundesverfassungsgericht im Volkszählungsurteil: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“²

Diese Furcht wird im Internet noch verstärkt durch die für den durchschnittlichen User nebulöse und technisch undurchschaubare Funktionsweise. Darüber hinaus kommt vorliegend hinzu, daß die Internet-Ermittlungstätigkeit bereits im Vorfeld des Anfangsverdachts ansetzt. Der User sieht sein „right to be let alone“³ also auch bei gesetzestreuem Verhalten in Gefahr.

Ein dadurch drohender Verzicht auf die Ausübung der Kommunikationsgrundrechte wird jedoch „nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“⁴

Vor diesem Hintergrund ist Ziel der vorliegenden Arbeit, die anlaßunabhängige Ermittlung im Internet, die sog. Internet-Streifenfahrt, auf ihre Rechtmäßigkeit zu überprüfen.

II. Rechtsinformatik als methodischer Zugang

*Rechtsinformatik ist die Wissenschaft von den Voraussetzungen, Anwendungen und Folgen der Informationstechnologie im Recht.*⁵

Das Thema „Ermittlungsmaßnahmen im Internet“ ist ein gut geeigneter Gegenstand für die Abschlußarbeit des Ergänzungsstudiengangs: Alle drei

² BVerfGE 65, 1 (43)

³ Lloyd, Information Technology Law, S. 36: Das Zitat wird dem US-Richter Cooley (1888) zugeschrieben.

⁴ BVerfGE 65, 1 (43)

⁵ Kilian, Warum Rechtsinformatik?, CR 2001, S. 132 ff. (133)

Bereiche der Rechtsinformatik werden relevant und erschließen schon nahezu sämtliche Facetten des Themas.

1) Voraussetzungen der Informationstechnologie

Die Rechtsinformatik befaßt sich im Rahmen der Wissenschaftstheorie damit, was „Information“ rechtlich bedeutet. Informationen sind weder körperliche Gegenstände noch Rechte. Vielmehr ist zwischen dem elektronischen Datum und einem körperlichen Träger zu unterscheiden. Diese Andersartigkeit elektronischer Daten wirkt sich auch im Strafverfahrensrecht aus. Gerade dieser sensible Bereich muß jedoch von übereilten technikbezogenen Gesetzesnovellen verschont bleiben: Gesetze, die durch eine Sonderdogmatik einen bestimmten Stand der Technik regeln wollen, sind zumeist schon vor ihrem Inkrafttreten veraltet und überholt von der Entwicklung der Informationstechnologie⁶.

Es ist deshalb ein Anliegen der Rechtsinformatik, durch Betrachtung der neuen technischen Verfahren herauszufinden, ob **funktionale Äquivalente** bekannter Maßnahmen vorliegen⁷. Auf diese Weise lassen sich häufig neue Probleme in den bewährten dogmatischen Strukturen abbilden und wissenschaftliche Erkenntnisse übertragen. Dies ist auch Ziel der vorliegenden Arbeit.

2) Anwendungen der Informationstechnologie

Die Anwendung der Informationstechnologie bei der Ermittlungsarbeit ermöglicht neue Arbeitsweisen und polizeiliche Methoden der Kriminalitätsbekämpfung⁸: So kann etwa Technologie unterstützend zum Einsatz kommen in Form von sog. Ermittlungstools und speziellen Datenbanken.

3) Folgen der Informationstechnologie

Weitreichende Folgen der Informationstechnologie bei der praktischen Rechtsanwendung ergeben sich aus den spezifischen Eigenschaften von Daten

⁶ Hilgendorf, Die Neuen Medien und das Strafrecht, ZStW 2001, S. 650 ff. (653)

⁷ Kilian, Warum Rechtsinformatik?, CR 2001, S. 132 ff. (133)

⁸ Meseke, Ermittlung und Fahndung im Internet, in: BKA (Hrsg.), Festschrift für Herold, S. 505 ff. (522)

und Informationen: Hervorzuheben ist an dieser Stelle vor allem das Fehlen örtlicher Gebundenheit, die Ubiquität von Informationen.

Zum einen ermöglicht dies Straftätern, „off shore“ zu gehen: Sie verlagern ihre inkriminierten Inhalte auf ausländische Server, um sich dem Zugriff einer restriktiveren Rechtsordnung zu entziehen. Dies stellt die Ermittler vor große Probleme im Bereich des Strafanwendungsrechts.

Zum anderen macht natürlich auch die Ermittlungstätigkeit selbst im Internet nicht automatisch an territorialen Grenzen Halt. Die Statistiken der anlaßunabhängigen Ermittlung weisen für bis zu 80 % der Fälle einen Auslandsbezug auf. Für jede Maßnahme ist deshalb zu bedenken, ob nicht im Vorgehen der Ermittler bereits ein Eingriff in die Gebietshoheit eines anderen Staates liegt.⁹

III. Gang der Darstellung

A. Als technische Grundlage für die weiteren Betrachtungen soll zunächst dargestellt werden, auf welche *Datenspuren* bei der Ermittlung in den typischen Internet-Diensten jeweils zurückgegriffen werden kann.

B. Die von der Streifenföhtigkeit vorliegenden Statistiken lassen auf eine deutliche *Delikts-Fokussierung* schließen. Da dieses Vorgehen auch für die rechtliche Beurteilung von Relevanz sein kann, soll dieser Ermittlungsschwerpunkt hier dargestellt werden.

C. Zur Überprüfung der Rechtmäßigkeit ist anschließend zunächst die *Eingriffsqualität* der Internetstreife in den einzelnen Internetdiensten zu prüfen.

D. Unabhängig von der Eingriffsqualität ist für staatliches Vorgehen das Vorliegen einer *Aufgabenzuweisungsnorm* erforderlich und daher für alle Maßnahmen zu untersuchen.

⁹ Spatscheck / Alvermann, Internet-Ermittlungen im Steuerstrafprozeß, wistra 1999, S. 333 ff., (334)

E. Für Maßnahmen mit Eingriffsqualität sind darüber hinaus denkbare *Ermächtigungsgrundlagen* zu prüfen.

F. Als weitere Tätigkeit der Recherchedienste sind die Maßnahmen zur *Identitätsbestimmung* zu erörtern.

G. Zur Problematik des *Eingriffs in einen fremden Hoheitsbereich* durch die Ermittlung wird anschließend bezüglich jener Maßnahmen Stellung genommen, deren Rechtmäßigkeit im Inland festgestellt werden konnte.

IV. Eingrenzung des Themas

Die vorliegende Untersuchung wählt dieselbe Grenze wie die BKA-Ermittler bei ihrer Streife: Von diesen werden nach der Identifizierung der Verantwortlichen die durch die Streife gewonnenen Verdachtsfälle an die sachlich und örtlich zuständigen Behörden weitergegeben.

Nachfolgend stützen diese Behörden ihre Ermittlungsmaßnahmen wegen des zuvor gewonnenen Anfangsverdachts dann auf die *StPO*. Dieses Vorgehen ist jedoch nicht mehr Gegenstand der vorliegenden Masterarbeit. Insbesondere ist daher die Problematik der TK-Überwachung konkreter, bereits identifizierter Zielpersonen hier nicht zu thematisieren.

Auch kann im Rahmen dieser Arbeit nicht auf die der Ermittlungstätigkeit vorgelagerte Frage eingegangen werden, welche Internetinhalte dem *Anwendungsbereich des deutschen Strafrechts* unterfallen¹⁰.

Ferner erfolgt eine Betrachtung der *Tätigkeit der Nachrichtendienste* nur im Rahmen der Erörterung des Trennungsgebots.

¹⁰ dazu z.B. Sieber, Internationales Strafrecht im Internet; NJW 1999, S. 2065 ff.; Breuer, Anwendbarkeit des deutschen Strafrechts auf exterritorial handelnde Internet-Benutzer, MMR 1998, S: 141 ff.;

A. Technische Möglichkeiten und Grenzen der Internetermittlung

„Bei der ‚Internetstreife‘ ist manches anders. Unser Revier ist das Internet.“¹¹

Nach Schätzungen der „nua.com -Internet Surveys“ halten sich in diesem Online-Revier in Deutschland derzeit 32,1 Millionen User auf, rund 39 % der Bevölkerung. Weltweit sind 605,6 Millionen Menschen im Internet aktiv, (Stand: September 2002)¹².

Die gängigen Internetdienste sollen hier im Überblick dargestellt werden. Von Interesse ist für das vorliegende Thema dabei der jeweilige „Datenschatten“, den ein Teilnehmer bei der Benutzung hinterläßt und der für die Ermittlungsbehörden den Hauptanhaltspunkt für die Identitätsbestimmung darstellt. Ferner sind mögliche, rechtlich relevante Unterschiede in der Kommunikationsstruktur der Dienste festzuhalten.

Die Recherchen der Ermittlungsbehörden konzentrieren sich vor allem auf folgende Dienste: World Wide Web, File Transfer Protocol, Internet-Relay-Chat und Usenet (Newsgroups).

I. WWW

Der wegen seiner Benutzerfreundlichkeit am meisten frequentierte Teil des Internets ist das World Wide Web (WWW).

Der Begriff WWW bezeichnet die Summe aller über das Anwendungsprotokoll Hypertext Transfer Protocol (http) erreichbaren Angebote, der Websites. Die Erstellung solcher Seiten - in der Textauszeichnungssprache HTML - ist die wohl verbreitetste Form, um sich anderen Internetnutzern mitzuteilen, dies unter möglicher Einbeziehung beliebiger Bild- und Tondateien.

¹¹ Steiger / Adler, Auf Streife, DPolBl 4/2001, S. 23 ff. (23)

¹² <http://www.nua.com/surveys/how_many_online/europe.html>

Die WWW-Anwendungsprogramme („browser“) beziehen jedoch zunehmend auch andere Angebote in ihre Darstellung ein, so daß aus User-Sicht die Dienste mehr und mehr verschmelzen¹³.

Für die Ermittlung interessant ist vor allem das Adressierungsschema URL (Uniform Resource Locator), da dessen Informationsgehalt über die bloße IP-Nummer, bzw. den DNS-Namen hinausgeht:

Nach der Bezeichnung des Anwendungsprotokolls, z.B. http, folgt die Bezeichnung des Rechners, (im Regelfall nicht als IP-Adresse, sondern als DNS-Name). Darüber hinaus wird anschließend aber auch das einzelne Angebot mit dem Dateinamen und ggf. der *Verzeichnisstruktur* einbezogen, so daß damit ein ganz konkretes Datei-Angebot weltweit unverwechselbar bezeichnet werden kann¹⁴.

Erwähnenswert sind aufgrund ihrer großen Bedeutung in den Anfängen der Internet-Ermittlungen auch die „Bulletin Board Systems“ (BBS). Diese elektronischen schwarzen Bretter existierten lange vor dem Internet, bekannt als sog. „*Mailboxen*“. Mittlerweile wurden die Bulletin Boards auf das WWW übertragen¹⁵. Reine „Mailbox“-Angebote gibt es aber nach wie vor. Von größerer Bedeutung als BBS ist nun allerdings der Diskussionsforen-Verbund „Usenet“, weshalb die Funktionsweise eines Forums im Zusammenhang damit vorgestellt wird, (sogleich unter V.).

II. File-Transfer-Protocol (FTP)

Von großer Bedeutung für den Austausch beliebiger Dateien ist das File-Transfer-Protocol.

Ein FTP-Server hält Dateien, insb. auch Software, für den Download bereit. Nach einer Anmeldung bei einem solchen FTP-Server kann der User auf dessen Server-Datenbestände zurückgreifen. Als Client agierend weist der User

¹³ Marr, Anlaßabhängige Ermittlung der Polizei, der kriminalist 2001, S. 227 ff. (227)

¹⁴ Köhler / Arndt, Recht des Internet, Rn. 12

¹⁵ Germann, Gefahrenabwehr und Strafverfolgung, S. 73

den Server zum Download an und legt die empfangenen Daten auf seiner eigenen Festplatte ab.

Einige FTP-Server bieten umgekehrt auch ein Eingangsfach an, in dem jeder User Dateien ablegen kann¹⁶. Meist wird dieses Material vor der weiteren Freigabe vom verantwortlichen Server überprüft. Bisweilen jedoch ist auch gleich ein unmittelbarer Download durch andere User aus diesem Eingangsfach, damit ein freier Datenaustausch unter den Clients, möglich.

Öffentlich zugänglich sind diejenigen FTP-Server, die im Rahmen der Anmeldung eine anonyme Kennung wie „anonymous“ oder „guest“ akzeptieren.

III. Internet Relay Chat (IRC)

Einige Anwendungen im Internet ermöglichen synchrone Kommunikation: Die Teilnehmer sind gleichzeitig online. Jede Nachricht wird sofort auf dem Bildschirm des Kommunikationspartners dargestellt.¹⁷ Wie am Telefon wird sofort geantwortet. Jeder Teilnehmer agiert somit als Sender und auch als Empfänger.

Eine solch synchrone Kommunikationsform ist der Internet Chat. Neben den populärer und im Angebot umfangreicher werdenden Messengerdiensten wie ICQ (I seek you), AIM¹⁸ und MSN¹⁹ ist das ursprüngliche Chat-System IRC im Internet immer noch von größter praktischer Bedeutung. Bezüglich der Datenspuren und des Vorgehens der Ermittler besteht zwischen den Diensten große Ähnlichkeit.²⁰ Deshalb wird nachfolgend nur auf den Internet Relay Chat eingegangen.

Einmal bei einem IRC-Server angemeldet kann sich der Teilnehmer einem

¹⁶ Heinzmann / Ochsenein, Strafrechtliche Aspekte des Internet, Kriminalistik 1998, S. 513 ff. (516)

¹⁷ Wiedemann, Tatwerkzeug Internet, Kriminalistik 2000, S. 229 ff. (231)

¹⁸ AOL Instant Messenger

¹⁹ Microsoft MSN Messenger

²⁰ Köhntopp / Köhntopp, Datenspuren im Internet, als pdf unter <<http://123.koehntopp.de/kris/artikel/datenspuren/>>, S. 15

beliebigen Chatroom (sog. channel) anschließen, um Nachrichten zu senden und zu empfangen. Derartige Channels existieren zu den unterschiedlichsten Themen.

Über einen Verbund von IRC-Servern gelangen die Mitteilungen im Regelfall in Echtzeit an *alle* übrigen Teilnehmer des jeweiligen Kanals.²¹ Neben diesen öffentlichen Nachrichten jedoch können auch private Nachrichten direkt an eine ausgewählte Person – mittels des „/msg“-Kommandos vor der Nachricht - über den IRC-Server gesandt werden.

Mit Hilfe des „/dcc“-Befehls²² können private Nachrichten sogar unter Umgehung des IRC-Servers an einzelne Teilnehmer versandt werden.

Über diese private dcc-Verbindung sind auch sog. „file-server“ erreichbar, ein typisches und die Ermittler sehr beschäftigendes IRC-Phänomen. Ein file-server ist technisch betrachtet ein Speichermedium auf dem Rechner eines IRC-Users, zu dem dieser den Zugang freigegeben hat. Dies ermöglicht ähnlich wie beim ftp-Server den Up- und Download von Dateien im Tauschverfahren²³.

Typisch für die Chatdienste ist die Teilnahme unter einem „**Nickname**“, einem frei wählbaren Pseudonym. Daneben jedoch stehen allen Besuchern des Chatrooms, somit auch den Ermittlern, über die „/whois“-Anfrage folgende Daten über jeden einzelnen Teilnehmer zur Verfügung²⁴:

die IP-Adresse,

der Namen des IRC-Servers, über den sich die Person eingewählt hat, sowie der Nutzernamen.

IV. Usenet / Newsgroups

Im Unterschied zum IRC sind Diskussionsforen, sog. newsgroups, der nicht-synchronen Kommunikation zuzuordnen, d.h. Rede und ggf. Gegenrede

²¹ Heinzmann / Ochsenein, Strafrechtliche Aspekte des Internet, Kriminalistik 1998, S. 513 ff. (516)

²² direct from computer to computer

²³ Steiger / Adler, Auf Streife, DPolBl 4/2001, S. 23 ff. (25)

²⁴ Köhntopp / Köhntopp, Datenspuren im Internet, als pdf unter <<http://123.koehntopp.de/kris/artikel/datenspuren/>>, S. 15

werden hier nicht in Echtzeit ausgetauscht. Die einzelnen Beiträge (Postings) sind wegen der großen Menge zwar nicht dauerhaft, jedoch mit einer (konfigurierbaren) Lebensdauer von 2 Stunden bis zu 30 Tagen verfügbar²⁵. Überdies halten News-Archive wie Deja.com in großen Datenbanken länger zurückliegende Postings bereit, wenn nicht der Autor im Header oder der ersten Zeile des Beitrags einer Archiv-Aufnahme widerspricht.

Ein weltweit genutzter Verbund von einzelnen Diskussionsforen ist das **Usenet**. Seine hierarchische Verzeichnisstruktur ermöglicht den gezielten Zugriff auf die jeweils gesuchten Themenbereiche und die Sub-Kategorien²⁶. Das Usenet steht grundsätzlich allen Themen offen. Entsprechend groß ist die fachliche Bandbreite vorhandener Newsgroups.

Die Beiträge werden auf News-Servern bereitgehalten. Das dem Usenet zugrundeliegende Anwendungsprotokoll „Network News Transfer Protocol“ (NNTP) ermöglicht den Servern, ihre Bestände regelmäßig untereinander abzugleichen. Die News-Server übermitteln sich anschließend gegenseitig die je neu eingegangenen Beiträge, so daß ein Beitrag alsbald in unübersehbarer Zahl kopiert weltweit vorliegt (sog. Flood-Fill-Mechanismus)²⁷.

Jeder User kann Beiträge für ein Forum an den News-Server senden, bei dem er angemeldet ist. Neben Texten können die Beiträge beliebige sonstige graphische oder akustische Informationen enthalten²⁸. Im Regelfall wird der Beitrag automatisch in das Diskussionsforum, die entsprechende Newsgroup, eingestellt und kann abgerufen werden.

Das NNTP ermöglicht jedoch auch die „Moderation“ von Newsgroups. In diesem Fall wird der Beitrag zuerst an den Moderator gesandt, direkt oder über den News-Server²⁹. Erst nach Zustimmung des Moderators wird der Beitrag

²⁵ Steiger / Adler, Auf Streife, DPolBl 4/2001, S: 23 ff. (24)

²⁶ Wiedemann, Tatwerkzeug Internet, Kriminalistik 2000, S. 229 ff. (231)

²⁷ Köhntopp / Köhntopp, Datenspuren im Internet, als pdf unter <<http://123.koehntopp.de/kris/artikel/datenspuren/>>, S. 14

²⁸ Gruhler, Das Ende der „totalen“ Freiheit im Internet, S. 6

²⁹ Germann, Gefahrenabwehr und Strafverfolgung, S. 73

veröffentlicht. Aus Ermittlersicht „ertragreicher“ sind daher freilich die erstgenannten, unmoderierten Newsgroups.

Die Ermittler können bei ihrer Arbeit wie beim IRC auf den Vorspann des Beitrags zurückgreifen³⁰: Dieser enthält im Usenet die Absenderadresse, Erstellungsdatum und –zeit, Diskussionsforum und Betreffzeile, eine weltweit eindeutige Kennung des Beitrags, seine Länge, sowie den Weg, über den er bisher im Usenet verbreitet wurde.

V. Möglichkeiten des Zugangsschutzes

Alle soeben dargestellten Dienste können statt der Öffnung für jedermann auch nur für einen beschränkten Nutzerkreis freigegeben werden³¹.

Bei FTP-Servern stellt der mit Nutzernamen und Kennwort geschützte Zugang in der Praxis sogar den Regelfall dar. Auch für die anderen Internetdienste ist es aber ohne größeren technischen Aufwand möglich, den zugelassenen Nutzerkreis zu beschränken.

Möglich ist dies etwa durch die Verwendung eines Cookies. Diese kleinen Informationsfragmente läßt ein Server beim Abfragen einer Seite vom Browser des Users abspeichern. Cookies werden fast ausschließlich zur Identifikation des Benutzers verwendet.

Zur Umsetzung einer Zugangsbeschränkung kann ein Cookie zum Beispiel allein den erwünschten Besuchern oder Teilnehmern übermittelt werden. Suchen diese die entsprechende Seite auf, wird der Cookie-Inhalt automatisch an den geschützten Server übertragen³². Ohne Cookie kann die Berechtigung dann nicht dargelegt werden, und der Zugang wird verweigert.

³⁰ Köhntopp / Köhntopp, Datenspuren im Internet, als pdf unter <<http://123.koehntopp.de/kris/artikel/datenspuren/>>, S. 14

³¹ Wiedemann, Tatwerkzeug Internet, Kriminalistik 2000, S. 229 ff. (235)

³² Wiese, Unfreiwillige Spuren im Netz, in: Bäumler (Hrsg.), E-Privacy, S. 9 ff. (13)

Denkbar ist aber auch eine Konfiguration im Zusammenhang mit der HTML-Programmierung eines Webangebots: Im selben Verzeichnisbereich wie die zur Web-Seite gehörenden Inhalte kann zum Beispiel eine sog. „htaccess“-Datei angelegt werden. Dadurch ist ein Schutz durch Paßwortabfrage realisierbar. Es können so aber auch automatisch bestimmte IP-Adressen, sowie ganze IP-Bereiche ausgeschlossen oder exklusiv zugelassen werden.

Schon für den interessierten Laien ist somit die Realisierung eines Zugangsschutzes kein unüberwindliches technisches Hindernis.

VI. Identitätsbestimmung anhand des Datenschattens

Um über das dem Internet zugrundeliegende TCP/IP- Protokoll Daten austauschen zu können, muß jedem Rechner, der sich mit dem Internet verbindet, eine IP-Nummer zugeteilt werden³³. Das derzeit noch eingesetzte Internet-Protokoll IPv4 verwendet eine nur 32 bit lange IP- Adresse. Damit stößt die Anzahl der möglichen IP-Adressen an gewisse Grenzen.

Eine Möglichkeit, den Bedarf an IP-Adressen zu verringern, ist die heute als Regelfall praktizierte Vergabe von dynamischen IP-Adressen. Die Adressen werden den Zugangsprovidern zugeteilt und einem Teilnehmer erst bei der Nutzung und flexibel nur zu diesem konkreten Online-Aufenthalt zugewiesen. Die benötigten IP-Adressen beschränken sich somit auf die Anzahl der gleichzeitigen Nutzer³⁴.

Auch auf diese Weise hinterläßt der User jedoch den dargestellten Datenschatten. Ohne spezielle Vorkehrungen ist online niemand anonym unterwegs. Vielmehr stellt die IP-Adresse ein (temporäres) Pseudonym dar³⁵: Sie ersetzt den Namen des Users durch ein Kennzeichen.

³³ Meseke, Ermittlung und Fahndung im Internet, in BKA (Hrsg.), Festschrift für Herold, S. 505 ff. (523)

³⁴ Köhntopp / Köhntopp, Datenspuren im Internet, als pdf unter <<http://123.koehntopp.de/kris/artikel/datenspuren/>>, S. 1

³⁵ Roßnagel / Scholz, Datenschutz durch Anonymität und Pseudonymität, MMR 2000, S. 721 ff. (725)

Das Wesen eines Pseudonyms ist im Unterschied zur Anonymität, daß es eine Zuordnungsregel gibt, über welche die Identitätsbestimmung möglich wird. Nur dem Access-Provider ist diese Zuordnungsregel bekannt.³⁶ Jeder Dritte ist also zur Identitätsbestimmung auf die Auskunft des Zugangsproviders angewiesen³⁷.

Ausgehend von den wie dargestellt anfallenden Datenspuren kommen für die Identitätsbestimmung insbesondere folgende Ansatzpunkte in Betracht:

- die Bestimmung des Users, dem zu einer bestimmten Zeit eine bei der Streife ermittelte IP-Adresse zugeordnet war,
- die Ermittlung des Inhabers einer Domain, auf welcher bei der Streifenfahrt inkriminiertes Material festgestellt wurde,
- die Zuordnung einer (z.B. im Header eines Usenet-Postings) aufgefallenen e-mail-Adresse zu deren Besitzer.

Die Ermittler nutzen diese Ermittlungsansätze, häufig auch in Reihe und kombiniert, um im Bedarfsfall den User bis zu seinem Rechner oder Telefonanschluß zurückzuverfolgen³⁸.

Im Fall von statischen IP-Adressen und Domainnamen ist die Zuordnung über sog. „Who-is“-Datenbanken im Internet möglich³⁹. Es liegen damit „öffentliche Pseudonyme“ vor⁴⁰. In den übrigen Fällen kommen behördliche Auskunftsansprüche gegenüber dem Provider in Betracht⁴¹. Diese Identitätsbestimmung soll als abschließende Maßnahme der Internetstreife gesondert dargestellt werden, (dazu Kap. F).

An Grenzen stoßen die Ermittler bei ihrer Arbeit, wenn die Spuren bewußt verwischt werden durch die Verwendung von Fake-accounts und

³⁶ Graf, Internet: Straftaten und Strafverfolgung, DRiZ 1999, S. 281 ff. (284)

³⁷ Huber, Ermittlung und Strafverfolgung bei Internetattacken, DSWR 2000, S. 63 ff. (64)

³⁸ Marr, Anlaßabhängige Ermittlungen der Polizei im Internet, der kriminalist 2001, S. 227 ff. (228)

³⁹ www.ripe.net, www.denic.de

⁴⁰ Roßnagel / Scholz, Datenschutz durch Anonymität und Pseudonymität, MMR 2000, S. 721 ff. (727)

⁴¹ Graf, Befugnisse und Grenzen der Ermittlungsbehörden, DPoIBl 4/2001, S. 6 ff. (8)

Anonymizern, die sowohl die Identität von WWW-Surfern als auch von e-mail-Absendern nahezu unmöglich machen können.

Auch der Einsatz von Proxy-Servern steht der Identitätsbestimmung häufig im Weg: Diese stellen eine Verbindung zwischen dem User und der von ihm angefragten Seite her, treten bei der Anfrage aber unter ihrer Proxy-eigenen IP-Adresse auf. Der besuchte Web-Server erfährt nicht die Original-IP des Users⁴².

Ein wichtiges Hilfsmittel zur Bewältigung dieser Probleme können die sog. Logfiles der Provider und Server-Betreiber darstellen: Jeder Web-Server kann eine Vielzahl der beim Zugriff des Users anfallenden Daten in diesen Logdateien speichern, darunter auch die IP-Adresse des Anfragenden und den genauen Zeitpunkt.

Aus den Logfiles läßt sich oft auch die sog. Remote-IP des zu identifizierenden Users erschließen: Eine solche Remote-IP fällt unter anderem bei jedem Upload von Inhalten durch den User für sein Online-Angebot auf den Server eines Host-Providers an⁴³: Auch wenn beim Host-Provider selbst die richtigen Personalien häufig nicht bekannt sind, läßt sich somit wiederum über den Zugangsprovider die Identität ermitteln.

All diese Hilfsmittel stehen nur zeitlich begrenzt zur Verfügung: Der bereichsspezifische Datenschutz in TDSV und TDDSG sieht einen Maximalumfang vor, der durch die Erfordernisse für ein ordnungsgemäße Vertragserfüllung bestimmt ist⁴⁴.

Zunehmend wird aber ein „sicherheitsbehördlicher Bedarf“ nach einer Pflicht zur Erhebung umfangreicher Logfiles und der Verlängerung der

⁴² Köhntopp / Köhntopp, Datenspuren im Internet, als pdf unter <<http://123.koehntopp.de/kris/artikel/datenspuren/>>, S. 5

⁴³ Marr, Anlaßabhängige Ermittlungen der Polizei im Internet, der kriminalist 2001, S. 227 ff. (228)

⁴⁴ Schuster, Die Grenzen polizeilicher Ermittlungen, in: Bäumler (Hrsg.), E-Privacy, S. 77 ff. (83)

Speicherfristen angemeldet.⁴⁵ Die neuen Regelungen zur TK-Überwachung, so z.B. § 100 g III StPO, tragen dem bereits Rechnung.⁴⁶

Datenschutzrechtlich ist diese Mentalität einer umfangreichen Vorratsdatenhaltung hinsichtlich der Verhältnismäßigkeit und der Zweckbindung sehr bedenklich.⁴⁷ Auch wird als Tendenz ein kompletter Richtungswechsel, die Abkehr vom Datenschutz im Interesse der „Sicherheit“, deutlich: Bislang war der Gesetzgeber bemüht, das Providerhandeln in Umfang und Speicherfrist zu begrenzen.⁴⁸ Nun wird dagegen sogar über eine Verpflichtung zur erweiterten Datenerhebung nachgedacht.

B. Tätigkeits- und Interessenschwerpunkt der Ermittler

Im Zusammenhang mit den Ermittlungsmaßnahmen im Internet ist eine Betrachtung des Lagebilds der Internet-Kriminalität geboten.

Zum einen enthalten einige der denkbaren Eingriffsgrundlagen Straftatenkataloge. Die mögliche Rechtfertigung eines Eingriffs kann sich daher auch nach dem jeweiligen Delikt richten.

Die Internet-Kriminalität ist zum anderen aber auch deshalb näher zu beleuchten, weil ihr Lagebild den Befürwortern staatlicher Überwachung stets als Begründungs- und Legitimierungsgrundlage dient⁴⁹. Zur Beurteilung dieser Argumentation muß das gezeichnete Bild eines Verbrecher-Paradieses hinterfragt werden.

⁴⁵ Hilbrans, Erfassungskonflikte im Cyberspace, DaNa 2/2001, S. 16 ff. (17)

⁴⁶ Eckhardt, Neue Regelungen der TK-Überwachung, DuD 2001, S. 197 ff. (199)

⁴⁷ Bäuml, Eine sichere Informationsgesellschaft, DuD 2001, S. 348 ff. (351); Köhntopp / Pfitzmann, Gibt es einen sinnvollen Kompromiß zwischen der Verhinderung von Cybercrime und Datenschutz?, DaNa 2/2001, S. 21 ff. (25)

⁴⁸ Weßlau, Gefährdungen des Datenschutzes durch den Einsatz neuer Medien im Strafprozeß, ZStW 2001, S. 681 ff. (703)

⁴⁹ Schetsche, Internetkriminalität: Daten und Diskurse, (1.1. Restriktive Deliktsfokussierung) <<http://www1.uni-bremen.de/~mschet/interkrim>>

I. PKS

Der sachlichen Annäherung an diesen modernen Deliktsbereich stehen jedoch einige klassische Probleme im Weg: So ist die Polizeiliche Kriminalstatistik (PKS) als Datenlieferant gerade für den hier relevanten Bereich denkbar ungeeignet: Die Delikte, bei denen Internet-Dienste als Kommunikations- und Tatmittel eingesetzt wurden, werden in der PKS nicht differenziert ausgewiesen.

Die Erfassung in der PKS läuft über sog. PKS-Schlüssel. So steht der PKS-Schlüssel 1434 für die Verbreitung von kinderpornographischem Material. Der Verbreitungsweg schlägt sich aber in diesem Schlüssel, damit auch in der PKS, nicht nieder. Selbst für die Beurteilung des Lagebilds der Internetkriminalität im Hellfeld ist die PKS daher nicht aussagekräftig.

Die Statistik zur „Computerkriminalität“ behandelt im Schwerpunkt Scheckkarten- und Computerbetrug gem. § 263 a StGB, führt also hinsichtlich der Internet-Kriminalität auch nicht weiter.

II. Periodischer Sicherheitsbericht

Allerdings befaßt sich der „Periodische Sicherheitsbericht“, der im Auftrag der Bundesministerien des Innern und der Justiz erstellt wurde, ausdrücklich mit dem Deliktsbereich Internet-Kriminalität⁵⁰. Verknüpft werden in diesem Bericht Daten der PKS und der Rechtspflegestatistik, dies aber auch ergänzt durch andere aktuelle Erkenntnisse:

Die registrierten Fallzahlen, auf die sich dieser Bericht hinsichtlich der Internet-Kriminalität stützt, stammen aus dem polizeilichen Meldedienst „Kriminalität in Verbindung mit Informations- und Kommunikationstechnik“ (IuK) der Länderpolizeien, aus der Vorgangsbearbeitung des BKA, sowie aus der Tätigkeit der „Zentralstelle für anlaßunabhängige Recherche in Datennetzen“ (ZaRD).

⁵⁰ Periodischer Sicherheitsbericht, 2.7. Internet-Kriminalität, S. 197
<http://www.bmi.bund.de/dokumente/Artikel/ix_49371.htm?nodeID=>

III. Fallzahlen der ZaRD, 1999 – 2001

	1999	2000	2001
Kinderpornographie	1008	1117	903
Staatschutz	8	243	89
Arzneimittelgesetz	27	37	36
Betäubungsmittelgesetz	17	18	11
Betrug	17	2	2
Tierpornographie	15	70	20
Urheberschutz	7	11	1
Jugendschutz	6	0	0
Sonstiger sexueller Mißbrauch	5	0	0
Softwarepiraterie	4	3	0
Waffengesetz	3	1	0
Kindesmißbrauch	0	13	6
Hehlerei	0	6	10
Computersabotage	0	2	0
Suizidankündigung	0	2	0
Bedrohung	0	1	0
Computerbetrug	0	1	0
Pornographie	0	1	1
Vergewaltigung	0	1	1
Straßenverkehrsgesetz	0	1	0
Zollvorschriften	0	1	0
Menschenhandel	0	0	2
Amtsanmaßung	0	0	1
Anleitung zu Straftaten	0	0	1
Urkundenfälschung	0	0	1
Totschlag	0	0	1
Sonstige *	9	0	0
Summe	1126	1531	1086

*: Die Kategorie „Sonstige“ wird seit 2000 einzeln aufgeschlüsselt.

Quelle: <http://md.hudora.de/jura/ZaRD>

Die BKA-Zentralstelle ZaRD erhebt jedoch gar nicht den Anspruch, daß ihre Fallzahlen ein objektives Lagebild der Internet-Kriminalität vermitteln: Zwar

wird stets behauptet, im Internet finde sich das komplette Spektrum von Kriminalität⁵¹, bis hin zum denkbaren Tötungsdelikt per Hacking in einen Krankenhaus-Computer⁵².

Die Fallzahlen der ZaRD spiegeln jedoch diese Aussage nicht wider. Die unverkennbare Häufung (85 % in 2001) der Deliktsgruppe „verbotene Pornographie“, insb. Kinderpornographie, ließe sich schon allein darauf zurückführen, daß sich diese Delikte einfacher erkennen lassen als etwa Vermögensdelikte. Eine Verzerrung des wiedergegebenen Lagebildes ist also unvermeidlich und auch unbestritten.

Aus ähnlichen Gründen muß auch das Zahlenmaterial des IuK-Meldedienstes, bei dem verbotene Pornographie ebenfalls einen Anteil von rund 70 % ausmacht, kritisch betrachtet werden⁵³: Im Bereich der Kinderpornographie im Internet ist die Bayerische Polizei besonders engagiert. Bayern wiederum weist auch das ausgeprägteste Meldeverhalten auf.

IV. Problematik der Deliktsfokussierung

Der Periodische Sicherheitsbericht bezeichnet Kriminalität im Internet als „**Kontrolldelikt**, das ohne polizeiliche Aktivitäten in der Regel nicht erkannt wird“⁵⁴. Anders als in der offline-Welt soll also die Hauptmöglichkeit der Überführung vom Dunkelfeld ins Hellfeld in der polizeilichen Verdachtssuche liegen. Gefunden wird - auch nach eigenen Aussagen der Ermittler - nur, wonach gesucht wird⁵⁵. Wonach aber gesucht wird, kann im Rahmen der anlaßunabhängigen Ermittlung in hohem Maße von den Ermittlern selbst festgelegt werden.

⁵¹ Meseke, Ermittlung und Fahndung im Internet, in BKA (Hrsg.), Festschrift für Herold, S. 505 ff. (519)

⁵² Schuster, Die Grenzen polizeilicher Ermittlungen, in Bäumlner (Hrsg.), E-Privacy, S. 77 ff. (80)

⁵³ Meseke, Internet und Kriminalität, (2. Statistik)

<http://www.bka.de/aktuell/agenda98/vtr98/vtr_meseke98.html>

⁵⁴ Periodischer Sicherheitsbericht, 2.7. Internet-Kriminalität, S. 197

<http://www.bmi.bund.de/dokumente/Artikel/ix_49371.htm?nodeID=>

⁵⁵ Vowinkel, Kinderpornographie: Polizei vernachlässigt Fahndung im Internet, WamS vom 30.12.01, <<http://www.welt.de/daten/2001/12/30/1230vm305032.htx?print=1>>

Bezeichnenderweise wurden auch in der offline-Welt die Vorwürfe selektiver Strafverfolgung im Rahmen einer Untersuchung der *Streifentätigkeit* erhoben⁵⁶. J. Feest und E. Blankenburg kamen durch teilnehmende Beobachtung einer Streife zu dem Schluß, neben dem ersten Code, dem materiellen Recht, existiere ein „zweiter Code“ eigener Anwendungsregeln⁵⁷: Wogegen vorgegangen wird und welche Vorkommnisse übergangen werden, richte sich auch nach dem subjektiven Erkenntnisinteresse der Beamten. Die Streifenpolizisten verfügen über einen großen Ermessensspielraum und ein hohes Maß an Definitionsmacht bei der Einschätzung der Verdachtslage.

Weiterführend für den online-Bereich ist hier weniger der erhobene Vorwurf schichtenspezifischer Selektion. Die grundlegende Problematik ist jedoch, daß die Streifentätigkeit von vornherein nur zur Erfassung von *sinnlich wahrnehmbar* deviantem Verhalten geeignet ist⁵⁸. Erfasst werden kann also nur ein kleiner Teilausschnitt von Kriminalität. Dies ist auf die Internetstreife übertragbar.

Auf den ersten Blick erscheint dies im Netz aber sogar weniger gegeben als in der offline-Welt. So sind etwa Vermögensdelikte online grundsätzlich auch beim Streifengang wahrnehmbar, etwa als § 263 StGB erfüllendes Online-Angebot, anders als vielfach in der realen Welt. Die Prüfung auf strafrechtliche Relevanz solcher Angebote gestaltet sich jedoch im Vergleich zu pornographischem oder rechtsextremem *Bildmaterial* wesentlich zeitintensiver.

Die Ermittler in Bayern bestätigen auch den Tätigkeitsschwerpunkt im Deliktsbereich der harten Pornographie, § 184 III StGB⁵⁹. Die BKA-Ermittler betonen dagegen, es existiere kein Rechereschwerpunkt⁶⁰. Jedoch wurden dazu auch schon andere Angaben gemacht⁶¹.

⁵⁶ Göppinger, Kriminologie, S. 485; Bock, Kriminologie, Rn. 262

⁵⁷ Bock, Kriminologie, Rn. 259

⁵⁸ Weßlau, Vorfeldermittlungen, S. 78

⁵⁹ Fiehl, Erfahrungen bei der Recherche, der kriminalist 1999, S. 2 ff. (2)

⁶⁰ Meseke, Lagedarstellung der Internetkriminalität, (Text7)

<http://www.bka.de/aktuell/agenda98/vortrag_meseke99.zip>

⁶¹ (Schuster im Interview mit) Schulzki-Haddouti, Von Kinderpornographie zur Globalisierung der Polizeiarbeit, <<http://www.heise.de/tp/deutsch/inhalt/te/2951/1.html>>

Die Deliktsfokussierung wird zudem auch verstärkt durch den noch darzustellenden Einsatz von Überwachungstools.

Die Problematik dieser selektiven Strafverfolgung mag zunächst von allein kriminologischem Interesse erscheinen. Auch für die rechtliche Beurteilung wird diese Deliktsfokussierung jedoch noch relevant: Denn die festgestellte erhöhte Selektionsmacht der Ermittlungsbehörden wird gerade bei der Vorfeldermittlung auch nicht durch die *Sachleitungsbefugnis der Staatsanwaltschaft* flankiert⁶². Darauf wird noch zurückzukommen sein.

V. Zusammenfassung zum Lagebild

Mangels geeigneten Datenmaterials läßt sich somit die dramatische Darstellung des Lagebilds weder untermauern noch widerlegen.

Wenig sachdienlich scheinen im übrigen jene verbreiteten Hochrechnungen, bei denen von allen weltweit vorhandenen Web-Seiten ein gewisser Prozentsatz (je nach Verfasser 1 – mind. 5 %) als inkriminiert eingestuft wird. Bisweilen wird dann diese Schätzung des weltweiten Dunkelfelds noch in Relation gesetzt zur (nationalen) PKS, um den Bedarf nach polizeilicher Präsenz im Internet zu untermauern⁶³.

Der dagegen erhobene Vorwurf der „Skandalisierungslogik“⁶⁴ scheint nicht übertrieben. Das einzige Datum, das - wie die PKS – das nationale Hellfeld der Kriminalität darstellt, ist die Angabe des ZaRD-Fallaufkommens. Aus einer Gegenüberstellung *dieser* beiden Werte ergibt sich ein Internet-Beitrag zur Gesamtkriminalität von unter 0,2 Promille. Die gemeldete ZaRD-Fallzahl ist jedoch aus den dargestellten Gründen auch für diesen Vergleich nicht aussagekräftig. Desgleichen sollte aber das unerforschte Dunkelfeld der Internetkriminalität nicht als Argumentationsgrundlage für die Erforderlichkeit der Überwachungsintensität herangezogen werden.

⁶² Keller / Griesbaum, Das Phänomen der vorbeugenden Bekämpfung von Straftaten, NStZ 1990, S. 416 ff. (420)

⁶³ Meseke, Internet und Kriminalität, (1. Einleitung)
<http://www.bka.de/aktuell/agenda98/vtr98/vtr_meseke98>

⁶⁴ Schetsche, Internetkriminalität: Daten und Diskurse, (2. Globaler Zuständigkeitsanspruch),
<<http://www1.uni-bremen.de/~mschet/interkrim>>

Der Tätigkeits- und Interessenschwerpunkt der Ermittler läßt sich den Statistiken jedoch entnehmen. Dieser kann im weiteren als Orientierungspunkt dienen. Zusammenfassend bilden folgende Straftatbestände den Ermittlungsschwerpunkt:

1) § 184 III StGB – „harte“ Pornographie:

Die geänderte Ansicht der Rechtsprechung⁶⁵ zum Verbreitungsbegriff ist stark umstritten. Im Ergebnis erfaßt die Gegenansicht, die für die Verbreitung an der Notwendigkeit einer Substanzübertragung festhält, die gleichen Sachverhaltskonstellationen im Internet über die Begehungsart des öffentlichen Zugänglichmachens⁶⁶.

Straftaten gem. § 184 III StGB unterfallen dem Weltrechtsprinzip, § 6 Nr. 6 StGB⁶⁷. Über den Wortlaut des § 6 StGB hinaus ist ein Inlandsbezug als Anknüpfungspunkt erforderlich⁶⁸.

2) §§ 86, 86 a, 130 StGB -Staatsschutz

Rund 40 % des Fallaufkommens in diesem Bereich entfielen 1999 auf den Linksextremismus⁶⁹. Ferner wird im Rahmen des Staatsschutzes politisch motivierte Ausländerkriminalität erfaßt, mit einem Anteil von etwa 20 % an der Gesamtfallzahl.

Das übrige Fallaufkommen ergibt sich aus dem rechtsextremistischen Bereich. All diese Straftatbestände, seit 1997 auch §§ 86, 86 a StGB, erfassen auch das *Zugänglichmachen* von Dateninhalten, sind somit auch hinsichtlich der Internet-Kriminalität einschlägig⁷⁰.

3) Entgegen der öffentlichen Wahrnehmung folgen diesen Delikten in der Statistik nicht Delikte der Software- und Datenpiraterie, sondern seit 1999

⁶⁵ BGH MMR 2001, S. 676 ff. (677)

⁶⁶ Gercke, Anmerkung zu BGH a.a.O., MMR 2001, S. 678 ff. (679)

⁶⁷ Graf, Möglichkeiten zur Verbesserung der Zusammenarbeit, (3. Straftaten im Internet), <http://www.bka.de/aktuell/agenda98/vortrag_graf.doc>

⁶⁸ Soiné, Strafverfolgung, Polizei und Internet I, Polizeispiegel 2001, 167 ff. (167)

⁶⁹ ohne Verfasserangabe, Internet und Kinderpornographie, Die Polizei 1999, S. 265 ff. (265)

⁷⁰ Derksen, Bekämpfung von Rechtsradikalismus und Rassismus im Internet, ZFIS 1999, S. 150 ff. (152)

kontinuierlich Verstöße gegen das **Arznei- und das Betäubungsmittelgesetz**. Erfolge ergeben sich hier vermehrt aus der Ermittlung in „Bodybuilding“-Usenet-Foren, in denen verbotene Substanzen angeboten werden⁷¹.

C. Eingriffsqualität der Internet-Recherche

Zur Überprüfung der Rechtmäßigkeit der anlaßunabhängigen Internetermittlung ist zunächst festzustellen, ob die derzeit praktizierte Streifenförmigkeit in Grundrechte der Betroffenen eingreift. Nur dann ist eine Ermächtigungsgrundlage erforderlich.

I. Recherchedienste

1) Bayern

Das Landeskriminalamt und das Polizeipräsidium München begannen bereits am 1. Februar 1995 mit ihrem Pilotprojekt, eigeninitiativ und ereignisunabhängig dem „allgemeinen Verdacht“⁷² von Straftaten im Internet nachzugehen.

Nach 4 Jahren wurde 1999 dann eine dauerhafte Zentralstelle für Bayern in einer Personalstärke von neun Beamten beim bayerischen LKA eingerichtet. Weiterhin ermitteln auch neun Beamte beim Polizeipräsidium München anlaßunabhängig im Netz⁷³.

Zu Beginn der Tätigkeit in Bayern lag im Zentrum des Ermittlerinteresses die Überwachung der Mailbox-Angebote (vgl. S. 7). Inzwischen erstreckt sich die Ermittlung auf alle gängigen Internet-Dienste, hauptsächlich jedoch auf Usenet und IRC. Eine konzentrierte Suche nach anderen Delikten als dem Bereich der harten Pornographie sei dabei aufgrund der geringen Personalstärke nicht zu bewerkstelligen⁷⁴.

⁷¹ Steiger / Adler, Auf Streife, DPolBl 4/2001, S. 23 ff. (24)

⁷² Fiehl, Bekämpfungssituation aus der Sicht der Polizei, (1. Ausgangslage) <http://www.bka.de/aktuell/agenda98/vtr98/vtr_fiehl98.html>

⁷³ Kant, Internet-Streifen, Bürgerrechte & Polizei 1/2002, S. 29 ff. (29)

⁷⁴ Fiehl, Erfahrungen bei der Recherche, der kriminalist 1999, S. 2 ff. (2)

2) BKA

Aufgrund der Erfahrungen in Bayern regte der bayerische Innenminister an, auch in anderen Bundesländern entsprechende Recherchezentralen einzuführen. Befürchtet wurden jedoch Doppelrecherchen und ein unkoordiniertes Vorgehen, - bis hin zur Situation, daß Internetermittler anderen Ermittlern zum Schein inkriminiertes Material anbieten, ohne ihre Kollegen als solche erkennen zu können⁷⁵.

Durch Beschluß der Innenministerkonferenz vom 21./22.10.98 wurde daher das Bundeskriminalamt (BKA) mit der Wahrnehmung der anlaßunabhängigen Recherchen in Datennetzen beauftragt. Es erfolgte die Einrichtung der „Zentralstelle für anlaßunabhängige Recherche in Datennetzen“ (ZaRD). Derzeit im Aufbau ist nun das sog. „Technische Servicezentrum IuK-Technologien“ (TeSIT).

Beim BKA in Wiesbaden ermitteln 12 Beamte anlaßunabhängig im Netz. Überdies sind in Bonn-Meckenheim 8 Beamte der Staatsschutzabteilung speziell mit der Internetermittlung für den Bereich der Staatsschutzdelikte betraut.

Auch das BKA ermittelt wie die bayerischen Kollegen in allen gängigen Internet-Diensten. Derzeit entfallen etwa 30 % der Gesamt Recherchezeit auf das WWW, 40 % auf IRC und 20 % auf die Recherche in Newsgroups. Die übrige Präsenzzeit im Netz wird sonstigen Diensten, vermehrt auch den populären Messengerdiensten, gewidmet.

II. Vorgehensweise der Ermittler

1) Surfen nach der „Jedermann-Methode“⁷⁶

Wie **jedermann** sind die Behörden bei Providern und entsprechenden Online-Diensten angemeldet.

⁷⁵ Götte, Spurensuche im Internet, Deutsche Polizei 11/98, S. 6 ff. (7)

⁷⁶ Fiehl, Bekämpfungssituation aus der Sicht der Polizei, (1. Ausgangslage)
<http://www.bka.de/aktuell/agenda98/vtr98/vtr_fiehl98.html>

Für Teledienste besteht keine dem § 18 VI MStV vergleichbare Regelung. Gestützt auf jene Norm kann die zuständige Aufsichtsbehörde unentgeltlichen und ungehinderten Zugang zu Mediendiensten verlangen, um deren Zulässigkeit zu überprüfen. Demgegenüber ist der Zugang zu Telediensten und sonstigen Inhalten für die Ermittler nicht unentgeltlich und kann ihr gegenüber vom Anbieter im Zugang beschränkt werden⁷⁷.

Auch setzen die Ermittler die „**jedermann**“ zur Verfügung stehende Internetsoftware ein, um systematisch in den Datennetzen zu recherchieren.

Die BKA-Ermittler sehen ihr Hauptziel und zugleich die Grenze ihres Aufgabenbereichs in der **Feststellung und Identifizierung des Verantwortlichen**. Erst dadurch und danach können die örtliche Zuständigkeit der Behörden und des Gerichts festgestellt und die Angelegenheiten entsprechend an das zuständige LKA **weitergeleitet** werden. Ergeben sich aus der Recherche Verdachtsfälle mit ausländischem Tatort, so werden diese den zuständigen Behörden auf dem Interpol-Weg übermittelt⁷⁸.

Die Recherchedienste sind *rund um die Uhr* aktiv, insbesondere, um auch die flüchtige, nicht gespeicherte Kommunikation im IRC erfassen zu können.

Zu ihren wesentlichen Aufgaben zählen die Recherchedienste darüber hinaus die taktische **Öffentlichkeitsarbeit**: Polizeiliche Präsenz im Internet habe „einen nicht zu unterschätzenden präventiven Charakter.“⁷⁹ Dieser Punkt wird bei der Überprüfung der Präventivkraft der Maßnahme noch relevant werden.

2) Einsatz von Überwachungstools

Die Suche nach einschlägigen Begriffen in üblichen Suchmaschinen, z.B. Google, liefert keine einer effizienten Ermittlung dienlichen Ergebnisse. Vom Bundesinnenministerium wurde daher das Bundesamt für Sicherheit in der Informationstechnik (BSI) damit beauftragt, ein Internetermittlungstool,

⁷⁷ Germann, Gefahrenabwehr und Strafverfolgung, S. 517

⁷⁸ Schuster, Die Grenzen polizeilicher Ermittlungen, in Bäumler (Hrsg.) E-Privacy, S. 77 ff. (83)

⁷⁹ Lorch, Ermittlungen im Internet, Kriminalistik 2001, S. 328 ff. (328)

genannt **INTERMiT**, zur automatisierten, gezielten Recherche zu entwickeln⁸⁰. Die Software befindet sich derzeit beim bayerischen LKA und beim BKA in der Erprobung.

Während INTERMiT nach Wörtern und Begriffen sucht, ermöglicht das von einem Ermittler entwickelte Programm **PERKEO** die automatisierte Feststellung von Bilddateien. PERKEO steht für „Programm zur Erkennung relevanter kinderpornographischer eindeutiger Objekte“ und wird inzwischen sowohl vom BKA für News-Server und im Web als auch u.a. von Providern selbst eingesetzt⁸¹.

Das Programm arbeitet mit der Erstellung von digitalen Fingerabdrücken: Das BKA bildet solche Prüfsummen von sichergestellten kinderpornographischen Bilddateien und stellt diese neuen Identifizierungsmuster regelmäßig in eine Vergleichsdatei ein⁸². Von der zu durchsuchenden Datei werden ebenfalls digitale Identifizierungsmuster erstellt und mit der Vergleichsdatei abgeglichen. Ermittelte Treffer werden mit Angabe der Verzeichnis-Fundstelle und des Dateinamens in einer Textdatei ausgegeben. – Nach dem gleichen Prinzip arbeitet Anti-Virus-Software. -

Die Trefferquote wird mit 30 % angegeben: Von 100 relevanten pornographischen Dateien in einer Recherchequelle sind also bereits rund 30 in PERKEO erfaßt und werden demnach automatisch wiedererkannt. Das Verfahren der Prüfsummenerstellung hat neben dem geringen Datenvolumen den großen Vorteil, daß in die Vergleichsdatenbank keine strafrechtlich relevanten Dateien, sondern nur deren digitalen Fingerabdrücke eingestellt werden müssen.

Jedoch erzeugt bereits eine 1-bit-Veränderung ein anderes Identifizierungsmuster, einen abweichenden digitalen Fingerabdruck⁸³. Ein minimal verändertes Bild würde schon nicht mehr erkannt werden. Dem wird

⁸⁰ Kant, Internet-Streifen, Bürgerrechte & Polizei 1/2002, S.29 ff. (34)

⁸¹ Lorch, PERKEO, <http://www.bka.de/aktuell/agenda98/vtr99/vtr_lorch.html>

⁸² Lorch, Ermittlungen im Internet, Kriminalistik 2001, S. 328 ff.(331)

⁸³ Zöllner, Verdachtslose Recherchen und Ermittlungen im Internet, GA 2000, S. 563 ff. (568)

zum einen dadurch begegnet, daß die Vergleichsdatenbank stetig aktualisiert wird. Ferner aber läßt die relativ hohe Trefferquote den Schluß zu, daß jedenfalls bislang die einschlägigen Dateien unverändert verbreitet werden⁸⁴.

III. Grundrechtsschutz im Internet - Eingriffsqualität der Streife

1) Art. 5 I GG

a) Schutzbereich

Art. 5 I GG führt die Reihe der Kommunikationsgrundrechte an (Art. 5, 8, 9, 10, 17 GG⁸⁵). Geschützt werden die freie Meinungsäußerung des Individuums in Art. 5 I 1 Hs. 1, die Informationsfreiheit in Art. 5 I 1 Hs. 2, ferner die Presse- und Rundfunkfreiheit in S.2.

Der Schutz des Art. 5 GG wächst mit neuer Technologie und neuen Kommunikationsmitteln mit und schützt daher auch die Meinungsäußerung im Internet. Die Internet-Angebote müssen vorliegend nicht im einzelnen unter die Alternativen in Art. 5 I GG subsumiert werden, da der Schutzbereich ohnehin einheitlich gefaßt ist.

b) Eingriff

Fraglich ist, ob die Internetstreife, durch die sich die Polizei Kenntnis über die Angebotsinhalte verschafft, einen Eingriff in die freie Meinungsäußerung darstellt.

Die Recherchedienste verfolgen bei ihrer Tätigkeit das Ziel, gegen rechtswidrige Angebote vorzugehen. Eine Auffassung führt exakt gegen diese Konstellation Art. 5 I 3 GG ins Feld: Jede mit System erfolgende Kontrolle zur Sanktionsvorbereitung stelle eine Form der Zensur dar, die gemäß Art. 5 I 3 verboten sei.

Dem widerspricht allerdings schon die historische Auslegung: Das Zensurverbot in Art. 5 I 3 GG sollte nur eine Vorzensur verhindern. Gegen die Ausdehnung auf die Nachzensur spricht auch, daß dieses Verbot den Staat

⁸⁴ Lorch, Ermittlungen im Internet, Kriminalistik 2001, S. 328 ff.(332)

⁸⁵ Riepl, Informationelle Selbstbestimmung im Strafverfahren, S. 19

gegenüber rechtswidrigen Meinungsäußerungen handlungsunfähig machen würde. Die Internetstreife stellt damit keine Zensur im Sinne des Art. 5 I 3 GG dar.

Ein Eingriff liegt vor, wenn die freie Meinungsäußerung behindert oder tatsächlich sanktioniert wird. Die bloße Kenntnisnahme und Rezeption der Angebote beeinträchtigt jedoch die Möglichkeit der Äußerung nicht und stellt somit keinen Eingriff in Art. 5 I GG dar.

2) Art. 8 I GG

Auch Art. 8 I GG gehört zu den Kommunikationsgrundrechten. Das Grundrecht schützt die Freiheit des Einzelnen, sich mit anderen zu einem gemeinsamen Zweck zu versammeln.

Fraglich ist, ob das virtuelle Zusammenkommen der Teilnehmer im Internet unter den Versammlungsbegriff des Grundgesetzes fällt⁸⁶. Die Frage stellt sich nur für den Chatroom, da bei der gemeinsamen Meinungsfindung innerhalb einer Newsgroup im Usenet die Teilnehmer nicht in Echtzeit und nicht unmittelbar interagieren.

Der verfassungsrechtliche Versammlungsbegriff ist in zahlreichen Punkten äußerst umstritten, so etwa hinsichtlich des geforderten gemeinsamen Zwecks und bezüglich der Anzahl der Personen.

In diesen Punkten wirft der Internet-Chat aber keine neuartigen Probleme auf: Nach der herrschenden Meinung ist in der realen Welt die Zusammenkunft von *zwei* Personen hinreichend, die sich zum *Zwecke gemeinsamer Meinungsbildung* und –äußerung versammeln, wobei nach dem weiten Versammlungsbegriff der Gegenstand dieser „Meinung“ beliebig ist und nicht öffentlicher oder politischer Natur sein muß.

All dies ließe sich auf die Online-Situation übertragen: Es handelt sich beim Chat gerade nicht um eine „bloße Ansammlung“, sondern mindestens zwei

⁸⁶ Stadler, Anlaßunabhängige Überwachung des Internet,

Teilnehmer kommen gezielt zu Zwecken gemeinsamer Kommunikation in den Chatroom.

Zur Bestimmung des Schutzbereichs hilft bisweilen auch bereits der Blick auf den Eingriff, also die Frage, wogegen geschützt werden soll⁸⁷. Im Internet sind durchaus Maßnahmen mit Eingriffscharakter hinsichtlich der Versammlungsfreiheit vorstellbar, insbesondere sogar durch die Internetstreife: Das Bundesverfassungsgericht hat in der Brokdorf-Entscheidung einen Eingriff durch „exzessive Observationen“⁸⁸ angenommen. Die Versammlungsfreiheit wird also auch durch **faktische Maßnahmen** beeinträchtigt, wenn diese in ihrer Wirkung imperativen Maßnahmen gleichkommen.

Wenn die Betroffenen als Folge der exzessiven Überwachung auf die Grundrechtsausübung verzichten, wird von einem Eingriff in Artikel 8 I GG ausgegangen. Bedroht und schutzwürdig erscheint damit grundsätzlich auch online die "Persönlichkeitsentfaltung in Gruppenform" zur Vermeidung der Isolierung voneinander.

Allerdings wirft das Internet eine **neue Frage im Schutzbereich** auf: Problematisch erscheint im Chatroom der Begriff des „Sich-Versammelns“ selbst⁸⁹.

Zweifel daran ergeben sich nicht schon aus dem Ausdruck „unter freiem Himmel“ in Art. 8 II GG, der online nicht anwendbar wäre. Dieser Terminus beruht auf der Annahme des Grundgesetzgebers, daß von Versammlungen in geschlossenen Räumen geringere Gefahren für kollidierende Rechte Dritter ausgehen. Auch offline wird entgegen dem Wortlaut die Differenzierung daher teleologisch am Vorliegen einer Begrenzung „zur Seite“ festgemacht. Dies ließe sich online vergleichen mit dem Zugangsschutz.

Problematisch ist jedoch, daß sich die Teilnehmer eben nur virtuell, nur im

<<http://www.afs-rechtsanwaelte.de/internetstreife.htm>>

⁸⁷ Pieroth / Schlink, Grundrechte, Rn. 237

⁸⁸ BVerfGE 69, 315 (349) - Brokdorf

⁸⁹ Kniessel, Versammlungs- und Demonstrationsfreiheit, NJW 2000, S. 2857 ff. (2860)

„Cyberspace“⁹⁰ gemeinsam, treffen. Für dieses Phänomen läßt sich auch als Hilfsmittel der Beurteilung kaum ein funktionales Offline-Äquivalent vorstellen. Fraglich ist dabei, ob die virtuelle Anwesenheit das körperliche „Sich-Versammeln“ ersetzen kann.⁹¹

Es findet sich nur ein einziger Hinweis zum Erfordernis der Körperlichkeit im Versammlungsbegriff. Dieser spricht gegen eine Einbeziehung des Chats in den Schutzbereich der Versammlungsfreiheit:

Eine Versammlung muß „friedlich und ohne Waffen“ erfolgen. Diese Voraussetzung wird in Anlehnung an die Legaldefinition der §§ 5 Nr. 3, 13 I Nr. 2 VersG negativ bestimmt: Eine Versammlung ist danach unfriedlich, wenn ein gewalttätiger und aufrührerischer Verlauf droht⁹². Eine Gewalttätigkeit wird hier - enger als in § 240 StGB – nur bei einer **aktiven körperlichen** Einwirkung auf Personen oder Sachen angenommen.

Die Voraussetzung der „friedlichen Versammlung“ **liefe** im virtuellen Raum somit mangels Körperlichkeit **stets gänzlich leer**. Das gemeinsame Chatten läßt sich folglich nicht vollumfänglich im klassischen Versammlungsbegriff abbilden. Dies spricht gegen eine Eröffnung des Schutzbereichs der Versammlungsfreiheit im virtuellen Raum. Eine Versammlung liegt somit im IRC nicht vor. Schon der Schutzbereich des Art. 8 I GG ist damit nicht eröffnet.

3) Art. 10 I GG

a) Schutzbereich

Auch Art. 10 I GG wird zu den kommunikativen Grundrechten gezählt. Dieses Grundrecht schützt unter anderem das Fernmeldegeheimnis:

Gewahrt werden soll die Vertraulichkeit von räumlich distanzierter Kommunikation, die über unkörperliche Signale zwischen den Teilnehmern

⁹⁰ Lloyd, Information Technology Law, S. 7: Der Ausdruck „Cyberspace“ wurde 1984 zur Bezeichnung dieser „imaginary location where the words of the parties meet in conversation“ (Lloyd) geprägt von William Gibson in dessen Roman „Necromancer“.

⁹¹ Kniessel, Versammlungs- und Demonstrationsfreiheit, NJW 2000, 2857 ff. (2860): „Die virtuelle Anwesenheit kann aber die körperliche wohl nicht ersetzen.“

⁹² BVerfGE 69, 315 ff. (360) - (Brokdorf)

ausgetauscht wird⁹³. Denn auf dem Übertragungsweg der Nachrichten zwischen Sender und Empfänger ist deren Privatsphäre besonders bedroht.

Aus diesem Schutzzweck ergibt sich zugleich auch die Grenze des Schutzbereichs, die durch einen Blick in das einfache Recht plastisch wird: § 3 Nr. 16 TKG definiert die Telekommunikation als „technischen Vorgang des Aussendens, Übermittels und Empfangens“. Über die Schutzlücke zwischen den Machtbereichen des Absenders und des Empfängers hilft das Telekommunikationsgeheimnis hinweg. Es greift jedoch weder vor Beginn noch nach Vollendung dieses Übermittlungsvorgangs.

Davon abgesehen ist vom Schutzzumfang jedoch nicht nur der Kommunikationsinhalt während der Übertragung umfaßt, sondern nach ständiger verfassungsgerichtlicher Rechtsprechung auch die näheren Umstände und die Vorgänge der Telekommunikation.⁹⁴ Geschützt sind danach die Verbindungsdaten, also Angaben über u.a. die Kommunikationsteilnehmer, Zeitpunkt und Dauer⁹⁵. Nicht umfaßt sind hingegen die Bestandsdaten⁹⁶.

Trotz des dynamisch zu verstehenden Schutzbereichs ist die Heranziehung für die Neuen Medien nicht unproblematisch: Die Einordnung in Individual- und Massenkommunikation gestaltet sich schwierig. Denn auch die Internetangebote, die nicht zugangsgeschützt und daher der Öffentlichkeit, einem allgemeinen Empfängerhorizont, zugänglich sind, werden durch die einzelnen User individuell abgerufen.

Auf den Inhalt der Angebote kann zur Bestimmung des Rezipientenkreises jedoch auch nicht zurückgegriffen werden: Dies ist dem Fernmeldegeheimnis wesensfremd. Das Ziel der Vertraulichkeit würde damit bereits zur Bestimmung des Schutzbereiches unterlaufen.

⁹³ Löwer in: von Münch/Kunig, GG I, Art. 10, Rn. 18

⁹⁴ Bizer, Verschlüsselung und staatlicher Datenzugriff, in: Büllersbach (Hrsg.), Datenschutz im Telekommunikationsrecht, S. 245 ff. (249)

⁹⁵ Holznagel / Enaux / Nienhaus, Grundzüge des Telekommunikationsrechts, S. 189

⁹⁶ Wuermeling / Felixberger, Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz, CR 1997, S. 230 ff. (234)

Somit muß zu einem umfassenden Schutz auf die technischen Voraussetzungen abgestellt werden: Schon die technische Möglichkeit des Vorliegens von Individualkommunikation eröffnet den Schutzbereich⁹⁷. Damit unterfallen alle Kommunikationsvorgänge im Internet *in ihrer Übermittlungsphase* dem Schutzbereich des Art. 10 I GG.

b) Eingriff

Bei der dargestellten Vorgehensweise der Internetstreife greift die Behörde auf die ins Netz gestellten WWW-Seiten zu, verschafft sich Kenntnis über den Inhalt der Usenet-Postings und nimmt am Internet-Chat teil: In allen betrachteten Diensten ist die Behörde damit selbst Kommunikationspartnerin der Anbieter, also Empfängerin der geäußerten Meinungen. Sie nimmt von den Inhalten erst nach Abschluß des Übermittlungsvorgangs Kenntnis, wenn diese bereits in ihren Empfänger-Machtbereich gelangt sind. Auch zwischen Sender und Empfänger gilt das Fernmeldegeheimnis nicht darüber hinaus⁹⁸. Zur Abwehr der Internetstreife kann sich der Absender somit gar nicht auf den Schutz aus Artikel 10 GG berufen, weil die Behörde nicht in den Übermittlungsvorgang eingreift, um sich Kenntnis zu verschaffen.

Eine mögliche Verschleierung der Ermittlereigenschaft ist in diesem Rahmen deshalb auch irrelevant: Dies würde nichts an der Tatsache des abgeschlossenen Übertragungsvorgangs ändern. Ein Eingriff in Art. 10 geht somit von der Streifentätigkeit selbst nicht aus.

4) Art. 2 I i.V.m. 1 I GG – Recht auf informationelle Selbstbestimmung

a) Schutzbereich

Zur Begründung der Grundrechtsrelevanz der informationellen Tätigkeit des Staates wurden zwei grundlegend verschiedene Konzepte entwickelt:

aa) Sphärentheorie

Dieser Ansatz des Privatheitsschutzes übernimmt eine Betrachtungsweise des Zivilrechts: Privatheit wird aufgefaßt als räumlich abgeschlossener Bereich⁹⁹.

⁹⁷ Germann, Gefahrenabwehr und Strafverfolgung im Internet, S. 118

⁹⁸ BVerfG NJW 1992, S: 1875 ff. (1875) - Fangschaltung

⁹⁹ Deutsch, Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, S. 39

Unterschieden in der Schutzwürdigkeit werden dabei drei „Schutzbereiche der Privatsphäre“: rechtlich ungeschützt, relativ geschützt und absolut geschützt.¹⁰⁰ Werden Inhalte zur Kenntnis einer unbeschränkten Öffentlichkeit gebracht, so erfährt hier die Privatheit keinen Schutz. Die veröffentlichten Internetinhalte sind nach der Sphärentheorie dem rechtlich ungeschützten Bereich zugehörig. Der einzelne soll davor geschützt werden, sich in einem unerwünschten Umfang offenbaren zu müssen. Macht er jedoch Inhalte willentlich publik, verläßt er den schutzwürdigen Rahmen der Privatsphäre.

bb) Abkehr von der Sphärentheorie – Recht auf informationelle Selbstbestimmung

Hatte sich die Sphärentheorie noch im Mikrozensus-Urteil wiedergefunden, so folgt das Bundesverfassungsgericht seit dem Volkszählungsurteil dem Gegenkonzept und konkretisierte es maßgeblich: Das sog. Recht auf informationelle Selbstbestimmung entwickelte sich in der Literatur im Rahmen der Referentenentwürfe zu einem Bundesdatenschutzgesetz¹⁰¹. Ziel des Ansatzes ist der umfassende Schutz personenbezogener Daten, der „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar natürlichen Person“ (§ 3 I BDSG).

Kern dieses Konzepts und auch Beweggrund für die Abkehr von der Sphärentheorie ist die Einsicht, daß von der modernen Datenverarbeitung neuartige Gefahren ausgehen: Bei der Betrachtung der Grundrechtsgefährdung kann in der Informationsgesellschaft nicht mehr allein auf die Art des einzelnen Datums abgestellt werden, wie dies bei der Sphärentheorie vollzogen wird. Maßgeblich ist auf die Nutzbarkeit und Verwendungsmöglichkeiten zu achten, will man der Gefahr einer Informationszusammenführung und der Bildung von Persönlichkeitsprofilen begegnen: Das informationelle Selbstbestimmungsrecht ist damit nicht datums-, sondern verarbeitungsorientiert¹⁰².

¹⁰⁰ Weßlau, Vorfeldermittlungen, S. 173

¹⁰¹ Deutsch, Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, S. 64

¹⁰² Riepl, Informationelle Selbstbestimmung im Strafverfahren, S. 8

Verfassungsrechtlich verankert ist das informationelle Selbstbestimmungsrecht in Art. 2 I i.V.m. Art. 1 I GG, als Ausprägung des allgemeinen Persönlichkeitsrechts: Gewährleistet ist „die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“¹⁰³. Das informationelle Selbstbestimmungsrecht stellt als Zusammenfassung des Persönlichkeitsschutzes ein an den Staat adressiertes Verbot dar, personenbezogene Daten zu erheben und zu verarbeiten¹⁰⁴.

Erforderlich für die Zugehörigkeit zum Schutzbereichs ist somit nur noch die Eigenschaft als personenbezogenes Datum, also als Information, die sich auf eine einzelne, natürliche Person bezieht oder geeignet ist, einen Bezug zu ihr herzustellen. Zu den schutzwürdigen „sachlichen Verhältnissen“ gehören dabei *auch Identifikationsangaben*, die ansonsten keine Aussage über die Person treffen: Daraus wird deutlich, daß nicht nur die Internetangebote dem Schutzbereich unterfallen, die etwa im Rahmen der Pflicht zur Anbieterkennzeichnung gem. § 6 TDG eine Identifizierung ermöglichen. Vielmehr führt die Architektur des Internets dazu, daß sämtliche Angebote schon dadurch personenbezogen werden, daß der Verantwortliche über seinen Datenschatten bestimmbar ist (vgl. S. 12). Aus der IP-Architektur des Netzes folgt eine umfassende Eröffnung des Schutzbereichs.

b) Eingriff

Nach der Bejahung eines derart weiten Schutzbereichs ist nun zu prüfen, ob die Internetermittler bei ihrer Tätigkeit Maßnahmen mit Eingriffscharakter vornehmen.

aa) Einwilligung

Einer Auffassung nach hat der für den Internet-Beitrag Verantwortliche, der **ohne Zugangsschutz** im Netz veröffentlicht, damit in den Zugriff durch jedermann *eingewilligt*¹⁰⁵. Ein Eingriff sei zu verneinen.

¹⁰³ BVerfGE 65, 1, Leitsatz 1

¹⁰⁴ Murswiek in Sachs, GG, Art. 2, Rn. 72

¹⁰⁵ Kudlich, Strafprozessuale Probleme des Internet, JA 2000, S. 227 ff. (229)
Graf, Internet: Straftaten und Strafverfolgung, DRiZ 1999, S. 281 ff. (285)

Ein denkbarer „geheimer Vorbehalt“, die Inhalte jedoch nicht Polizeibeamten zur Verfügung stellen zu wollen, sei in Anlehnung an die Kasuistik zu § 123 StGB unbeachtlich¹⁰⁶. Herangezogen wird damit die Rechtsprechung in den sog. „**Testkäufer“-Fällen**¹⁰⁷:

(1) Testkäufer und virtuelles Hausrecht

Zu Beginn der 60er Jahre setzten die Hersteller preisgebundener Waren zur Überprüfung des Einzelhandels sog. Testkäufer ein. Diesen Testkäufern versuchten die Ladeninhaber den Zutritt durch entsprechende Verbotsschilder zu verwehren, obgleich das Ladenlokal für den allgemeinen Publikumsverkehr geöffnet war.

Die Zutrittsbefugnis wird bei der Öffnung für den allgemeinen Publikumsverkehr generell und unter Verzicht auf eine Prüfung im Einzelfall erteilt. Der Testkäufer betrat den Laden wie ein „normaler Käufer“. Der psychische Widerstand des Rechteinhabers wird also durch Besucher gebrochen, die unerwünscht sind, sich aber äußerlich unauffällig verhalten. Eine Verschiebung vom räumlichen auf diesen geistigen Aspekt würde den Schutzbereich des Hausrechts überdehnen¹⁰⁸. Das „Testkäufer“-Verhalten hält sich deshalb im Rahmen der Einwilligung.

Auf den ersten Blick scheint die Konstellation des Testkäufers in der Tat übertragbar auf geheime Vorbehalte der Betreiber von Internetangeboten. Das über das Kaufinteresse hinausgehende Kontrollinteresse tritt beim Testkäufer ebenso wenig nach außen zu Tage wie das Ermittlerinteresse beim Besuch einer Internetseite¹⁰⁹.

Der gefällige Vergleich mit dem Hausrecht wird aufgegriffen und näher ausgeführt durch aktuelle zivilrechtliche Entscheidungen:

¹⁰⁶ Zöller, Verdachtslose Recherchen und Ermittlungen im Internet, GA 2000, S. 563 ff. (569)

¹⁰⁷ Bär in: Wabnitz / Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, Kap. 18, Rn. 250

¹⁰⁸ Hanack, Hausfriedensbruch durch Testkäufer, JuS 1964, S. 352 ff. (355)

¹⁰⁹ Bär, Auf dem Weg zur „Internet-Polizei“? in Bäumler (Hrsg.), Polizei und Datenschutz, S: 167 ff. (170)

Einem Betreiber eines „allgemein zugänglichen Dienstes ohne besondere Zugangskontrollen und verbindlich formulierte Nutzungsbedingungen“¹¹⁰ wird ein **virtuelles Hausrecht** zugestanden.

Die oben dargestellten Grundsätze hinsichtlich § 123 StGB überträgt das Gericht auf den Internet-Chat. In diesem virtuellen Diskussionsraum sei mangels Einschränkungen ein „Geschäft für den allgemeinen Publikumsverkehr“ eröffnet worden¹¹¹. Der Betreiber des Chatrooms will sein Angebot dabei nur im Rahmen der störungsfreien Nutzung zur Verfügung stellen. Auch hier könne der Chat-Betreiber sein virtuelles Hausrecht aber nicht willkürlich ausüben und niemandem den Zugang verweigern, der sich „nicht außerhalb des ‚üblichen Chatterverhaltens‘ bewegt“¹¹². Es gelte das allgemeine Verbot widersprüchlichen rechtlichen Verhaltens gem. § 242 BGB¹¹³.

(2) Übertragbarkeit auf das informationelle Selbstbestimmungsrecht

Bei Bejahung eines derart umfassenden Verzichts auf das Grundrecht wäre der Eingriffscharakter der Ermittlungsmaßnahmen zu verneinen¹¹⁴. Aufgrund dieser weitreichenden Konsequenz ist sehr sorgfältig zu prüfen, ob mit dem Testkäufer-Vergleich wirklich das passende funktionale Äquivalent für die Internet-Ermittlung herangezogen wird.

Das informationelle Selbstbestimmungsrecht ist ganz spezifischen Gefahren ausgesetzt. Anders als bei einer Sache besteht bei Daten gerade durch die moderne Datenverarbeitung die Möglichkeit, daß diese **über den eigenen Informationsgehalt hinaus** durch Verknüpfung mit anderen Daten eine neue Dimension bekommen. Genau deshalb sieht das Bundesverfassungsgericht unter den Bedingungen der automatischen Datenverarbeitung „kein belangloses Datum“ mehr¹¹⁵.

¹¹⁰ OLG Köln, 23.06.2000, Beschluß 19 U 2/00, el. publiziert unter <<http://www.olg-koeln.nrw.de/home/presse/archiv/urteile/2000/19U002-00>>

¹¹¹ LG Bonn, NJW 2000, S. 961 ff. (961)

(aufgehoben vom OLG Köln durch Beschluß 19 U 2/00 im Rahmen der Prozeßkostenentscheidung. Jedoch stimmt das OLG Köln dem „virtuellen Hausrecht“ ausdrücklich zu: <<http://www.olg-koeln.nrw.de/home/presse/archiv/urteile/2000/19U002-00>>)

¹¹² LG Bonn, NJW 2000, S. 961 ff. (962)

¹¹³ Sakowski, Virtuelles Hausrecht, <<http://www.sakowski.de/onl-r/onl-r65.html>>

¹¹⁴ Pieroth / Schlink, Grundrechte, Rn. 140

¹¹⁵ BVerfGE 65, 1 ff. (45)

An die Einwilligung im Bereich des informationellen Selbstbestimmungsrecht werden daher besondere Anforderungen gestellt. Eine Definition der Einwilligung in das informationelle Selbstbestimmungsrecht findet sich etwa in Art. 2 h der EG- Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/46/EG):

„jede Willensbekundung, die ohne Zwang, **für den konkreten Fall und in Kenntnis der Sachlage** erfolgt und mit der die betroffene Person akzeptiert, daß personenbezogene Daten, die sie betreffen, verarbeitet werden.“

Auch ein Blick auf das einfache Recht verdeutlicht die erhöhten Anforderungen an eine Einwilligung in das informationelle Selbstbestimmungsrecht:

§ 4 a BDSG fordert die Schriftform, „soweit nicht wegen besonderer Umstände eine andere Form angemessen ist“.

§ 89 X TKG erwähnt die Möglichkeit einer Einwilligung im „elektronischen Verfahren“, auch diese muß aber „ausdrücklich“ erfolgen.

Problematisch erscheint vorliegend weniger die fehlende Schriftform. „Besondere Umstände“ im genannten Sinne können im Internetverkehr wohl angenommen werden. Gemeinsam ist aber der Richtlinie und den angeführten Beispielen im einfachen Recht, daß die Erteilung ausdrücklich und frei von Zweifeln erfolgen soll. Es spiegelt sich darin die Berücksichtigung der besonderen Gefahrenlage wieder.

Der Betroffene kann vorliegend ein legitimes Interesse daran haben, eine Information für die Allgemeinheit freizugeben, ohne dabei zugleich auch in die nicht überschaubare Verwendung, etwa die Katalogisierung der Persönlichkeit durch Datenzusammenführungen einzuwilligen.

Alldem trägt der Testkäufer-Vergleich durch seine Übersimplifizierung „Keine Eingriffsqualität bei *allgemein zugänglichen Daten*“ nicht Rechnung:

Geschütztes Rechtsgut des § 123 StGB ist das Hausrecht¹¹⁶. Das Hausrecht ist ein Konglomerat verschiedener Rechte, die sich aus **Eigentum und/oder Besitz** ergeben¹¹⁷. Bei der Gewährung des Zutritts zu einem Raum ergeben sich aber keine Problemstellungen, die der weiteren Verwendbarkeit von Daten über ihren eigenen Informationsgehalt hinaus funktional vergleichbar sind.

Das informationelle Selbstbestimmungsrecht ist durch die dargestellte Möglichkeit der Verknüpfung und Profilbildung ganz anderen Gefahren ausgesetzt als das (Sach-) Eigentum. **Es sind zwei verschiedene grundrechtliche Schutzbereiche berührt.** Bei der Wahl eines funktionalen Äquivalents ist stärker auf die Vergleichbarkeit der Schutzbereiche und der Gefahren für das Grundrecht zu achten.

Auch das „virtuelle Hausrecht“ im IRC führt hinsichtlich der Einwilligung in das informationelle Selbstbestimmungsrecht nicht weiter: Selbst, daß ein Chatroombetreiber den Zugang zum Server freigibt, muß noch nicht bedeuten, daß die einzelnen Teilnehmer auch vollumfänglich und ohne Vorbehalt auf das informationelle Selbstbestimmungsrecht bezüglich ihrer Beiträge verzichten. Schon die Grundrechtsträger sind hier also zu unterscheiden.

Die Freigabe der Daten im Internet bedeutet somit jedenfalls nicht, daß in jegliche Verwendung der Daten eingewilligt wurde. Fraglich ist aber, ob eine Einwilligung zumindest in die dem Internet typischen Verwendungszwecke angenommen werden kann. Die im Rahmen der „Jedermann-Methode“ durchgeführten Ermittlungsmaßnahmen hielten sich dann gerade in diesem typischen Rahmen.

Eine solche Differenzierung ist vom Urheberrecht bekannt: Ein Urheber, der Inhalte ohne Zugangsschutz online stellt, stimmt konkludent dem Abruf der Daten durch jedermann und auch der (einfachen) Verlinkung zu, weil sich diese Verwendungsarten als *integraler Bestandteil* des Internets darstellen. In

¹¹⁶ Hanack, Hausfriedensbruch durch Testkäufer, JuS 1964, S. 352 ff. (353)

¹¹⁷ Christensen, Taschenkontrolle im Supermarkt und Hausverbot, JuS 1996, S. 873 ff. (873)

weitergehende Nutzungsarten wird jedoch nicht, auch nicht konkludent, eingewilligt.

Trotz der Nähe von Daten, sog. informationellen Gütern, zu den Immaterialgüterrechten kann jedoch auch diese Differenzierung nicht auf die Einwilligung in die Datenerhebung durch die Ermittler übertragen werden. Die Einwilligung in das informationelle Selbstbestimmungsrecht muß ohne jeden Zweifel feststehen. Dem Prinzip des „informed consent“ wird eine konkludente Einwilligung nicht gerecht¹¹⁸. Auch in die Ermittlungsmaßnahmen, die nur typische Nutzungshandlungen darstellen, wird somit nicht eingewilligt.

bb) Zwischenergebnis nach der sog. Eingriffstheorie

Aufgrund der fehlenden Einwilligung bejaht deshalb eine Auffassung vor dem Hintergrund, daß es kein belangloses Datum mehr geben dürfe, den Eingriff in das informationelle Selbstbestimmungsrecht¹¹⁹: Bei jeglicher Erhebung, Speicherung und sonstiger Verarbeitung, jeder staatlichen Informationsbeschaffung, sei die Eingriffsqualität zu bejahen, (sog. Eingriffstheorie)¹²⁰.

Eine Erhebung personenbezogener Daten mit Eingriffsqualität sei bereits anzunehmen, wenn Daten aus Quellen wie Telefon- oder Adreßbüchern gewonnen werden¹²¹. Damit verglichen besteht durch die mit automatischer Datenverarbeitung operierende Internetstreife in der Tat eine noch gesteigerte Gefährdung der Persönlichkeitsprofil-Bildung.

Problematisch ist jedoch die These, es bestehe im Eingriffscharakter ein Unterschied zwischen Online- und klassischer Offline-Streife¹²²: Das Bundesverfassungsgericht wies zwar auf die gesteigerte Gefährdungslage

¹¹⁸ Information des Bundesdatenschutzbeauftragten zur Einwilligung:
<http://www.bfd.bund.de/information/info5/kap03/03_03>

¹¹⁹ (Hamann im Interview mit) Schulzke-Haddouti, Maschinenstürmer im Bundesinnenministerium, <<http://www.heise.de/tp/deutsch/inhalt/te/1547/1.html>>

¹²⁰ Schwan, Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte, Verwaltungsarchiv 1975, S. 120 ff. (128)

¹²¹ Stadler, Anlaßunabhängige Überwachung des Internet,
<<http://www.afs-rechtsanwaelte.de/internetstreife.htm>>

¹²² (so: Hamann im Interview mit) Schulzki-Haddouti, Maschinenstürmer im Bundesinnenministerium, <<http://www.heise.de/tp/deutsch/inhalt/te/1547/1.html>>

automatischer Datenverarbeitung hin, machte diese aber mit keinem Wort zur Voraussetzung der Eingriffsqualität¹²³.

So mag also ein Unterschied in der Eingriffsintensität bestehen, mit einer möglichen Konsequenz unterschiedlicher Ermächtigungsgrundlagen.¹²⁴ Auch kommen für die beiden Streifenfahrten unter Umständen unterschiedliche Aufgabenzuweisungsnormen (präventiv und rein repressiv) in Betracht.

Hinsichtlich der Eingriffsqualität selbst hingegen kann eine Differenzierung zwischen der Streifenfahrt in der realen Welt und der online-Streife von dieser Ansicht nicht argumentativ herangezogen werden. Vielmehr bedeutet die Entscheidung für einen derart weiten Eingriffsbegriff bei konsequenter Anwendung auch die Eingriffsqualität der Streifenfahrt in der realen Welt: Auch bei dieser Maßnahme werden aktiv personenbezogene Daten aufgenommen, in der Absicht, diese ggf. für entsprechende Sanktionen weiterzuverwenden.¹²⁵

Diese Annahme eines so umfassenden Eingriffsbegriffs ist im Konzept aner kennenswert. Hierbei wird in erster Linie nur das informationelle Selbstbestimmungsrecht gegen jegliche Relativierungstendenzen verteidigt¹²⁶. In der Bringschuld hinsichtlich der Argumentation stehen gerade jene Vertreter, die dieses ursprünglich sehr umfassend gesehene Recht nunmehr wieder in seine Schranken verweisen wollen. Zunehmend liefert jedoch gerade das im Volkszählungsurteil postulierte Ziel diese geforderten Argumente zur Einschränkung, wie nun darzulegen sein wird:

cc) Ziel des Volkszählungsurteils und status quo der Zielerreichung

Bisher schien der beste Weg zur Wahrung des informationellen Selbstbestimmungsrechts ein sehr weit verstandener Schutzbereich und eine niedrige Schwelle zur Eingriffsqualität, wie gerade für die Streifenfahrt dargestellt. **Das vom Bundesverfassungsgericht erkannte und allem**

¹²³ Deutsch, Die heimliche Erhebung von Informationen, S. 72

¹²⁴ Kant, Internet-Streifen, Bürgerrechte & Polizei 1/2002, S. 29 ff. (36)

¹²⁵ Germann, Gefahrenabwehr und Strafverfolgung, S. 476

¹²⁶ Weßlau, Vorfeldermitteilungen, S. 181

zugrundegelegte Ziel, den Umgang mit personenbezogenen Daten für den Betroffenen überschaubar zu machen, ist aber auf dem bisher beschrittenen Weg nicht mehr zu erreichen.

Eine interessante Parallele zum Datenschutz läßt sich derzeit im Verbraucherschutz beobachten: Um dem Bürger Sicherheit zu geben, sind dort umfassende Informationspflichten vorgesehen. Mit zunehmender Informationstechnologie und Ausdehnung des e-commerce wächst auch die Unsicherheit. Dem wird begegnet mit weiteren, immer zahlreicheren Informationspflichten¹²⁷.

Inzwischen haben diese Pflichten jedoch - insbesondere im IT-Bereich - ein solch verwirrendes Ausmaß erreicht, daß sich ein Online-Anbieter nahezu entscheiden muß: Kommt er jeder einzelnen Informationspflicht auf seiner Web-Seite korrekt nach, kann er das erste und oberste Gebot nicht mehr erfüllen: Übersichtlichkeit und Überschaubarkeit für den Verbraucher.

Vor demselben Dilemma steht derzeit das Datenschutzrecht:

Setzt man die Eingriffsschwelle derart niedrig an, ist dem Betroffenen damit nur vordergründig gedient. Normenklare und bereichsspezifische Ermächtigungsgrundlagen sind bei einer solch niedrigen Eingriffsschwelle nicht im nötigen Umfang zu realisieren¹²⁸:

Bis heute, seit dem Volkszählungsurteil ohne Unterbrechung, läuft die „Gesetzesmaschinerie auf vollen Touren“¹²⁹. Noch immer ist man mit der Schließung von Gesetzeslücken befaßt: So brauchte der Bundesgesetzgeber nach dem Volkszählungsurteil mehr als 15 Jahre, um in einem derart sensiblen Bereich wie dem Strafverfahrensrecht schließlich umfassendere Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zu schaffen. Mit jedem Entwicklungsschritt der Informationstechnologie scheinen nur neue Lücken im Gesetz hinzuzukommen.

¹²⁷ Köhler / Arndt, Recht des Internet, S. 55

¹²⁸ Germann, Gefahrenabwehr und Strafverfolgung, S. 482

¹²⁹ Duttge, Zur Hypertrophie des Datenschutzes, NJW 1998, S. 1615 ff. (1616)

Angesichts dieser bezüglich Gesetzeslage, -fülle und -qualität gänzlich unbefriedigenden Situation ist eine Besinnung auf das ursprüngliche Ziel des Volkszählungsurteils geboten: Der Pluralismus in der Gesellschaft braucht Bürger, die von ihren kommunikativen Grundrechten umfassend Gebrauch machen¹³⁰. Sie sollen sich dazu bereit und in der Lage sehen, weil sie überschauen, „wer was wann und bei welcher Gelegenheit über sie weiß.“¹³¹

Interessant erscheint dazu gerade angesichts der Vorfeldermittlung der Internetstreife die Betrachtungsweise, im Bemühen der Verfassungsrichter stecke hier eine Verlagerung ins Vorfeld des Grundrechtsschutzes, eine Verstärkung des Präventionsgedankens¹³². In Anbetracht der ausufernden Vorfeldarbeit des Staates scheint es nur legitim und angebracht, auch die Abwehrrechte des Bürgers gegen den Staat vorzuverlagern.

Angesichts der stetig komplexer werdenden modernen Datenverarbeitung liegt der Weg zu dem hohen Ziel der unbefangenen Kommunikation jedoch nicht in undurchsichtigen Regelungswerken infolge einer sehr niedrigen Eingriffsschwelle¹³³. Gerade im Bestreben, dem im Volkszählungsurteil aufgezeigten Fernziel gerecht zu werden, muß dieses Lagebild anerkannt werden, um den Blick auf eine adäquate Lösung zu öffnen.

Ist das aufgezeigte Dilemma heute ganz unübersehbar, so ist die Erkenntnis selbst nicht neu: Es zeichneten sich schon kurz nach dem Volkszählungsurteil Relativierungstendenzen ab, um des Problems Herr zu werden¹³⁴. Fraglich ist jedoch, auf welche Weise dies geschehen muß, um das Ziel des Bundesverfassungsgerichts gerade besser als mit der bisher verfolgten Lösung zu erreichen.

¹³⁰ Hoffmann-Riem, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998), S. 513 ff. (522)

¹³¹ BVerfGE 65, S. 1 ff. (42)

¹³² Duttge, Zur Hypertrophie des Datenschutzes, NJW 1998, S. 1615 ff. (1618)

¹³³ Germann, Gefahrenabwehr und Strafverfolgung, S. 482

¹³⁴ Riepl, Informationelle Selbstbestimmung im Strafverfahren, S. 28

Keinesfalls im Interesse des Bürgers liegt es hingegen, noch 15 Jahre nach dem Volkszählungsurteil „eine Behördenpraxis, die erst aufgrund eines Wandels der verfassungsrechtlichen Anschauungen den bis dahin angenommenen Einklang mit der Verfassung verliert, **vorübergehend hinzunehmen**, bis der Gesetzgeber ausreichend Gelegenheit gehabt hat, die Regelungslücke zu schließen“¹³⁵.

Angesichts dessen muß der – während nahezu vier Legislaturperioden - zeitlich überforderte Gesetzgeber also offenbar auf andere Weise entlastet werden.

dd) Lösungen auf der Ebene des Eingriffsbegriffs

Die Lösung wird überwiegend in einer rationaleren Betrachtung der Eingriffsqualität gesehen. Damit werden Ressourcen der Legislative frei, mit denen schneller, normenklarer und gründlicher dort Regelungen geschaffen werden können, wo diese tatsächlich dem Ziel der informationellen Selbstbestimmung dienlich sind. Es liegen verschiedene Ansätze zur Wahl des Eingrenzungskriteriums vor:

(1) Zugänglichkeit der Daten

Einer Ansicht nach stellt nur die hoheitliche Datenerhebung einen Eingriff in das informationelle Selbstbestimmungsrecht dar.¹³⁶ Was die Streifenbeamten aber im Zugriff auf allgemein zugängliche Informationsquellen aufnehmen, könne auch jeder beliebige Dritte wahrnehmen¹³⁷.

Im Ergebnis kommt dieser Lösungsansatz der Annahme einer umfassenden, vorbehaltlosen Einwilligung gleich und ist aus den dazu bereits ausgeführten Gründen abzulehnen: Die spezifischen Gefährdungen durch die Datenverarbeitung finden in dieser generellen Eingrenzung über die Zugänglichkeit keine ausreichende Berücksichtigung.

¹³⁵ so aber, noch die Lösung über die Generalklausel zulassend: LG Frankfurt, NJW 1999, S. 73 f. (74) (Akten der StA) - **Hervorhebung nicht im Original** -

¹³⁶ Meseke, Ermittlung und Fahndung im Internet, in BKA (Hrsg.), Festschrift für Herold, S. 505 ff. (521)

¹³⁷ Weßlau, Vorfeldermittlungen, S. 197

(2) Erfordernis einer konkreten Grundrechtsgefährdung

Eine Auffassung kehrt gleichsam die Regel zur Ausnahme um: Für eine offene Gesellschaft sei der freie Informationsfluß von konstituierender Bedeutung. Ein Verfügungsrecht über die eigenen informationellen Güter solle dem einzelnen danach nur in einer besonderen, rechtfertigungsbedürftigen Gefährdungslage eingeräumt werden¹³⁸.

Diese sei etwa bei der allgemeinen Streife noch nicht anzunehmen, weil sich hier die Gefährdung des Grundrechts im „allgemeinen Lebensrisiko“¹³⁹ halte. Eine gesteigerte Gefährdung sei hingegen anzunehmen bei der Streife in zugangsgeschützten Bereichen. Der Betroffene müsse hier nicht mit einer Observation rechnen und sei deshalb besonders gefährdet. - Hierin liegt eine Übereinstimmung zum zuvor dargestellten Eingrenzungskriterium. -

Nicht zielführend ist aber bereits die der Ansicht zugrundeliegende Haltung, ein unbestimmtes „Gefühl von Furcht“ sei ohne Belang und Bedeutung¹⁴⁰. Der Bereich informationeller Selbstbestimmung reicht so tief in die Persönlichkeitssphäre, daß den Befürchtungen des Bürgers vor einer unüberschaubaren Ausforschung durchaus jede Beachtung zu schenken ist. Bedroht ist die unbefangene Kommunikation eben nicht erst bei einer konkret erfahrbaren Ausforschungssituation.

Davon abgesehen ist die unklare Gefährdungslage auch kein rein emotionales, sondern durchaus ein der (insb. automatischen) Datenverarbeitung wesensimmanentes Problem: Welche Verarbeitung und Nutzung mit einem Datum möglich sind, ist bei der ursprünglichen Erhebung ja gerade noch nicht abzusehen¹⁴¹.

(3) Eingrenzung über den Begriff der Erhebung

Eine denkbare Eingrenzung des Eingriffs könnte sich auch an dem Eingriffstyp der Datenerhebung orientieren, da eine Erhebung am Beginn jeder

¹³⁸ Duttge, Zur Hypertrophie des Datenschutzes, NJW 1998, S. 1615 ff. (1619)

¹³⁹ WeBlau, Vorfelddermittlungen, S. 197

¹⁴⁰ so aber: Duttge, Zur Hypertrophie des Datenschutzes, NJW 1998, S. 1615 ff. (1618)

¹⁴¹ Germann, Gefahrenabwehr und Strafverfolgung, S. 488

Datenverarbeitung steht. Das Volkszählungsurteil verwendet diesen Begriff, ohne ihn jedoch näher aufzuschlüsseln. Ein Orientierungspunkt dazu findet sich nur im einfachen Recht: Danach bedeutet Datenerhebung das „Beschaffen von Daten über den Betroffenen“ (§ 3 III BDSG).

Aus dieser Formulierung ergibt sich nach einer Auffassung die Begrenzung des Erhebungsbegriffs auf eine „intendierte, auf den Betroffenen gezielte Beschaffung“¹⁴². Die zufällige Wahrnehmung scheidet als Erhebung in diesem Sinne aus, auch wenn durch sie personenbezogene Daten gewonnen werden.

Die Auswertung allgemein zugänglicher Quellen (z. B. Telefonbücher, *Medien*) sei ferner ein bloßer Rückgriff auf Informationen, die Dritte bereits erhoben haben¹⁴³. Fraglich ist hierbei, ob dies auch auf das Internet zutreffen würde, wenn die Daten dort vom Betroffenen selbst eingestellt wurden. Denn dabei liegt trotz der allgemeinen Zugänglichkeit eine vorherige Erhebung durch Dritte gerade nicht vor.

So wird die Beobachtung bei Observationen in der realen Welt dann auch als klassischer Fall der Datenerhebung anerkannt, genauso wie die Datenerhebung beim Betroffenen selbst.

Unabhängig von der Einordnung der Internetstreife jedoch kann die Begrenzung auf das *gezielte* Vorgehen nicht überzeugen: Gerade das Beispiel der Streife in der realen Welt zeigt, daß eine im Beginn ungezielte Maßnahme nahezu übergangslos in eine gezielte Beobachtung überführt wird, wenn die Beamten auf eine Person aufmerksam werden¹⁴⁴. Auch die Maßnahmen, die im Beginn nicht „auf einen Betroffenen gezielt“ eingesetzt werden, tragen in sich bereits das Fernziel der Erlangung personenbezogener Daten nach der Verdachtsgewinnung. Die zuvor ungezielt erlangten Daten wirken darin auch fort. Daraus wird deutlich, daß das Kriterium des gezielten Eingriffs diese Daten nicht ausreichend unter Schutz stellt.

¹⁴² Tinnefeld, Persönlichkeitsrecht und Modalitäten der Datenerhebung im Bundesdatenschutzgesetz, NJW 1993, S. 1117 ff. (1117)

¹⁴³ Tinnefeld, Persönlichkeitsrecht und Modalitäten der Datenerhebung im Bundesdatenschutzgesetz, NJW 1993, S. 1117 ff. (1117)

¹⁴⁴ Weßlau, Vorfelddermittlungen, S. 193

Auch wirkt die Ausgrenzung der bereits „von Dritten erhobenen Daten“ willkürlich: Es ist nicht ersichtlich, warum ein kombinierter Rückgriff auf je für sich bereits erhobene Daten nicht genau das im Volkszählungsurteil gezeichnete Bedrohungsszenario verwirklicht.

(4) Eingrenzungskriterium der Überschaubarkeit

Ein eng am Wortlaut des Volkszählungsurteils orientiertes Eingrenzungskriterium findet sich im Begriff der „Überschaubarkeit“¹⁴⁵. Hierin drückt sich das Wesen des informationellen Selbstbestimmungsrechts aus: In seiner freien Entfaltung ist der Bürger gehemmt, wenn er „nicht mit hinreichender Sicherheit **überschauen** kann“, „wer was wann und bei welcher Gelegenheit“ über ihn weiß¹⁴⁶. Soweit ihm diese Informationen jedoch bekannt sind, stellt es sich gerade auch als Ausübung seines Rechts auf informationelle Selbstbestimmung dar, daß er auf dessen Schutz verzichtet und von seinen Kommunikationsrechten Gebrauch macht. Die vorher absehbare Erhebung solcher Daten begrenzt seine Freiheit nicht, da sie *in diesem Rahmen* in seine Abwägung hinsichtlich der Offenbarung und bleibenden Entäußerung der Informationen einbezogen werden kann.

Dieses Kriterium wird mithin den Anforderung des Bundesverfassungsgerichts und insbesondere der Gefahrenlage gerecht. Der Gedanke der Überschaubarkeit findet sich desgleichen im Prinzip des „informed consent“ wieder. Die zur Einwilligung und zu den weiteren Relativierungsbemühungen vorgetragenen Bedenken ergeben sich somit diesem Abgrenzungsmerkmal gegenüber nicht. Gleichfalls ist dieses Kriterium geeignet, Bagatellfälle sachgerecht auszuschließen und die Uferlosigkeit, der sich die Vertreter der Eingriffstheorie gegenübersehen, zu vermeiden¹⁴⁷.

c) Eingriffsqualität der einzelnen Maßnahmen

Unter Zugrundelegung des Gesagten sind somit die Aussagen des Zwischenergebnisses nach der Eingriffstheorie erneut zu überprüfen. Ergänzt

¹⁴⁵ Germann, Gefahrenabwehr und Strafverfolgung, S. 489

¹⁴⁶ BVerfG 65, 1 (42)

¹⁴⁷ Germann, Gefahrenabwehr und Strafverfolgung, S. 489

man also den Eingriffstatbestand um die Voraussetzung der fehlenden Überschaubarkeit, so ergibt sich für die Internetkommunikation folgende Betrachtung:

aa) WWW

Die bloße Rezeption der Webseiten auf der Suche nach strafrechtlich relevanten Angebotsinhalten stellt nach dieser Eingrenzung anders als nach der Eingriffstheorie keinen Eingriff dar. Denn auch die Kenntnisnahme speziell durch polizeiliche Ermittler muß insoweit als absehbar und überschaubar bewertet werden: Wer Inhalte online stellt, kann davon ausgehen, daß dies entsprechende staatliche Kontrolle und bei strafrechtlicher Relevanz Sanktionierung nach sich zieht. Selbst wenn das Internet von dem Betroffenen noch als rechtsfreier – bzw. *rechtsdurchsetzungsfreier* - Raum betrachtet würde, kommt hier ein Vergleich mit der Wertung des § 17 StGB in Betracht: Es besteht die Pflicht zu Gewissensanspannung und Einsatz aller Erkenntniskräfte, in diesem Rahmen auch Überschaubarkeit.

Anders als bei der Eingrenzung über die öffentliche Zugänglichkeit ist die Eingriffsqualität jedoch zu bejahen, wenn die Behörden die Informationen aus dem Angebot mit Zusatzinformationen verknüpfen und aus dieser Datenzusammenführung neue Informationen entnehmen. Als Beispiel kommt hier die Überprüfung in Betracht, wann eine Person im Internet aktiv war und ob sie demgemäß auch für bestimmte andere Straftaten in diesem Zeitraum als mutmaßlicher Täter in Betracht kommt.¹⁴⁸ Dies sprengt den Rahmen der Überschaubarkeit. Obwohl rein technisch auch diese Vorgehensweise der sog. „Jedermann-Methode“¹⁴⁹ zuzuordnen ist, braucht die Behörde neben der Aufgabenzuweisungsnorm hierzu also ferner noch eine Eingriffsgrundlage zur Datenerhebung, (ggf. sogar zur Datenerhebung mit technischen Mitteln¹⁵⁰).

bb) FTP

Etwas anderes könnte sich für die Ermittler beim Zugriff auf FTP-Server

¹⁴⁸ Germann, Gefahrenabwehr und Strafverfolgung, S. 512

¹⁴⁹ Fiehl, Bekämpfungssituation aus der Sicht der Polizei, (1. Ausgangslage)
<http://www.bka.de/aktuell/agenda98/vtr98/vtr_fiehl98.html>

¹⁵⁰ Kant, Internet-Streifen, Bürgerrechte & Polizei 1/2002, S. 29 ff. (36)

ergeben. Anders als beim WWW besteht hier eine Möglichkeit der Identifikation einzelner Teilnehmer. Fraglich ist, ob trotz der reinen Rezeption der Inhalte hier in die Prüfung der Überschaubarkeit auch die Ermittlereigenschaft des Kommunikationsteilnehmers einzubeziehen ist.

Beim *anonymen* FTP-Server ist die Möglichkeit der Nutzung ohne konkrete Offenlegung der Identität jedoch ausdrücklich vorgesehen. (Nur in diesen FTP-Typ kann auch bei reiner Streifentätigkeit ohne weiteres vorgedrungen werden.) Der Zugang ist ohne Kontrolle im Einzelfall jedermann geöffnet: Es ist lediglich aus technischen Gründen die Eintragung der Angaben „guest“ oder „anonymous“ erforderlich.

Eine Angabe der Ermittlertätigkeit würde hier wohl auch gar nicht von den Anbietern zur Kenntnis genommen, vielmehr würde lediglich automatisiert der Zugang verweigert, weil die Eingabe ins Formularfeld unbekannt ist.

cc) IRC

Das Vorgehen der Behörde im IRC ist die am heftigsten umstrittene Maßnahme. Auch bei bloßer Rezeption der einzelnen Beiträge kann es hierbei für die Beurteilung der Überschaubarkeit auch auf die Identität der Kommunikationspartner ankommen. Anders als bei Usenetpostings und WWW-Veröffentlichungen begibt sich der Teilnehmer an einem Internetchat nicht der Möglichkeit, den Rezipientenkreis zu überblicken. Es besteht jederzeit die Möglichkeit der „/Whois-Abfrage“ (S. 9).

Fraglich ist, ob das Auftreten unter einem Nickname, ohne Hinweis auf die Ermittlereigenschaft zumindest im Nutzernamen, deshalb die Eingriffsqualität begründet und ob durch diese Verschleierung die Überschaubarkeit zu verneinen ist. Die bayerische Behörde sieht sich durch das BayPAG ohnehin auch zu verdecktem Vorgehen befugt und macht ihre Behördeneigenschaft im Nutzernamen nicht deutlich¹⁵¹.

¹⁵¹ Fiehl, Bekämpfungssituation aus der Sicht der Polizei, (1.Ausgangslage)
<http://www.bka.de/aktuell/agenda98/vtr98/vtr_fiehl98.html>

Auch das BKA ordnet dieses Vorgehen ohne Offenlegung im Nutzernamen noch nicht als Verschleierung ein. Der ermittelnde Beamte müsse seine Identität nicht ungefragt offenbaren¹⁵². Verglichen wird das Vorgehen auch mit dem Besuch eines Polizisten bei öffentlichen Veranstaltungen: Dieser könne statt Uniform seine Zivilkleidung tragen und müsse auch nicht auf seine Ermittlereigenschaft hinweisen¹⁵³.

Bei diesem Argumentationsgang wird jedoch bereits die Frage der Rechtfertigung mit der Feststellung der Eingriffsqualität vermischt. Zur Beurteilung des Eingriffscharakters ist allein auf die Überschaubarkeit abzustellen: Im IRC kann jeder Teilnehmer den aktuellen Empfängerkreis übersehen und wie dargestellt die Nickname-Pseudonyme einfach aufdecken. Bei der Anmeldung beim IRC-Server ist der echte Name als Nutzernamen anzugeben: Die Behörde kann einen beliebigen Nickname wählen, muß aber im Nutzernamen ihre Behördeneigenschaft ausdrücklich darlegen. Verwendet der Ermittler im Nutzernamen seinen wirklichen Namen ohne Behördenzusatz, so ist der hoheitliche Hintergrund für die anderen Teilnehmer nicht überschaubar¹⁵⁴. In diesem Vorgehen liegt daher ein Eingriff in das informationelle Selbstbestimmungsrecht. Das Datenschicksal der Angebote ist für den einzelnen nicht mehr berechenbar.

Die Konstellation erinnert an den Streitstand zum Vernehmungsbegriff und zur Belehrungspflicht bei informatorischer Befragung: Die Bedenken der Anhänger des sog. funktionalen Vernehmungsbegriffs gewinnen bei der zunehmenden Verschiebung der polizeilichen Tätigkeit ins Vorfeld neue Relevanz.

Schon jenseits des Aufbaus einer Vertrauensbeziehung - etwa zur Besorgung eines Paßworts zum zugangsgeschützten Bereichs - liegt aufgrund der fehlenden Überschaubarkeit des Datenschicksals in der unterlassenen

¹⁵² Graf, Befugnisse und Grenzen der Ermittlungsbehörden, DPoIb1 4/2001, S. 6 ff. (7)

¹⁵³ Ochsenbein, Strafrechtliche Aspekte des Internet, Kriminalistik 1998, S. 685 ff.(687)

¹⁵⁴ Germann, Gefahrenabwehr und Strafverfolgung im Internet, S. 520

Offenlegung der Ermittlereigenschaft ein Grundrechtseingriff in das informationelle Selbstbestimmungsrechts¹⁵⁵.

Gleiches gilt für eine Teilnahme am Usenet durch nicht nur bloße Rezeption, sondern aktives Posting ohne Offenlegung der Behördeneigenschaft¹⁵⁶.

dd) Eingriffsqualität des Einsatzes von Ermittlungstools

Als funktionales Äquivalent in der realen Welt drängt sich für die Ermittlungstools zunächst das Instrument der Rasterfahndung auf. Diese Ermittlungsmaßnahme wurde bereits in den Anfängen der Computertechnologie als „klinisch saubere Fahndungsmethode“¹⁵⁷ der Zukunft gefeiert. Unschuldige sollen danach automatisch aus dem Visier der Ermittler herausfallen, ohne individuell durch Ermittlungen behelligt werden zu müssen. Gleiches könnte insbesondere auch für den Einsatz von PERKEO geltend gemacht werden.

Die Kritiker der Rasterfahndung hingegen sehen mit Recht in diesem Argumentationsgang belegt, daß bei der Rasterfahndung in Widerspruch zur Unschuldsvermutung ein Generalverdacht über jeden einzelnen verhängt wird. Dieser solle sich dann gleichsam glücklich schätzen, wieder herausgerastert zu werden. Dies widerspricht dem Rechtsstaatsprinzip.

Bei der Variante der „positiven Rasterfahndung“ wird in verschiedenen Datenbeständen nach Personen gesucht, die bestimmte Merkmale aufweisen. Die Kriterien im Raster werden mit den anderen Dateien abgeglichen, um passende positive Gegenstücke zu finden. **Ergebnis ist eine neue Datensammlung** derer, die Träger der positiven Merkmale sind.

Diese Vorgehensweise entspricht auf den ersten Blick in der Tat dem beschriebenen Verfahren beim PERKEO-Einsatz. Fraglich ist, ob damit auch die Kritikpunkte der Rasterfahndung übertragbar sind. Damit käme bei

¹⁵⁵ BT-Drucksache 14/5555, 18. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz vom 13.03.01, S.105

¹⁵⁶ Kant, Internet-Streifen, Bürgerrechte & Polizei 1/2002, S. 29 ff. (35)

¹⁵⁷ Horst Herold im Interview, Die Polizei als gesellschaftliches Diagnoseinstrument, in: Appel, Hummel, Hippe (Hrsg.), Die Neue Sicherheit, S. 65 ff. (84)

Vergleichbarkeit der Verfahren dem PERKEO-Einsatz Eingriffsqualität zu. Denn die Rasterfahndung gewährleistet keinerlei Überschaubarkeit: Vielmehr realisiert sich in diesem Verfahren je nach den gewählten Rasterkriterien exakt die Gefahr der Verbindung von Einzeldaten zur Gewinnung eines Informationsgehalts über die Ausgangsdaten hinaus. Damit liegt gleichsam der Prototyp des gefürchteten Eingriffs in das informationelle Selbstbestimmungsrecht vor.

Bei genauer Betrachtung liegt in diesem Punkt aber der entscheidende Unterschied des PERKEO-Einsatzes: Es werden gerade nicht Daten verknüpft, sondern es wird nur eine einzelne Bilddatei, bzw. deren Prüfsumme, abgeglichen. Damit wird die Überwachung erleichtert, erfährt aber keine neue Qualität verglichen mit der manuellen Durchsicht der WWW-Seiten durch die Ermittler selbst. Deshalb ist weiterhin von der Überschaubarkeit auszugehen: Die bloße quantitative Steigerung der Durchsicht macht die einzelne Datenerhebung nicht unüberschaubar.

Für PERKEO können damit in der Tat die Argumente berechtigterweise geltend gemacht werden, die gegenüber der Rasterfahndung noch unhaltbar waren: Die maschinelle Durchsicht gefährdet die Privatsphäre der Gesamtheit der Nutzer weniger als die manuelle WWW-Durchsicht: Es ergibt sich im Ansatz ein Datenschutz durch Technik, ähnlich dem Konzept des sog. Systemdatenschutzes. Ferner ermöglicht der Einsatz des digitalen Fingerabdrucks eine derart hohe Treffsicherheit, dass anders als bei der Rasterfahndung auch kein fälschlicher Verdacht auf Unschuldige geworfen wird.

Etwas anderes ergibt sich hingegen dann, wenn auch die manuelle Durchsicht selbst aus Datenschutzgründen schon nicht gestattet ist: Bedenklich ist daher der aktuelle Einsatz bei Universitäten und Providern, wenn diese die Ordner ihrer Clients nach rechtswidrigen Hinweisen scannen und dabei zumindest per Ermittlungstool auch die geschützten Daten von redlichen Usern kontrollieren. Denkbar scheint in diesen Fällen eine entsprechende Klarstellung in den jeweiligen Geschäftsbedingungen.

Der Eingriffscharakter von INTERMiT kann hier nicht mit letzter Sicherheit beurteilt werden: Zur genauen Funktionsweise sind aus ermittlungstaktischen Gründen keinerlei Details des Suchvorgangs bekannt. Bei der Verwendung von Wörtern drohen die problematischen Folgen der Rasterfahndung zwar eher als beim PERKEO-Bilddateienabgleich. Das System der herkömmlichen Suchmaschinen andererseits verknüpft nicht mehrere Datenbestände miteinander. Dabei geht die Informationsgewinnung selbst wiederum qualitativ nicht über die bloße Durchsicht hinaus. Liegt INTERMiT dasselbe Verfahren zugrunde, so ist dies für den von der Überwachung Betroffenen überschaubar und stellt keinen Eingriff dar.

5) Art. 13 GG

a) Schutzbereich

Art. 13 I GG schützt den Wohn- und Wirkbereich als Stätte der persönlichen Entfaltung und Selbstverwirklichung: Geschützt sind damit nicht nur die privaten Wohnräume, sondern auch solche Geschäftsräume, die dem allgemeinen Publikumsverkehr entzogen sind.

Hinsichtlich Art. 13 GG ist vorliegend sorgfältig zwischen den Grundrechtsträgern zu unterscheiden: Die Eröffnung des Schutzbereichs kommt hier zum einen in Betracht für den Host-Provider, auf dessen Server die Angebote vorgehalten werden. Solche Server stellen gleichsam die „physikalischen Pfeiler“¹⁵⁸ dar, auf denen der virtuelle Raum ruht. Diese Geschäftsräume sind dabei auch – in der realen Welt - nicht der Öffentlichkeit zugänglich.

Anders stellt sich die Lage für die Verantwortlichen der Angebote dar: Diese stellen ihr Angebot ins Netz, indem sie die Dateien auf dem Server des Hostproviders ablegen. In ihren Wohn- und Wirkbereich wird damit im Regelfall nicht vorgedrungen: Auf ihren eigenen Rechner wird im Regelfall nicht zugegriffen. Etwas anderes ergibt sich nur bei der Öffnung von Teilen der Festplatte für andere User: bei der Einrichtung eines File-Servers auf dem

¹⁵⁸ Dix, Internationale Aspekte in: Bäumler (Hrsg.), E-Privacy, S. 93 ff. (93)

eigenen PC. Nur in diesen Fällen kommt die Eröffnung des Schutzbereichs von Art. 13 auch für den Anbieter selbst in Betracht.

Daß der Öffentlichkeit hierbei der virtuelle Zugang gestattet ist, steht der Eröffnung des Schutzbereichs nicht entgegen: Ansatzpunkt für Art. 13 GG ist nicht etwa ein Bereich im virtuellen Raum, sondern abzustellen ist wie erwähnt auf die Verkörperung¹⁵⁹: Der Rechner selbst steht in einem Wohn- oder Wirkbereich, der dem allgemeinen Publikumsverkehr entzogen ist.

b) Eingriff

Ein Eingriff kann sich nicht nur in einem körperlichen Vorgehen, etwa in einer Durchsuchung vor Ort am Rechnerstandort, manifestieren. Aus der in Art. 13 III GG erwähnten Schranke der akustischen Überwachung ergibt sich vielmehr, daß auch unkörperlichen Maßnahmen Eingriffsqualität beigemessen wird.

War die Eröffnung des *virtuellen* Raums für den allgemeinen Verkehr im Schutzbereich ohne Belang, so kann sie doch der Eingriffsqualität entgegenstehen: Zurückzukommen ist wieder auf die „Testkäufer“-Analogie. Durch die Inbetriebnahme eines Servers, bzw. die Einrichtung eines File-Servers auf der eigenen Festplatte wird in den Zugriff generell eingewilligt¹⁶⁰. Der Zugriff auf das Speichermedium im Rahmen des üblichen Userverhaltens stellt sich als integraler Bestandteil des Internets dar. Geheimen Vorbehalten gegen einen behördlichen Abruf der Daten kommt insofern keine Wirkung zu.

Die Ablehnung der Testkäufer-Kasuistik im Rahmen des informationellen Selbstbestimmungsrechts beruht allein auf der spezifischen Gefahrenlage jenes Rechts und dem Prinzip des „informed consent“. Im Rahmen von Art. 13 GG scheint die Heranziehung des Hausrechts als funktionales Äquivalent jedoch überzeugend: Die Ermittler „in die Wohnung“ zu lassen, stellt eine Einwilligung, den Verzicht auf den grundrechtlichen Schutz der Wohnung dar¹⁶¹. Ein Eingriff in Art. 13 liegt damit weder gegenüber dem Host-Provider,

¹⁵⁹ Bär, Auf dem Weg zur „Internet-Polizei“?, in: Bäuml (Hrsg.), Polizei und Datenschutz, S. 167 ff. (174)

¹⁶⁰ Kudlich, Strafprozessuale Probleme des Internet, JA 2000, S. 227 ff. (233)

¹⁶¹ Pjeroth / Schlink, Grundrechte, Rn. 130

noch im Falle von File-Servern gegenüber dem für die Inhalte Verantwortlichen vor.

6) Art. 3 I GG

Nur klarstellend sei noch erwähnt, daß aus dem Vorwurf der selektiven Strafverfolgung keine subjektiven Rechte aus Art. 3 I GG für den dabei vergleichsweise Benachteiligten erwachsen. Zwar gebietet das Legalitätsprinzip die Verfolgung jedes Verdächtigen und ist eine Ausprägung des Willkürverbots im Sinne des Art. 3 I GG. Selbst wenn man den objektiven Wertgehalt des Art. 3 GG vorliegend für berührt hält, besteht jedoch keinesfalls ein subjektives Recht, ein Anspruch auf eine „Gleichbehandlung im Unrecht“.

IV. Zusammenfassung zur Eingriffsqualität

Ein Eingriff (in. Art. 2 I i.V.m. 1 I GG) konnte somit nur hinsichtlich jener Ermittlungsmaßnahmen festgestellt werden, bei denen die Ermittler technisch die Gelegenheit haben, ihre Identität und Ermittlereigenschaft darzulegen, sie dies aber unterlassen: im Internet Relay Chat, wie auch bei behördlichen Usenet-Postings.

D. Aufgabenzuweisungsnorm

Auch bei in weitem Umfang verneinter Eingriffsqualität des digitalen Streifengehens „nach der „Jedermann-Methode“¹⁶² ist die Prüfung der Rechtmäßigkeit noch nicht abgeschlossen: Anders als „jedermann“ darf der Staat auch bei eingriffsfreien Maßnahmen nur im Rahmen und in den Grenzen eines zugewiesenen Aufgabenbereichs agieren¹⁶³.

I) Gefahrenabwehr oder Strafverfolgung – **tertium non datur?**

„Das Bayerische Landeskriminalamt und das Polizeipräsidium München bewiesen Weitsicht und Kompetenz, als sie sich schon vor Jahren **nicht lange**

¹⁶² Fiehl, Bekämpfungssituation aus der Sicht der Polizei, (1. Ausgangslage)
<http://www.bka.de/aktuell/agenda98/vtr98/vtr_fiehl98.html>

¹⁶³ Gusy, Polizeirecht, Rn. 12

an Zuständigkeitsfragen aufhielten, sondern damit begannen, wertvolle und beispielhafte Pionierarbeit im Kampf gegen die Kriminalität im Internet zu leisten.“¹⁶⁴

Aussagen wie diese werfen die Frage auf, ob hinreichend berücksichtigt wird, daß neben dem materiellen Strafrecht auch das Grundgesetz gleichermaßen online wie offline Geltung beansprucht. Denn sich mit Aufgabenzuweisungsnormen und Zuständigkeitsfragen „aufzuhalten“, scheint gerade im Bereich der anlaßunabhängigen Ermittlung erforderlich.

Gegen die Initiativermittlungsbefugnis, die dem BKA durch das Terrorismusbekämpfungsgesetz 2002 eingeräumt werden sollte, hatte sich ein Sturm der Kritik erhoben: Die anlaßunabhängige Ermittlung ist mangels eines Anfangsverdachts jedoch auch eine Initiativermittlung, eine Verdachtsgewinnungsmaßnahme. Die Problematik ergibt sich schon auf der Ebene des Aufgabenbereichs und stellt sich somit auch bei Maßnahmen ohne Eingriffsqualität¹⁶⁵.

Es verwundert daher, daß diese höchst umstrittene Grauzone bei der Internetstreife zumeist mit der Feststellung umgangen wird, als Rechtsgrundlage genüge **entweder** die Eröffnung des polizeilichen Aufgabenbereichs **oder** die Aufgabenzuweisung in den §§ 161, 163 StPO¹⁶⁶.

Eine genaue Einordnung unterbleibt zumeist. Fraglich ist aber gerade, ob sich die anlaßunabhängige Internetstreife überhaupt einem der beiden klassischen Aufgabenbereiche zuordnen läßt. Diese umstrittene Problematik hinsichtlich der Vorfeldermittlung droht bei einer bloßen Präventions-Repressions-Abgrenzung übersehen zu werden. Die Auffassung, bei fehlenden Verdachtsmomenten solle der Zugriff nur dem Ausschluß künftiger Gefahren

¹⁶⁴ Paulus, Pädö-Kriminelle in Datennetzen, Kriminalistik 2000, S. 390 ff. (393) -

Hervorhebung nicht im Original -

¹⁶⁵ Weßlau, Vorfeldermittlungen, S. 159

¹⁶⁶ Zöller, Verdachtslose Recherche und Ermittlungen im Internet, GA 2000, S. 563 ff. (569); Bär, in: Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, Kap. 18, Rn. 249, ders., in: Kröger / Gimmy, Handbuch zum Internetrecht, S. 638 (=ders., Strafrechtliche Kontrolle in Datennetzen, MMR 1998, S. 463 ff.); ders., Auf dem Weg zur „Internet-Polizei“? in: Bäumlner (Hrsg.) „Polizei und Datenschutz“, S. 167 ff. (169)

dienen¹⁶⁷, deckt sich gerade nicht mit der praktizierten Internetstreife: Die verdachtsunabhängig gewonnenen Informationen werden zur Einleitung eines Strafverfahrens an die zuständigen Behörden weitergeleitet¹⁶⁸.

In Betracht kommt daher, daß die Ermittlung jenseits von konkreter Gefahr und Anfangsverdacht ein selbständiges Aufgabengebiet bilden muß.¹⁶⁹

II) Funktion einer Aufgabenzuweisungsnorm

Eine Aufgabenzuweisungsnorm beschreibt die äußere Grenze des Handlungsraums der Exekutivtätigkeit. Innerhalb dieser Grenze stecken die Befugnisnormen dann die konkreten Eingriffsgrundlagen ab. Erst zahlreiche Versuche in Rechtsprechung und Literatur, der Aufgabennorm konkrete Befugnisse zu entnehmen, weckten den Bedarf nach einer klaren Unterscheidung von Aufgabe und Befugnis auch im Polizeirecht.

Die selbstständige Funktion der Aufgabennorm liegt demnach zum einen darin, die Grenze festzulegen, die die Exekutive auch mit eingriffslosem Handeln nicht überschreiten darf¹⁷⁰. Ferner spielt die Aufgabenzuweisungsnorm im Rahmen der Verhältnismäßigkeitsprüfung einer Maßnahme eine gewichtige Rolle: Die dabei zu untersuchende Mittel-Zweck-Relation orientiert sich an der Aufgabenzuweisungsnorm, da diese den vom Gesetzgeber festgelegten Zweck wiedergibt.

III) Aufgabenbereich der Bayerischen Polizeibehörde

Repression und Prävention verfolgen zwei unterschiedliche Zweckrichtungen. Zwar treten im praktischen Polizeialltag präventiv-repressive Gemengelagen auf¹⁷¹. Die Aufgabenbereiche selbst sind jedoch streng auseinanderzuhalten, um einem System der Gesamtüberwachung vorzubeugen¹⁷². Fraglich ist also, ob die Internetstreife von einem Aufgabenbereich erfaßt wird.

¹⁶⁷ Bär, in: Kröger / Gimmy, Handbuch zum Internetrecht, S. 641

¹⁶⁸ Moritz, in: Loewenheim/Koch, Praxis des Online-Rechts, S. 481

¹⁶⁹ Weßlau, Vorfeldermittlungen, S. 111

¹⁷⁰ Gusy, Polizeirecht, Rn. 11

¹⁷¹ Kniesel, Neue Polizeigesetze contra StPO, ZRP 1987, S. 377 ff. (378)

¹⁷² Nitz, Einsatzbedingte Straftaten Verdeckter Ermittler, S. 16

1) Strafverfolgung

Strafverfolgung dient der Durchsetzung des staatlichen Strafanspruchs. Die rechtliche Grundlage für die Strafverfolgungstätigkeit bildet die Strafprozeßordnung: Mittels der dort geregelten Maßnahmen ist unter der Sachleitungsbefugnis der Staatsanwaltschaft eine bereits verwirklichte rechtswidrige Tat aufzuklären. Dabei sind die Beweise für den Strafprozeß zu erheben.

Entscheidend im vorliegenden Zusammenhang ist, daß gemäß §§ 152 II, 160 I StPO zureichende tatsächliche Anhaltspunkte einer Straftat vorliegen müssen: ein Anfangsverdacht. Erst damit setzt die Kompetenz der Staatsanwaltschaft ein und gem. § 163 StPO auch erst die Eilkompetenz der Polizei¹⁷³.

Es liegt jedoch im Wesen und schon in der Bezeichnung der anlaßunabhängigen Ermittlung, daß in dem § 152 II StPO vorgelagerten Vorfeldbereich operiert wird. Die Straftaten sind zwar schon begangen, jedoch noch nicht zur Kenntnis der Behörde gelangt.

Aus diesem Grund ist auch der schmale Bereiche der Vorermittlung, bzw. Verdachtserforschung, nicht einschlägig¹⁷⁴: Die StPO erkennt derartige Maßnahmen in § 159 StPO an, dessen Anwendungsbereich auch teilweise als nicht auf die sog. „Leichensachen“ beschränkt aufgefaßt wird¹⁷⁵. Selbst wenn man eine formlose „informativische Befragung“ und Besichtigung jedoch über die Generalklausel zuläßt, so muß dabei ein weiter zu erforschender Sachverhalt bereits polizeibekannt sein. Die anlaßunabhängige Internetstreife fügt sich daher auch in diesen Bereich nicht ein.

Der Aufgabenbereich der StPO kann daher nicht herangezogen werden.

2) Klassische Gefahrenabwehr

Häufig erfolgt die Definition des Bereichs der Gefahrenabwehr durch rein negative Abgrenzung zur Strafverfolgung¹⁷⁶. Entsprechend wird auch die

¹⁷³ Lisken, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. C, Rn. 79

¹⁷⁴ Rogall, Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht, S. 88

¹⁷⁵ Keller / Griesbaum, Das Phänomen der vorbeugenden Bekämpfung von Straftaten, NStZ 1990, S. 416 ff. (417)

¹⁷⁶ Floerecke, Kriminalprävention durch Polizei, KrimJournal 1983, S. 167 ff. (174)

Internetstreife diesem Bereich zugeordnet: Aufgrund des fehlenden Anfangsverdachts sei die StPO hier nicht heranzuziehen. Also seien die hier zu prüfenden Vorfeldermittlungen dem Bereich der Gefahrenabwehr zuzuschlagen.

Indes ergibt ein Blick auf den klassischen Begriff der Gefahrenabwehr, daß die Tätigkeit der anlaßunabhängigen Ermittlung auch hier nicht eingeordnet werden kann:

Im 1977 von der Innenministerkonferenz beschlossenen „Musterentwurf eines einheitlichen Polizeigesetzes“ beschreibt § 1 I MEPOIG den Aufgabenbereich mit der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung. Bekanntlich unterscheidet das Polizeirecht zwischen abstrakten und konkreten Gefahren. Anders als für die Gefahrenabwehrverordnungen war bislang für die Eingriffsgrundlagen eine konkrete Gefahr Voraussetzung: Mit hinreichender Wahrscheinlichkeit muß bei ungehindertem Verlauf in absehbarer Zeit ein Schaden für die öffentliche Sicherheit drohen.

Zur öffentlichen Sicherheit zählt auch die gesamte geschriebene Rechtsordnung. Eine konkret bevorstehende Straftat zu verhindern würde somit unproblematisch dem klassischen Gefahrenabwehrbegriff unterfallen. So wenig wie ein Anfangsverdacht liegt aber zu Beginn der vorliegenden Tätigkeit eine den Ermittlern bekannte konkrete Gefahr vor. Sie sind sich auch keines Gefahrenverdachts bewußt, welcher sie immerhin zu Gefahrerforschungseingriffen berechtigen würde.

Auf den dargestellten klassischen Bereich der Gefahrenabwehr können sich die Ermittler deshalb auch nicht stützen, wenn sie auf eine präventive Wirkung ihres Vorgehens verweisen.

3) Entstehung einer dritten polizeilichen Aufgabenkategorie

Das hier aufgezeigte Konfliktfeld zwischen Anfangsverdacht und konkreter Gefahrenverdacht ist keineswegs neu.

Angesichts einer „Änderung der Verbrechenswirklichkeit“¹⁷⁷ wurden in der aufgezeigten Grauzone Lücken der strafprozessualen Ermittlungstätigkeit ausgemacht. Eine proaktive Vorgehensweise der Polizei im Vorfeld von zureichenden tatsächlichen Anhaltspunkten wurde speziell zur Bekämpfung von Organisierter Kriminalität gefordert.¹⁷⁸

Der Musterentwurf wurde daraufhin, ferner auch als Reaktion auf das Volkszählungsurteil, verändert. Am 12.03.1986 wurde durch den Arbeitskreis II der Innenminister und -senatoren der sog. „Vorentwurf zum Musterentwurf für ein einheitliches Polizeigesetz des Bundes und der Länder“ verabschiedet, den die Innenminister am 18.04.1986 mit Vorbehalten annahmen.¹⁷⁹ § 1 I S. 2 lautet nun:

„Sie hat im Rahmen dieser Aufgabe auch für die Verfolgung von Straftaten vorzusorgen und Straftaten zu verhüten (vorbeugende Bekämpfung von Straftaten) sowie Vorbereitungen zu treffen, um künftige Gefahren abwehren zu können (Vorbereitung auf die Gefahrenabwehr).“

Schon aus dem Wortlaut „**im Rahmen** dieser Aufgabe“, der in § 1 S. 1 genannten Aufgabe der Gefahrenabwehr, wird deutlich, daß dies lediglich als Klarstellung verstanden wurde. Eine Erweiterung des polizeilichen Aufgabenbereichs war damit nicht intendiert.

Zu prüfen ist zunächst, ob sich die Internetstreife in einen dieser drei Bereiche einordnen läßt:

a) Vorbereitung auf die Gefahrenabwehr

Hauptziel der Behörde ist hierbei, sich für die Abwehr einer künftigen konkreten Gefahr zu rüsten. Hierzu zählt zum einen die Gefahrenverdachtssuche. Im Vorfeld des klassischen Gefahrenabwehrbegriffs wird dadurch ermöglicht, eine Gefahrensituation überhaupt wahrzunehmen.

¹⁷⁷ Knemeyer, Polizei- und Ordnungsrecht, Rn. 14

¹⁷⁸ Kniesel / Vahle, Zur Novellierung des nordrhein-westfälischen Polizeirechts, DÖV 1990, S. 646 ff. (648)

¹⁷⁹ Bäumlner, Öffentliche Sicherheit und Datenschutz,

<<http://www.datenschutzzentrum.de/material/themen/divers/lverwg30.htm>>

Sobald sich die Tatsachen zu einem Gefahrenverdacht verdichten, geht das polizeiliche Handeln dann über in den klassischen Gefahrerforschungseingriff.

Zur Gefahrenabwehrvorsorge ist auch eine klassische Streifenfahrt zu zählen, wenn deren Ziel neben der Verdachtsgewinnung auch ist, handlungsfähig und schneller am Ort der Gefahr zu sein¹⁸⁰. Fraglich ist, ob dies auch für die virtuelle Streifenfahrt bejaht werden kann.

Zwar ist – anders als für Rundfunk und Mediendienste – für Teledienste und sonstige Kommunikation keine besondere Aufsicht vorgesehen¹⁸¹. Die allgemeinen Sicherheitsbehörden sind zuständig, im unaufschiebbaren Fall auch die Polizei. Die hier dargestellten Ermittlungsmaßnahmen dienen aber nicht im Schwerpunkt dazu, Beseitigungen anzuordnen oder behördlich Sperrungen vorzunehmen, um Störungen der öffentlichen Sicherheit zu begegnen. Im Gegenteil wird bisweilen zum Zweck der Verdachtsverdichtung abgewartet oder werden einschlägig bekannte Foren wieder aufgesucht, um neue Ermittlungserfolge zu erzielen. Der virtuellen Streife kommt somit keine Funktion der Gefahrenabwehrvorsorge zu.

b) „Vorbeugende Bekämpfung von Straftaten“

Der Vorläufer dieses Begriffs, die „Vorbeugende Verbrechensbekämpfung“, wird historisch auf Erlasse des Reichssicherheitshauptamtes von 1938 zurückgeführt und war damals bereits umstritten¹⁸².

Als erstes Gesetz nahm das BKAG a.F. 1951 jenen Begriff auf, indem es klarstellte, die „vorbeugende Verbrechensbekämpfung“ und die Verfolgung von Straftaten „bleiben“ Sache der Länder. Da die Polizeigesetze der Länder jedoch erst später in Kraft traten und ein Bundesgesetz auch die Aufgabenbereiche der Landespolizeien nicht erweitern kann, kann sich dieser Verweis nur auf das zu jenem Zeitpunkt gängige Polizeiverständnis, mithin den klassischen Begriff der Gefahrenabwehr, bezogen haben¹⁸³. Der Begriff der

¹⁸⁰ Zimmermann, Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, S. 3145 ff. (3147)

¹⁸¹ Germann, Gefahrenabwehr und Strafverfolgung im Internet, S. 359

¹⁸² Merten / Merten, Vorbeugende Verbrechensbekämpfung, ZRP 1991, S. 213 ff. (218)

¹⁸³ Rachor, Vorbeugende Straftatenbekämpfung und Kriminalakten, S. 11

„vorbeugenden Bekämpfung von Straftaten“ tauchte dann erstmals im Musterentwurf von 1977 auf, in welchem § 10 I Nr. 2 die erkennungsdienstliche Behandlung auch zu diesem Zweck zuläßt. Die problematische Ausdehnung polizeilicher Vorfeldtätigkeit zog jedoch erst der Vorentwurf zum Musterentwurf 1986 nach sich.

aa) Verhütung von Straftaten

(1) Prävention durch Repression ?

Welche Art von Präventivwirkung diesem Bereich zugehörig ist, wird unterschiedlich aufgefaßt.

Einer Ansicht nach unterfällt die von den Ermittlern angestrebte Steigerung des Entdeckungsrisikos schon gar nicht dem Feld der Gefahrenvorbeugung. Hinsichtlich Streifenfahrten sei vielmehr zu differenzieren:

Die *sichtbare* Präsenz von Polizeikräften, die abschreckt und verhindert, daß eine bereits geplante und konkret bevorstehende Straftat gerade zu diesem Zeitpunkt realisiert wird, soll diesem präventiv-polizeilichen Bereich unterfallen.

Die Internetstreife hingegen agiert bewußt ohne Offenlegung ihrer Ermittlereigenschaft, ist damit der unsichtbaren Präsenz von Polizeikräften in Form der Zivilstreife vergleichbar. Gerade aber solche Verschleierung der Ermittlereigenschaft spreche schon gegen eine auf Verhinderung zielende Maßnahme¹⁸⁴.

Wird aufgrund von befürchteter, aber unsichtbarer Polizeipräsenz schon gar keine Straftat geplant, weil gleichsam die Kosten-Nutzen-Analyse dagegen spricht, so sei dies als eine notwendige Begleiterscheinung noch der Strafdrohung selbst zuzuordnen¹⁸⁵. „Prävention durch Repression“ in der

¹⁸⁴ Hund, Polizeiliches Effektivitätsdenken contra Rechtsstaat, ZRP 1991, S. 463 ff (466)

¹⁸⁵ Schwan, Die Abgrenzung des Anwendungsbereiches der Regeln des Straf- und Ordnungswidrigkeitenverfolgungsrechtes, VerwArch 1979, S. 109 ff. (126)

Ausprägung negativer Generalprävention unterfällt nach dieser Ansicht nicht dem polizeirechtlichen Präventionsbegriff¹⁸⁶.

Einem sehr umfassenderen Verständnis gemäß unterfallen jedoch auch verdeckte Maßnahmen, etwa Kontrollen der Geschwindigkeit im Straßenverkehr, diesem präventiv-polizeilichen Bereich¹⁸⁷:

So wird etwa zu der verdeckten Geschwindigkeitskontrolle vorgetragen, die *jederzeitige Möglichkeit* solch verdeckter Kontrollen und etwaiger Sanktionen solle Kraftfahrer anhalten, sich nicht nur an ihnen bekannten Kontrollpunkten, sondern *überall und jederzeit* an die vorgeschriebenen Begrenzungen zu halten. Dies gleicht der angestrebten panoptischen Wirkung der Internetüberwachung im Konzept deutlich.

(2) Präventivwirkung der Internetstreife

Selbst der zuletzt dargestellten Ansicht folgend wäre jedoch fraglich, ob eine solche Präventivwirkung der Internetstreife überhaupt beigemessen werden kann.

Kriminologisch läßt sich dies auf den ersten Blick mit der Erkenntnis stützen, daß der Verfolgungsintensität eine größere Präventivkraft zukommt als der Höhe des Strafmaßes. In der Terminologie des rational-choice-Ansatzes ausgedrückt stellt ein kalkuliert vorgehender Täter in seine Kosten-Nutzen-Analyse das Entdeckungsrisiko als „Kosten“-Faktor ein¹⁸⁸.

Hält ihn das Entdeckungsrisiko dagegen nicht ab, so vermag dies auch eine hohe Strafandrohung nicht. Denn er geht dann davon aus, ohnehin nicht gefaßt zu werden. Vor diesem Hintergrund könnte also der Internetermittlung tatsächlich entscheidende Bedeutung zukommen.

¹⁸⁶ Roggan, Über das Verschwimmen von Grenzen zwischen Polizei- und Strafprozeßrecht, <<http://www.jura.uni-bremen.de/grenzen.pdf>>;

Germann, Gefahrenabwehr und Strafverfolgung, S. 247, dort insb. Fußnote 552 a.E.

¹⁸⁷ OVG Münster, NJW 1997, S. 1596 f. (1596)

¹⁸⁸ Bock, Kriminologie, Rz. 187

So ist auch Berichten aus der Hacker-Szene zu entnehmen, daß in der Tat ein Klima der Furcht bis hin zur Paranoia besteht¹⁸⁹. Trotz der sehr geringen Personalstärke der Internet-Ermittler und entsprechend eingeschränkter Verfolgungsintensität wird die Polizeipräsenz also von den Hackern berücksichtigt.

Erneut erinnert dies sehr stark an Benthams Panopticon-Konzept: Die Wirkung einer nicht sichtbaren Überwachung ist permanent, auch wenn ihre Durchführung nur sporadisch ist.¹⁹⁰ Die Struktur des Internets scheint hervorragend geeignet, dieses Konzept der entpersonalisierten „Überwachung durch Architektur“ zu verwirklichen. Gerade auf die Effizienz zielte Bentham, der Begründer des Utilitarismus, bei seinem Entwurf ab. Bezeichnenderweise stehen die ökonomischen Kriminalitätstheorien geistesgeschichtlich auch genau in dieser Tradition von Benthams Utilitarismus¹⁹¹.

Jedoch muß man über diese allgemeinen Plausibilitätserwägungen hinausgehen, um die Präventivkraft der *konkreten* Maßnahme zu beurteilen. Fraglich ist daher, ob die anlaßunabhängige Ermittlung zur Verhinderung von Straftaten beiträgt, sie neben der allgemeinen Verunsicherung also tatsächlich ein Unterlassen von kriminellem Verhalten bewirkt.

Ein für diese Überlegung interessantes Phänomen beobachten die Ermittler derzeit online: Es erfolgt eine Verlagerung des Fall-Aufkommens vom IRC ins Usenet, obwohl zur Versendung inkriminierter Inhalte die dortige nicht-synchrone Kommunikation aufgrund der Speicherung der Nachricht eher nachteilig ist.

In Hackerkreisen wird das Usenet überdies als „langsam und unzuverlässig“ betrachtet, wogegen im IRC das „Handelszentrum... – Fusion aus Vollzeit-Devisenbörse und Straßenmarkt“¹⁹² verortet wird.

¹⁸⁹ McCandless, Warez World, in: Medosch/Röttgers (Hrsg.), Netz-Piraten, S. 35 ff. (42)

¹⁹⁰ Nogala, Der Frosch im heißen Wasser, in Schulzki-Haddouti (Hrsg.), Das Ende der Anonymität, S. 149 ff. (153); Foucault, Überwachen und Strafen, S. 258

¹⁹¹ Göppinger, Kriminologie, S. 144

¹⁹² McCandless, Warez World, in: Medosch/Röttgers (Hrsg.), Netz-Piraten, S. 35 ff. (40)

Eine plausible Erklärung für die Verlagerung des virtuellen Tatorts läßt sich aber aus den jeweils erzeugten Datenschatten erschließen:

Im IRC-Header wird die IP-Adresse angegeben. Zwar ist auch diese z.B. durch sog. IP-Spoofing manipulierbar. Jedoch erfordert dies technisches Hintergrundwissen und ist noch erschwert bei der Vergabe von dynamischen IP-Adressen.

Der Datenschatten im Usenet weist die IP-Adresse dagegen im Regelfall nicht aus. Der Ursprung eines Usenet-Postings läßt sich durch Einsatz von gängigen „remailern“ wesentlich einfacher verfremden. Die Identitätsbestimmung hängt dann davon ab, wie aussagekräftig die Logfiles der Server und Provider sind und gestaltet sich dementsprechend wesentlich schwieriger.

Somit läßt die Schwerpunktverlagerung einen vorsichtigen Schluß zu auf ein aus der offline-Welt bekanntes Phänomen: Im Zusammenhang mit einer Verstärkung normaler Streifenfahrten haben Untersuchungen ergeben, daß die Präventivwirkung des gesteigerten Entdeckungsrisikos deutliche Grenzen hat, solange sich die Kriminalität auf weniger kontrollierbare oder seltener kontrollierte Orte **verlagern** kann¹⁹³.

Dieser Vorwurf eines nur „segmentarisch erfolgreichen Ordnungskonzepts“¹⁹⁴ ist gegen die eine verstärkte Polizeipräsenz behandelnde *Broken-Windows-Theorie von Wilson und Kelling* erhoben worden: Dieser amerikanische Ansatz setzte der bisherigen kriminologischen Forschung insbesondere die These entgegen, eine erfolgreiche Kriminalitätsbekämpfung sei u.a. durch polizeiliche Maßnahmen realisierbar, ohne grundlegend die Kriminalitätsentstehungsbedingungen zu ändern.

Jedoch können die Erkenntnisse dieser umstrittenen Theorie wegen grundlegender Unterschiede in der Streifen-Praxis nicht umfassend

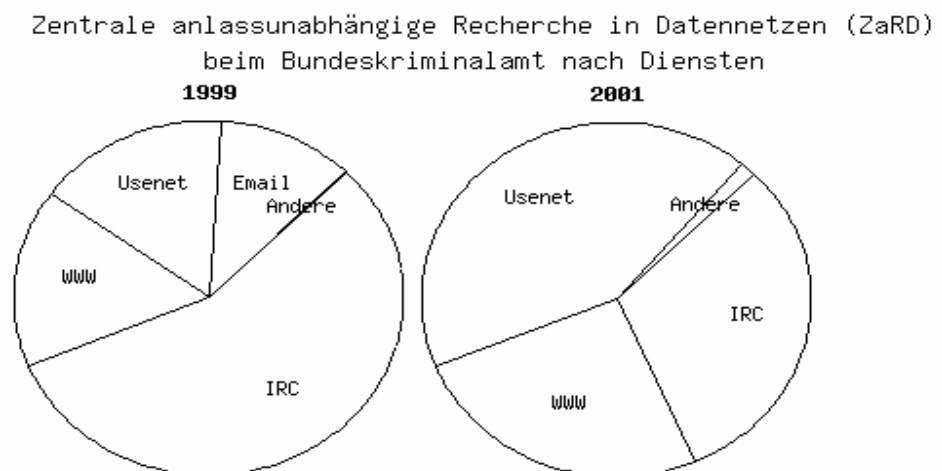
¹⁹³ Floerecke, Kriminalprävention durch Polizei?, KrimJournal 1983, S. 167 ff. (179)

¹⁹⁴ Legge, New York - weder Modell noch Fortschritt ? in: Feltes (Hrsg.), Das Modell New York: Kriminalprävention durch Zero Tolerance, zum download: <http://www.felix-verlag.de/download/Band_12.doc>, S. 116 ff. (133)

argumentativ herangezogen werden. Das Konzept verfolgte eine Verstärkung der sozialen Kontrolle mit dem sog. „community policing“: eine verstärkt offen und uniformiert präsente, sehr bürgernahe Polizeiarbeit¹⁹⁵. Einzelne Beamte agierten als feste Vertrauensperson eines bestimmten Viertels, auch um ein verstärktes Sicherheitsgefühl der Bevölkerung zu erreichen. Das Broken-Windows-Konzept ist mithin kein funktionales Äquivalent zur rein panoptisch-abschreckend operierenden Internetstreife.

Die Möglichkeit des Ausweichens in weniger kontrollierbare Bereiche besteht jedoch gegenüber offenen und nicht sichtbaren Maßnahmen gleichermaßen¹⁹⁶. Diese kritischen Beobachtungen zum Broken-Windows-Ansatz sind damit auf die Internetstreife übertragbar:

Eine solche Verdrängung und Verlagerung der Kriminalität ist aufgrund der vorliegenden Fallzahlen nun auch im Internet denkbar. Die Kriminalitätsrate scheint demnach durch verstärkte (und medienwirksam publik gemachte¹⁹⁷) Streifengänge weder online noch offline nachhaltig beeinflusst zu werden. Zwar besteht auch im Internet keine beliebige Mobilität: Der beobachteten Deliktsverschiebung ins Usenet folgte naturgemäß ein verstärkter Einsatz in eben diesem Internetbereich:



Grafik: <http://md.hudora.de/jura/ZaRD/>

¹⁹⁵ Wilson / Kelling, The police and neighborhood safety: Broken windows, in: Feltes (Hrsg.), Das Modell New York: Kriminalprävention durch Zero Tolerance, zum download: <http://www.felix-verlag.de/download/Band_12.doc>, S. 50 ff.

¹⁹⁶ WeBlau, Vorfelderermittlungen, S. 102

¹⁹⁷ Floerecke, Kriminalprävention durch Polizei?, KrimJournal 1983, S. 167 ff. (177)

Möglich bleibt jedoch stets, im Internet noch stärker als in der realen Welt, der Rückzug in stark zugangsgeschützte Bereiche. Der Hintergrund der bloßen Schwerpunktsverschiebung bleibt online wie offline: Es erfolgt reine Symptomunterdrückung, keine Bekämpfung der Kriminalitätsentstehungsbedingungen.

Diese Thesen müssen angesichts des unerforschten Online-Dunkelfelds und der Möglichkeit intervenierender Variablen gewagt erscheinen. Jedoch ist nicht ersichtlich, warum die bisherigen kriminologischen Erkenntnisse hier nicht im Wesen auf die online-Welt übertragbar sein könnten. Die einzig vorliegenden Beobachtungen stützen dabei gerade die hier gezogenen Schlußfolgerungen. Zur Bestätigung einer präventiven Wirkung der Streifenfahrt sind dagegen bisher nur Alltagstheorien vorgebracht worden¹⁹⁸, die ohne Argumentation schlicht als „unumstritten“ und „ohne Zweifel“¹⁹⁹ gültig dargestellt werden.

Selbst wenn also mit der zweiten Auffassung (S. 61) auch die nicht sichtbaren Maßnahmen dem präventiv-polizeilichen Begriff zugeordnet werden²⁰⁰, kann die Annahme einer Präventivwirkung der Streife daher nicht überzeugen. Der Teilbereich „Verhinderung von Straftaten“ ist damit für die Internetstreife keine einschlägige Aufgabenzuweisungsnorm.

bb) Strafverfolgungsvorsorge

In diesem 3. Bereich spielt sich die Reaktion auf die „veränderte Verbrechenswirklichkeit“ hauptsächlich ab. Hauptargument für die Ausweitung der polizeilichen Ermittlungstätigkeit ins Vorfeld war dabei die besondere Gefährlichkeit der Organisierten Kriminalität²⁰¹. Die undurchschaubaren Strukturen in diesem Deliktsbereich seien nur im Wege eines proaktiven Vorgehens zu durchdringen.

In den gemeinsamen Richtlinien der Justiz- und Innenminister zur Organisierten Kriminalität finden sich dazu niedergelegte Kriterien. Jedoch

¹⁹⁸ Floerecke, Kriminalprävention durch Polizei?, KrimJournal 1983, S. 167 ff. (170)

¹⁹⁹ Fiehl, Erfahrungen bei der Recherche in den Datennetzen, der kriminalist 1999, S. 2 ff. (4)

²⁰⁰ OVG Münster, NJW 1997, S. 1596 f. (1596)

²⁰¹ Denninger, in: Lisken / Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. E. Rn. 192

sind diese im Falle der allgemeinen Internet-Kriminalität nicht einschlägig: Ein außergewöhnliches Gewinn- und Machtstreben oder eine Einflußnahme auf Politik und Medien kann z.B. im Rahmen der Verbreitungsdelikte nicht ausgemacht werden. „Bezahlt“ wird hier meist nur mit ebenfalls einschlägigem Dateimaterial, im Tauschverfahren²⁰².

Neben der organisierten Kriminalität gilt das Interesse der Vorfeldermittlung seit ihrem Beginn jedoch auch den Deliktsbereichen, die schwer aufklärbar sind, weil ein typisches Instrument sozialer Kontrolle versagt²⁰³: Bisher gelangen die polizeilich registrierten Straftaten zu 90 – 95 % durch die **Anzeige** der Opfer oder Zeugen zur Kenntnis der Polizei²⁰⁴. Das Anzeigeverhalten ist somit bislang die wichtigste Determinante der polizeilich registrierten Kriminalität.

Problematisch sind daher insbesondere die sog. opferlosen Delikte²⁰⁵. Auch erfolgt keine Anzeige, wenn der Geschädigte an der Aufklärung nicht interessiert ist, weil er sich dabei auch selbst belasten würde.

Der Bereich der Internet-Kriminalität geriet als ein solches „Kontrolldelikt“²⁰⁶ in das Interessengebiet der Ermittler, weil ein Großteil der Straftaten zumeist von Usern außerhalb der jeweiligen Szene nicht wahrgenommen wird. Auch die Opfer wissen ihrerseits häufig nicht um die Verbreitungswege des Materials. Ferner ist problematisch, daß private Nutzer sich in Erklärungsnot angesichts der Entdeckung inkriminierter Dateien sehen, sowie bei einer „Beweissicherung“ für die Anzeigenerstattung tatsächlich in eine rechtliche Grauzone geraten²⁰⁷.

Auch wird vermutet, daß größere Unternehmen, wenn sie Opfer von Vermögensdelikten im Internet werden, durch die Offenbarung von

²⁰² McCandless, Warez World, in: Medosch / Röttgers (Hrsg.): Netz-Piraten, S. 35 ff. (41)

²⁰³ Wiedemann, Tatwerkzeug Internet, Kriminalistik 2000, S. 229 ff. (235)

²⁰⁴ Bock, Kriminologie, Rn. 297

²⁰⁵ Göppinger, Kriminologie, S. 484

²⁰⁶ Periodischer Sicherheitsbericht, 2.7. Internet-Kriminalität, S. 197,

<http://www.bmi.bund.de/dokumente/Artikel/ix_49371.htm?nodeID=>

²⁰⁷ Graf, Befugnisse und Grenzen der Ermittlungsbehörden, DPoIBl 4/2001, S. 6 ff. (7)

Sicherheitsdefiziten einen Kundenverlust und Trittbrettfahrer befürchten und deshalb die Tat ohne Anzeigenerhebung hinnehmen²⁰⁸.

Mittlerweile steht nach alledem im Zentrum der Strafverfolgungsvorsorge nicht mehr nur die Verwertung von Informationen aus den Kriminalakten abgeschlossener Strafverfahren. Es geht auch nicht allein um den Bereich des „Vorfelds *künftiger* Straftaten“. Vielmehr erfolgt unter dem Etikett der vorbeugenden Straftatenbekämpfung seit jeher auch eine Verdachtssuche hinsichtlich **bereits begangener** Delikte, die der Polizei nur noch nicht bekannt sind²⁰⁹. Es geht somit wesentlich um das Vorfeld des Anfangsverdachts²¹⁰.

Die Strafverfolgungsvorsorge läßt sich danach in drei Bereiche unterteilen: Verdachtsgewinnung - Verdachtssteuerung - Verdachtsverdichtung²¹¹.

Von Interesse ist vorliegend die Maßnahme der Verdachtsgewinnung. Die Polizei erkennt erst aufgrund ihrer Streifenförmigkeit „im Nebel des Vorfelds“²¹², daß eine Straftat begangen wurde. Der so gewonnene Tatverdacht wird zur förmlichen Einleitung eines strafrechtlichen Ermittlungsverfahrens genutzt und eröffnet den zuständigen Behörden ab dann den Anwendungsbereich strafprozessualer Maßnahmen.

Somit fügt sich die anlaßunabhängige Ermittlung zwar in den Bereich der vorbeugenden Bekämpfung von Straftaten ein. Ein Anwendungsbereich scheint gefunden. Die eingriffslose Maßnahme der Internetstreife wirkt danach zunächst rechtmäßig.

4) Rechtmäßigkeit der Erweiterung des Gefahrenabwehrbegriffs

Zu prüfen ist jedoch, ob diese Einordnung nicht Teil eines um sich greifenden

²⁰⁸ Weichert, Cyber-Crime-Bekämpfung und Datenschutz, DaNa 2001, S. 5 ff. (6)

²⁰⁹ Schoreit, Gefahrenabwehr – vorbeugende Verbrechensbekämpfung – Legalitätsprinzip, DRiZ 1991, S. 320 ff. (324)

²¹⁰ Germann, Gefahrenabwehr und Strafverfolgung, S. 255

²¹¹ Rachor, in: Lisken / Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. F, Rn. 182

²¹² Lisken, in: Lisken / Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. C, Rn. 82

„Etikettenschwindels“²¹³ ist.

a) Wortlaut von Musterentwurf und Landespolizeigesetzen

Der Musterentwurf sieht die Erweiterung des polizeilichen Aufgabenbereichs nur klarstellend „im Rahmen dieser Aufgabe“, der Gefahrenabwehr, vor. Tatsächlich aber wird der Polizei damit ein Bereich zugewiesen, der unter den bisherigen Aufgabenbereich klassischer Gefahrenabwehr in keiner Weise zu subsumieren ist.

Die Länder orientierten sich vielfach an der Formulierung des Musterentwurfs, so wurde etwa § 1 I NGefAG wie folgt ausgeführt: „Die Polizei hat im Rahmen ihrer Aufgabe nach Satz 1 insbesondere auch für die Verfolgung von Straftaten vorzusorgen und Straftaten zu verhüten.“

Eine konstitutive Erweiterung durch einen neuen, selbständigen Aufgabenbereich kann jedoch nicht im Wege einer bloßen Klarstellung „im Rahmen“ des klassischen Gefahrenabwehrbegriffs vollzogen werden.

Selbst der Teilbereich der Gefahrenabwehrvorsorge, der aufgrund seiner Nähe zur herkömmlichen Polizeiarbeit weniger als Fremdkörper erscheint, geht über den bisherigen Aufgabenbereich hinaus: Denn auch Gefahrerforschungsmaßnahmen sind nach dem klassischen Gefahrenabwehrverständnis erst ab dem Stadium des Gefahrenverdachts zulässig.²¹⁴ Auch dieser Tätigkeitsbereich wurde also fälschlich „im Rahmen“ der klassischen Gefahrenabwehr verortet.

Gerade im vorliegend herangezogenen Gebiet der Strafverfolgungsvorsorge, der Verdachtsgewinnung, ist keinerlei Gefahrenabwehr zu erkennen: So wird etwa bei der Internetstreife lediglich eine bereits begangene Straftat entdeckt. Die Polizei agiert im Vorfeld traditioneller Strafverfolgung²¹⁵. Es handelt sich bei der Strafverfolgungsvorsorge also um antizipierte Strafverfolgung²¹⁶.

²¹³ Rachor, Vorbeugende Straftatenbekämpfung und Kriminalakten, S. 9

²¹⁴ Gusy, Polizeirecht, Rn. 186

²¹⁵ Gusy, Polizeirecht, Rn. 187

²¹⁶ Merten, Zulässigkeit der langfristigen Video-Überwachung, NJW 1992, S. 354 ff. (355)

Etwas anderes könnte sich aus den Befugnisnormen in den Polizeigesetzen ergeben: Der Schluß von der Befugnis- auf die Aufgabennorm wird - anders als sein Umkehrschluß - verfassungsrechtlich für zulässig gehalten²¹⁷. Zwar ist auch dies angesichts der Bedeutung von Aufgabenzuweisungsnormen bedenklich²¹⁸.

Im Falle des maßgeblichen bayerischen Polizeirecht erscheint dieses Vorgehen aber zumindest zur Auslegung nötig, da die Aufgabenzuweisungsnorm im Anschluß an den veränderten Musterentwurf nicht einmal ergänzt wurde: Art. 31 I 1 BayPAG, der allgemeinen Befugnis zur Datenerhebung, läßt sich jedoch entnehmen, daß die Neuregelung der Aufgabenzuweisungsnorm nur unterblieb, weil wie selbstverständlich die vorbeugende Bekämpfung von Straftaten miteinbezogen wird: So zählt gemäß dieser Norm zum Bereich der Gefahrenabwehr „**insbesondere**“ die vorbeugende Bekämpfung von Straftaten.

Aus den dargestellten Gründen ist dies unzureichend. Für die rein repressive Verdachtsgewinnung durch die bayerische Internetstreife besteht somit schon nach dem einfachen Recht keine ausreichende Aufgabenzuweisungsnorm²¹⁹.

b) Gesetzgebungskompetenz der Länder

Angezweifelt wird jedoch nicht nur die soeben aufgezeigte Regelungslücke im einfachen Recht, sondern die Gesetzgebungskompetenz der Länder insgesamt:

aa) Art. 70, 72, 74 I Nr. 1 GG

Die Aufgabenteilung von Repression und Prävention muß sich an den **verfassungsrechtlichen Vorgaben** zur Gesetzgebungskompetenz von Bund und Ländern orientieren. Allerdings beziehen sich die Art. 70 ff. GG nicht explizit auf Prävention und Repression, weshalb die Einordnung der Vorfeldermittlung umstritten ist:

²¹⁷ Soiné, Datenverarbeitung für Zwecke künftiger Strafverfahren, CR 1998, S. 257 ff. (261)

²¹⁸ Weßlau, Vorfeldermittlungen, S. 143

²¹⁹ Germann, Gefahrenabwehr und Strafverfolgung, S. 260

Nach Art. 70, 72, 74 I Nr. 1 GG besteht eine Bundesgesetzgebungskompetenz für das „Strafrecht“ und das „gerichtliche Verfahren“. Eine Ansicht ordnet die vorbeugende Verbrechensbekämpfung hierbei dem „Strafrecht“ zu²²⁰. Der Begriff des Strafrechts bezieht sich jedoch auf das materielle Recht, wie sich systematisch schon aus der gesonderten Nennung der Strafvollstreckung ergibt.²²¹ Das Strafverfahren und als Teil dessen auch das Ermittlungsverfahren unterfallen dem Bereich „gerichtliches Verfahren“²²².

Eine Ansicht folgt in der Festlegung des Beginns des Ermittlungsverfahrens im Sinne des Art. 74 Nr. 1 GG dem einfachen Recht, der Regelung in der StPO: Schon insoweit sei die Einordnung des Vorverfahrens unter das „gerichtliche Verfahren“ des Art. 74 Nr. 1 GG zweifelhaft²²³. Allenfalls dieses unmittelbare Vorfeld eines konkreten Gerichtsverfahrens, *nicht* aber der hier relevante Bereich im Vorfeld des Verdachts, sei somit von der Bundeskompetenz in Art. 74 Nr. 1 GG umfaßt. Im Gegenteil werde das System der StPO „gesprengt“²²⁴, würde die Vorfeldermittlung dort geregelt. Der Bund habe gar keine Gesetzgebungskompetenz über den Anfangsverdacht der StPO hinaus.

Dem ist mit der anderen Auffassung entgegenzuhalten, daß das Ziel von Strafverfolgungsvorsorge die Einleitung eines strafrechtlichen Ermittlungsverfahrens ist²²⁵. Die Tätigkeit dient somit allein der Durchsetzung des strafrechtlichen Vollstreckungsanspruchs. Warum gerade die Entscheidung des einfachen Gesetzgebers auch für die Reichweite des verfassungsrechtlichen Begriffs in Art. 74 I Nr. 1 GG maßgeblich sein soll, ist nicht ersichtlich²²⁶. Es ist somit davon auszugehen, daß unter den Begriff des „gerichtlichen Verfahrens“ auch die vorbeugende Bekämpfung von Straftaten fällt, durch die der Strafanspruch des Staates verwirklicht werden soll²²⁷.

²²⁰ Merten / Merten, Vorbeugende Verbrechensbekämpfung, ZRP 1991, S. 213 ff. (218)

²²¹ Siebrecht, Die polizeiliche Datenverarbeitung im Kompetenzstreit zwischen Polizei- und Prozeßrecht, JZ 1996, S. 711 ff. (713)

²²² Kunig in von Münch / Kunig, GG II, Art. 74, Rn. 12

²²³ Deutsch, Die heimliche Erhebung von Informationen, S. 186

²²⁴ Kniesel, Neue Polizeigesetze contra StPO, ZRP 1987, S. 377 ff. (380)

²²⁵ Rachor, in: Lisken / Denninger, Handbuch des Polizeirechts, Kap.F, Rn. 170

²²⁶ Germann, Gefahrenabwehr und Strafverfolgung im Internet, S. 257

²²⁷ Soiné, Datenverarbeitung für Zwecke künftiger Strafverfahren, CR 1998, S. 257 ff. (260)

bb) Problematik der konkurrierenden Gesetzgebung

Zu beachten ist jedoch im weiteren, daß Art. 74 GG die konkurrierende Gesetzgebung betrifft. Die oben eingewandte Argumentation gestützt auf das einfache Recht könnte eher hier zum Tragen kommen: Die fehlende Regelung in der StPO zur Strafverfolgungsvorsorge kann auf zwei Arten interpretiert werden.

Einer Auffassung nach wollte der Bund nur die Strafverfolgung, nicht aber die Strafverfolgungsvorsorge in der StPO regeln. Das dem Anfangsverdacht vorausgehende Vorfeld solle danach einer Regelung durch die Länder offenstehen²²⁸. Landesgesetze sollen danach materielles Strafprozeßrecht beinhalten können²²⁹.

Die Gegenauffassung hält die Regelung des repressiven Bereichs in der StPO für abschließend²³⁰. Die vorbeugende Verbrechensbekämpfung werde durch das Recht der Strafverfolgung „konsumiert, aufgesogen, verbraucht“²³¹.

(1) Anhaltspunkte in der StPO

Als Argument werden Regelungen innerhalb der StPO herangezogen: Insbesondere § 81 b Alt. 2 StPO führte bereits in der Vergangenheit zu Diskussionen über die Gesetzgebungskompetenz in der Grauzone. Die Norm wird als materielles Polizeirecht verstanden. Entsprechend sei auch der Verwaltungsrechtsweg einzuschlagen²³². Die Gesetzgebungskompetenz des Bundes ergebe sich aber aus dem *engen Sachzusammenhang*²³³.

Eindeutig ergibt sich ein vorbeugender Charakter ferner aus § 112 a StPO, der vorbeugenden Maßnahme der Sicherungshaft, und 126 a StPO, der einstweiligen Unterbringung. Auch für diese Präventivregelungen wird die

²²⁸ Rachor in Liskén / Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. F, Rn. 367

²²⁹ OVG Schleswig, NJW 1999, S. 1418 ff. (1418)

²³⁰ Lindig, Die neuen „ereignis- und verdachtsunabhängigen“ Befugnisse im Polizeirecht, (1 b) dd) (2)), <<http://www.jurawelt.com/aufsaeetze/oer/3573?stylelite=1>>

²³¹ Schwan, Die Abgrenzung des Anwendungsbereiches der Regeln des Straf- und Ordnungswidrigkeitenverfolgungsrechtes, VerwArch 1979, S. 109 ff. (123)

²³² BVerwG NJW 1983, S. 772 f. (772)

²³³ Merten / Merten, Vorbeugende Verbrechensbekämpfung, ZRP 1991, 213 ff. (219); BVerwG NJW 1983, S. 772 f. (773)

StPO als richtiger Standort gesehen wegen des engen Sachzusammenhangs zum Strafverfahren.

Somit sei in der StPO die vorbeugende Bekämpfung von Straftaten damit bereits geregelt, was für den abschließenden Charakter der StPO spreche.

Da diese Regelungen aber gerade selbst wegen ihres Präventionscharakters hinsichtlich der Gesetzgebungskompetenz umstritten sind, scheinen sie hier als tragfähige Argumentationsgrundlage nicht ausreichend. Ferner wird zu § 81 b StPO eingewandt, dieser regle zwar als konkurrierendes Bundesrecht den betreffenden Bereich abschließend. Er beziehe sich jedoch nur auf den „Beschuldigten“ im Sinne der StPO²³⁴.

In die Argumentation zum abschließenden Charakter wurde auch bereits § 484 StPO einbezogen, als diese Norm erst im Entwurfsstadium vorlag.²³⁵ Auch in dieser Regelung wurde der Wille des Bundesgesetzgebers entdeckt, seine Kompetenz im Bereich der Strafverfolgungsvorsorge in Anspruch zu nehmen. Diese Vorschrift zur Datenverarbeitung für Zwecke künftiger Strafverfahren wurde mittlerweile eingefügt durch das Strafverfahrensänderungsgesetz 1999 (StVÄG 1999) vom 2.8.2000.

Die Bundesregierung entgegnete einer vom Bundesrat zu § 484 IV StPO begehrten Klarstellung zum Entwurf des StVÄG 1999:

„Die Speicherung personenbezogener Daten für Zwecke des Polizeirechts ist weder Regelungsgegenstand des Gesetzentwurfs insgesamt noch des § 484 StPO im Besonderen. § 484 StPO enthält - nur - Dateiregelungen für Zwecke künftiger Strafverfahren.“²³⁶

Diese Aussage läßt die Lesart zu, daß Zwecke künftiger Strafverfahren keine Zwecke des Polizeirechts sind. Dies wäre in der Tat ein Argument für den abschließenden Regelungsstandort der StPO.

²³⁴ OVG Schleswig, NJW 1999, S. 1418 ff. (1418)

²³⁵ Merten / Merten, Vorbeugende Verbrechensbekämpfung, ZRP 1991, S. 213 ff. (219)

²³⁶ <<http://www.datenschutz-berlin.de/jahresbe/99/doc/90.htm>>

§ 484 IV StPO selbst läßt jedoch in seinem Wortlaut jede Normenklarheit vermissen. Diese Norm könnte auch für den Regelungsstandort des Polizeirechts sprechen²³⁷, weshalb sie nicht entscheidend zur Klärung der vorliegenden Frage beizutragen vermag.

(2) Konsequenzen einer Regelung im Polizeirecht

Deutlich für eine als abschließend gewollte Regelung durch den Bundesgesetzgeber sprechen aber die Konsequenzen einer Umgehung des Anfangsverdachts, die auch bei der Internetstreife zu beobachten sind:

(a) Verlust der Sachleitungsbefugnis der Staatsanwaltschaft

Herrin des Ermittlungsverfahrens ist die Staatsanwaltschaft. Ihr wird die **Sachleitungsbefugnis über das Verfahren** bereits im Vorfeld entzogen. Damit entfällt eine Instanz verfahrensrechtlicher Sicherungen, welche das Volkszählungsurteil gerade eingefordert hat²³⁸.

In Anbetracht der Charakterisierung der Internetkriminalität als „Kontrolldelikte“ wird dies besonders deutlich: Abgesehen von Zufallstreffern wird im Internet von den Ermittlern nur gefunden, wonach auch gesucht wird. Die Entscheidung darüber, was Gegenstand eines Ermittlungsverfahrens ist, fällt somit nicht die Staatsanwaltschaft. Vielmehr obliegt dies bereits im Vorfeld der Selektionsmacht der Ermittler, die darüber befinden können, welche Teile des Dunkelfelds sie erhellen²³⁹. Wie gezeigt wird zumindest in Bayern bewußt mit dem Schwerpunkt „Kinderpornographie“ ermittelt. Andere Deliktsbereiche haben damit eine sehr geringe Entdeckungs- und naturgemäß eine ebenso geringe Aufklärungswahrscheinlichkeit.²⁴⁰

Die fehlende Einbindung der Staatsanwaltschaft ist damit auch eine Gefahr für das Legalitätsprinzip, durch das eine gleichmäßige Strafrechtspflege garantiert

²³⁷ Keller / Griesbaum, Das Phänomen der vorbeugenden Bekämpfung von Straftaten, NStZ 1990, 416 ff. (418) (zu § 484 VI StVÄG 1989)

²³⁸ Riepl, Informationelle Selbstbestimmung im Strafverfahren, S. 209

²³⁹ Hund, Polizeiliches Effektivitätsdenken contra Rechtsstaat, ZRP 1991, S. 463 ff. (464)

²⁴⁰ Keller / Griesbaum, Das Phänomen der vorbeugenden Bekämpfung von Straftaten, NStZ 1990, S. 416 ff. (420)

werden soll. Zwar wird diese Straftatenerforschungspflicht erst ab Vorliegen des Anfangsverdachts ausgelöst.²⁴¹ Nimmt man jedoch im Vorfeld Einfluß darauf, bei welchen Delikten der Anfangsverdacht gewonnen wird und bei welchen es dazu zwangsläufig nicht kommen wird, so hat dies bereits entscheidende Konsequenzen.

(b) Grenzenloses Vorfeld

Auch eine weitere Funktion des Anfangsverdachts würde unterlaufen: Der Anfangsverdacht ist nicht nur Anlaß, sondern beschränkt auch die Ermittlungen auf die Aufklärung dieses konkreten Verdachtsfalles²⁴². Jenseits des Anfangsverdachts dagegen ist ein solch bindender Zweck der Ermittlungen noch nicht vorhanden. Somit könnte jedenfalls im hier maßgeblichen eingriffslosen Bereich nach allem Ausschau gehalten werden. Der Vorfeldarbeit „fehlt die Begrenzung, welche die Strafverfolgung in dem Erfordernis des Anfangsverdachts und die Gefahrenabwehr im Erfordernis der konkreten Gefahr besitzt.“²⁴³

Im Falle der Datenerhebung begegnet dies auch vor dem Hintergrund des Zweckbindungsgrundsatzes Bedenken: Bei einer Vermischung von Repression und Prävention in einem, dem präventiv-polizeilichen, Aufgabenbereich scheinen die Daten damit noch für keinen der beiden Zwecke eindeutig festgelegt²⁴⁴.

Auch die Argumentations- und Legitimationsgrundlage „Organisierte Kriminalität“, die die Einführung des dritten Aufgabengebiets begleitete, übt hier keine limitierende Funktion aus. Vielmehr ist infolge der Neufassung des Aufgabenbereichs die Zunahme der Vorfeldermittlung für das Polizeirecht *insgesamt* in den letzten Jahren „charakteristisch und offenbar unaufhaltsam“²⁴⁵. Auch die vormals gegebenen natürlichen Grenzen der

²⁴¹ Soiné, Datenverarbeitung für Zwecke künftiger Strafverfahren, CR 1998, S. 257 ff (260)

²⁴² Weßlau, Vorfeldermittlungen, S. 293

²⁴³ Hund, Überwachungsstaat auf dem Vormarsch - Rechtsstaat auf dem Rückzug?, NJW 1992, S. 2118 ff. (2120)

²⁴⁴ Artzt, Doppelfunktionales Handeln des Polizeivollzugsdienstes, Kriminalistik 1998, S. 353 ff. (354)

²⁴⁵ Liskan/Denninger im Vorwort zur 3. Auflage des Handbuch des Polizeirechts

personellen und zeitlichen Ressourcen verschieben sich und halten die Vorfeldermittlung kaum noch auf²⁴⁶: Durch die Digitalisierung der Telekommunikationsvermittlungstechnik hat sich der Ressourcenbedarf und Kontrollaufwand im Vergleich zum Impulswählverfahren deutlich verringert.²⁴⁷ Dazu kommt nun noch der Einsatz von Ermittlungstools.

(c) Verabschiedung des Anfangsverdachts

Besonders deutlich wird der praktizierte fließende Übergang vom Polizeirecht in die StPO in einer BGH-Entscheidung zur langfristigen Video-Überwachung: Eine in Absprache mit der Staatsanwaltschaft durchgeführte Video-Überwachung wird „jedenfalls auch“²⁴⁸ auf eine polizeirechtliche Grundlage gestützt. Die Ermittlungsbehörde operierte damals ohne zureichende tatsächliche Anhaltspunkte für das Vorliegen einer Straftat, dies sogar in Abstimmung mit der Staatsanwaltschaft. Gleichwohl ging der Senat mittels der „jedenfalls auch“-Feststellung über den fehlenden Anfangsverdacht hinweg.

(d) Beschränkungen in den Befugnisnormen

Eine mögliche Abschwächung der soeben dargestellten Folgen wird zwar den Polizeigesetzen bisweilen durch Beschränkungen in den Befugnisnormen angestrebt²⁴⁹. Diese Lösung sieht der Alternativvorschlag des § 8 a II im Vorentwurf zum Musterentwurf von 1986 vor. Buchstabe a) verweist dort auf den Katalog des § 100 a StPO, und unter b) werden unter anderem auch die Ermittlungsschwerpunkte im Internet (§§ 86 a und 184 StGB) erfaßt.

Einige Landesgesetze sehen Einschränkungen auch für verdeckte Maßnahmen zur vorbeugenden Bekämpfung von Straftaten vor.

Somit würde die genannte BGH-Entscheidung zur Videoüberwachung heute wohl anders ausfallen: Zur Anwendung kam auch dort das bayerische Polizeirecht. In § 33 II BayPAG ist für die verdeckte Anfertigung von Bildaufnahmen eine konkrete Gefahr Eingriffsvoraussetzung, - anders als für

²⁴⁶ Rachor, Vorbeugende Straftatenbekämpfung und Kriminalakten, S. 12

²⁴⁷ Krader, Kampf gegen die Internetkriminalität, DuD 2001, S. 344 ff. (344)

²⁴⁸ BGH NJW 1991, S. 2651 f. (2651)

²⁴⁹ Gusy, Polizeirecht, Rn. 187

die allgemeine Befugnis zur Datenerhebung in § 31. Gleichwohl zeigt die BGH-Entscheidung die Beliebigkeit und den fließenden Übergang, mit der mit Hilfe des Polizeirechts über das Erfordernis des Anfangsverdachts hinweggesehen werden kann²⁵⁰.

Die Einschränkung im Rahmen der Befugnisnorm kann im übrigen aus mehreren Gründen nicht überzeugen: Nimmt man etwa den gewerbs- oder bandenmäßige Diebstahl als Beispiel (vgl. § 8 a II, 2. Alt ME), so kann im Vorfeld des Anfangsverdachts, wenn die Straftaten also noch gar nicht bekannt sind, diese Einschätzung gar nicht an tatsächlichen Anhaltspunkten festgemacht werden²⁵¹.

Ferner zeigt gerade die hier zu prüfende Problematik, daß diese Begrenzungen für **eingriffslose Maßnahmen** keinerlei Wirkung haben. Damit wird jedoch die wichtige Funktion einer Aufgabenzuweisungsnorm gänzlich untergraben, und die Polizei könnte in der Folge doch „wie jedermann“ agieren. Denn die Erweiterung **im Aufgabenbereich** wurde im Musterentwurf, dem die meisten Polizeigesetze gefolgt sind, ohne jede Einschränkung „klargestellt“.

5) Zusammenfassung

In der Gesamtschau wird ersichtlich, daß mit der Auffassung, die Regelung des Bundesgesetzgebers sei nicht abschließend, Folgen verbunden sind, die das ganze System der StPO unterlaufen. Derartige Konsequenzen sprechen damit klar für eine als abschließend gewollte Regelung in der StPO.

Damit ist der Bereich der Strafverfolgungsvorsorge der Ländergesetzgebungskompetenz entzogen. Das BayPAG eröffnet somit schon deshalb keinen rechtmäßigen Aufgabenbereich für die bayerische Internetstreife. Auch eine Maßnahme, die nicht in Grundrechte eingreift, braucht jedoch eine rechtmäßige gesetzliche Aufgabenzuweisung.²⁵² Nichts anderes gilt für die Maßnahmen mit Eingriffsqualität.

²⁵⁰ Merten, Zulässigkeit der langfristigen Video-Überwachung, NJW 1992, S. 354 ff. (355)

²⁵¹ Gusy, Polizeirecht, Rn. 187

²⁵² Weßlau, Vorfeldermittlungen, S. 160

Wie unter 4 a) dargestellt hängt dieses Ergebnis auch nicht von der Ablehnung der Gesetzgebungskompetenz der Länder ab. Auch die Gegenauffassung kann wegen der ungenügenden Regelung im BayPAG auf keinen Aufgabenbereich verweisen, der die rein *repressive* Verdachtsgewinnung durch die Internetstreife erfaßt²⁵³.

Die bayerische Internetstreife ist damit rechtswidrig.

IV) Aufgabenzuweisungsnorm der BKA-Streife

Zu prüfen ist für die Rechtmäßigkeit der BKA-Internetstreife, ob das BKAG eine Aufgabenzuweisungsnorm vorsieht, die den Ermittlern auch die Verdachtsgewinnung gestattet.

1) Regelung im BKAG

Das Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes nahm 1951 in § 4 I, 1973 dann in § 5 I 1 BKAG a.F. als erstes Gesetz den Begriff der „vorbeugenden Verbrechensbekämpfung“ auf:

Das BKAG von 1997 jedoch hat den Begriff aufgegeben und spricht in der Aufgabenzuweisungsnorm (§ 2 I BKAG) von der „Verhütung und Verfolgung von Straftaten“. Daß damit auch weiterhin die vorbeugende Bekämpfung von Straftaten möglich ist, ergibt sich wiederum aus einem konkretisierenden Schluß von einer Befugnisnorm auf die Aufgabennorm²⁵⁴: § 20 BKAG regelt die Datenerhebung als Vorsorge für künftige Strafverfolgung.

2) Gesetzgebungskompetenz

Die ausdrückliche Verschränkung von präventivem und repressivem Bereich im BKAG erscheint zunächst wiederum aus Gründen der Gesetzgebungskompetenz bedenklich²⁵⁵. Es besteht hier jedoch kein Anlaß, aufgrund der Länderkompetenz für Gefahrenabwehr die formelle Verfassungsmäßigkeit des § 2 BKAG in Zweifel zu ziehen. Denn die Verschränkung beider Bereiche erklärt sich durch die Eigenschaft des BKA als

²⁵³ Germann, Gefahrenabwehr und Strafverfolgung, S. 260

²⁵⁴ Soiné, Datenverarbeitung für Zwecke künftiger Strafverfahren, CR 1998, S. 257 ff. (261)

²⁵⁵ Denninger, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. E, Rn. 181

„Doppelzentralstelle“ und ist nur in den Grenzen dieser Zentralstellenfunktion zulässig:

Verfassungsrechtliche Kompetenz- und zugleich auch Legitimationsnorm für die Zentralstellenfunktion des Bundeskriminalamts ist Art. 87 I S. 2 GG. Die Verschränkung von „Verhütung und Verfolgung“ im BKAG wird dadurch möglich, daß sich in Art. 87 GG eine Kompetenznorm für beide Aufgabenbereiche findet²⁵⁶: Das dort in Abs. 1, S. 2 verwendete Adjektiv „polizeilich“ bezeichnet den präventiv-polizeilichen Bereich.

Eine Zentralstelle ist als Behördentypus eigener Art zu sehen: eine Bundesbehörde der unmittelbaren Bundesverwaltung ohne eigenen Unterbau. Die Zentralstelle soll die polizeiliche Zusammenarbeit zwischen Bund und Ländern in den in Art. 87 I S.2 GG genannten Bereichen ermöglichen. Der Bundesgesetzgeber hat das Bundeskriminalamt zu einer **Doppelzentralstelle** gemacht, als er dem BKA zwei Sachgebiete, „Kriminalpolizei“ und „polizeiliches Auskunfts- und Nachrichtenwesen“, zur Wahrnehmung zuwies. Dies erfolgte bewußt aufgrund der vielfältigen Überschneidungen, „z.B. im Bereich der vorbeugenden Bekämpfung von Straftaten“²⁵⁷. Ausschließlich vor diesem Hintergrund erklärt sich somit die Aufgabennorm in § 2 I BKAG, die zugleich Unterstützung bei „Verhütung **und** Verfolgung von Straftaten“ vorsieht.

Für die Zentralstelle ist aufgrund der Koordinationsfunktion eine Überschneidung von Aktivitäten des Bundes und der Länder geradezu wesentypisch: Keinesfalls kann aber die Zentralstelle die Materie der Prävention in vollem Umfange unter Ausschluß der Länder an sich ziehen. Somit besteht für die Zentralstelle eine Ausnahme vom grundsätzlichen Verbot der Mischverwaltung²⁵⁸.

Eine „Mischung von Bundesbehörde und Länderkompetenz“²⁵⁹ liegt also bei

²⁵⁶ Begründung zum BKAG, BT-Drucksache 13/1550, S. 19 ff. (20)

²⁵⁷ Ahlf in Ahlf / Daub / u.a., BKAG, § 2, Rn. 3

²⁵⁸ Ahlf in Ahlf / Daub / u.a., BKAG, § 2, Rn. 2

²⁵⁹ (Hamann im Interview mit) Schulzke-Haddouti, Maschinenstürmer im Bundesinnenministerium, <<http://www.heise.de/tp/deutsch/inhalt/te/1547/1.html>>

genauer Betrachtung gar nicht vor: In den engen Grenzen der koordinierenden Zentralstellen-Funktion enthält Art. 87 I 2 GG eine Gesetzgebungskompetenz des Bundes für den präventiven Bereich.

- Wie dargestellt, ist für die Internetstreife im übrigen ohnehin der repressive Bereich relevant. Für diesen besteht, wie unter D. III 4 b) gezeigt, eine Kompetenz des Bundesgesetzgebers auch im Vorfeld. -

In § 2 I i.V.m. § 2 II Nr. 1 BKAG findet sich somit eine formell verfassungsmäßige Aufgabenzuweisungsnorm für die Internetstreife. Inwieweit sich diese Aufgabenzuweisung jedoch mit dem sog. Trennungsgrundsatz vereinbaren läßt, muß nachfolgend noch geprüft werden.

V. Vorfeldtätigkeit und Trennungsgebot

Es wurde bereits daran erinnert, daß die Initiativermittlungsbefugnis des BKA, die der Entwurf zum Terrorismusbekämpfungsgesetz 2001 vorsah, höchst umstritten war. Hauptkritikpunkt war dabei die Unvereinbarkeit mit dem sog. Trennungsgebot. Dieses Gebot könnte auch der Verfassungsmäßigkeit der Aufgabenzuweisungsnorm im BKAG entgegenstehen, somit auch der Rechtmäßigkeit der BKA- Internetstreife.

Relevant ist die Frage der Vereinbarkeit von Vorfeldtätigkeit und Trennungsgebot auch für eine denkbare Regelung der Strafverfolgungsvorsorge in der StPO de lege ferenda. Denn mit der Verneinung der Ländergesetzgebungskompetenz wurde nicht zugleich gesagt, daß das Vorfeld des Anfangsverdachts der staatlichen Kontrolle gänzlich entzogen sein soll. Vielmehr folgt daraus zunächst nur, daß allein möglicher Regelungsstandort ein Bundesgesetz wäre²⁶⁰.

Ob jedoch - de lege ferenda zum Beispiel in der StPO - ein Vorgehen zur Verdachtsgewinnung zulässig wäre, müßte auch noch hinsichtlich des Trennungsgebots überprüft werden.

²⁶⁰ für die StPO als Regelungsstandort z.B. auch Merten / Merten, Vorbeugende Verbrechensbekämpfung, ZRP 1991, S. 213 ff. (219); Standort StPO sei „ehrlicher“: Rachor, in: Lisken / Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. F; Rn. 367

1) Wesen des Trennungsgebots

Die Trennung von Polizei und Verfassungsschutz begründet sich aus den Erfahrungen mit dem Terror der Gestapo, die nachrichtendienstliche *und* exekutive Befugnisse hatte und dadurch unbeschränkte Machtfülle erreichte. Zur Gefährlichkeit der Gestapo trug auch bei, daß diese weisungsbefugt gegenüber allen Polizeibehörden, der verwaltungsgerichtlichen Kontrolle entzogen und an die Gesetze nicht gebunden war.

Die Militärgouverneure der Alliierten gestatteten im April 1949 im sog. Polizeibrief deshalb zwar die Einrichtung einer Verfassungsschutzbehörde, diese dürfe aber keinerlei Polizeibefugnisse haben. Vielmehr sollte dem Nachrichtendienst **die Strukturaufklärung** mit nachrichtendienstlichen Mitteln **im Vorfeld der konkreten Gefahr und des Anfangsverdachts** vorbehalten bleiben²⁶¹. Der Oberbegriff der „nachrichtendienstlichen Mittel“ kann so zusammengefaßt werden, daß der Nachrichtendienst „*dem Bürger im Gewande des Bürgers gegenübertreten*“²⁶² darf, verdeckt, heimlich und in Verkleidung - jedoch ohne Ausübung von Zwang.

2) Trennungsgebot de lege lata

Im einfachen Recht findet sich der Grundsatz der organisatorischen Trennung in § 2 I 3 BVerfSchG. Demnach darf der Nachrichtendienst keiner polizeilichen Dienststelle angegliedert werden.

In § 8 III BVerfSchG ist die Befugnistrennung geregelt: Danach dürfen dem Nachrichtendienst keine polizeilichen Befugnisse zur Verfügung gestellt werden.

3) Verbindlichkeit des Trennungsgebots

Umstritten ist jedoch, in welchem Maße dem Trennungsgebot heute noch Verbindlichkeit zukommt. Eine einfachgesetzliche Regelung in §§ 2 und 8 BVerfSchG würde den Gesetzgeber de lege ferenda nicht davon abhalten, vom Trennungsprinzip abzurücken²⁶³.

²⁶¹ Liskén, in: Liskén/Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. C, Rn. 11

²⁶² Schlink, Das nachrichtendienstliche Mittel, NJW 1980, S. 552 ff. (554)

²⁶³ Erfurth, Verdeckte Ermittlungen, S. 43

Bestünde nur diese einfachgesetzliche Regelung, so gingen zudem davon keine Beschränkungen für die Polizei aus²⁶⁴. Ein Umkehrschluß zu § 8 III BVerfSchG wäre dann nicht zwingend.

a) Polizeibrief als Verfassungsbestandteil

Einer Auffassung zufolge ist das Trennungsprinzip ein verfassungsrechtliches Gebot: Das Genehmigungsschreiben der Militärgouverneure zum Grundgesetz vom 12.5.1949 nahm den Polizeibrief in Bezug. Damit sei das Trennungsgebot Verfassungsbestandteil geworden, woran sich auch seitdem nichts geändert habe²⁶⁵.

Bejaht man dies, so hätte dies auch Einfluß auf die Arbeit der Polizei. Denn eine politische Überwachungsbehörde könnte sich auch ergeben, wenn von Seiten der Polizei das Trennungsgebot nicht beachtet wird²⁶⁶:

Verhindert werden soll dann eine Behörde, die verfassungsfeindliche Bestrebungen im Vorfeld von konkreter Gefahr und Anfangsverdacht erforschen und zudem Gefahren abwehrt und Strafverfolgung betreiben kann.²⁶⁷

Angesichts der Tatsache, daß den zweiten Schwerpunkt der Internet-Vorfeldermittlung der Staatsschutz bildet, ist aber in der derzeitigen Praxis eine Überschneidung der Aufgabenbereiche von Polizei und Nachrichtendienst beim Staatsschutz feststellbar: Das BKA agiert bei der anlaßunabhängigen Internetstreife auch im Bereich politischer Kriminalität. Teilweise wird die Vorfeldtätigkeit durch die Polizei im Staatsschutz-Bereich als generell unzulässig erachtet²⁶⁸.

b) Trennungsgebot als Folge des Rechtsstaatsprinzips

Der historischen Herleitung aus dem Polizeibrief ist entgegenzuhalten, daß mit

²⁶⁴ Lammer, Verdeckte Ermittlungen im Strafprozeß, S. 148

²⁶⁵ Denninger, Die Trennung von Verfassungsschutz und Polizei und das Grundrecht auf informationelle Selbstbestimmung, ZRP 1981, S. 231 ff. (231); Liskén, Polizei und Verfassungsschutz, NJW 1982, S. 1481 ff. (1482)

²⁶⁶ Deutsch, Die heimliche Erhebung von Informationen, S. 30

²⁶⁷ Hund, Polizeiliches Effektivitätsdenken contra Rechtsstaat, ZRP 1991, S. 463 ff. (467)

²⁶⁸ Weßlau, Vorfeldermittlungen, S. 226

der Wiedererlangung der vollen Souveränität durch den Deutschlandvertrag von 1955 und die Drei-Mächte-Erklärung von 1968 die alliierten Vorbehaltsrechte erloschen sind²⁶⁹.

Gleichwohl ist den historischen Erfahrungen des Gestapo-Terrors weiterhin Rechnung zu tragen. Über den Bereich der politischen Kriminalität hinaus konnten Argumente gegen die Kombination von Vorfeldermittlung und Zwangsbefugnissen ohnehin nicht unmittelbar aus dem Trennungsgebot abgeleitet werden. Dennoch wurde - und wird - auch im nicht-politischen Bereich aufgrund des Rechtsstaatsprinzips die Zulässigkeit einer Geheimpolizei abgelehnt²⁷⁰.

4) Folge für die Vorfeldermittlung

Fraglich ist jedoch, ob damit jegliche Vorfeldermittlung und jeglicher Einsatz nachrichtendienstlicher Mittel durch die Polizei ausgeschlossen ist²⁷¹. Nach dieser Auffassung wäre in der Tat die anlaßunabhängige Internetstreife mit dem Trennungsgebot nicht vereinbar.

Dagegen wird zum einen vorgeschlagen, die Polizei könne mit nachrichtendienstlichen Befugnissen agieren, unter anderem verdeckt ermitteln, weil, (bzw. heute: solange) dabei der Vorfeldbereich nicht berührt sei²⁷². Auch wird vertreten, das proaktive Vorgehen der Polizei sei möglich, jedoch nicht mit nachrichtendienstlichen Mitteln²⁷³. Diese beiden Auffassungen schließen sich auch nicht gegenseitig aus:

Dem Rechtsstaatsprinzip wird Rechnung getragen, wenn jedenfalls die kumulative Anwendung von Vorfeldermittlung und nachrichtendienstlichen Befugnissen dem Nachrichtendienst vorbehalten bleibt. Für diesen wiederum muß es bei der Regelung des § 8 III BVerfSchG bleiben.

²⁶⁹ Gusy, Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten, ZRP 1987, S. 45 ff. (46)

²⁷⁰ Lammer, Verdeckte Ermittlungen, S. 149

²⁷¹ so Liskén, Polizei und Verfassungsschutz, NJW 1982, S. 1481 ff. (1483) und ders., in Liskén / Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. C, Rn. 16

²⁷² Erfurth, Verdeckte Ermittlungen, S. 44

²⁷³ Weßlau, Vorfeldermittlungen, S. 227

Durch das Terrorismusbekämpfungsgesetz 2001 wurden allerdings die Befugnisse des Nachrichtendienstes bedenklich ausgeweitet²⁷⁴. Ferner kam es zur Einrichtung eines sog. „Informationsboards“ beim BKA, einem „runden Tisch“ zur Zusammenarbeit von BKA und Nachrichtendiensten. Zwar wurde das Trennungsgebot angesprochen, eine Entscheidung dazu jedoch ausdrücklich vertagt²⁷⁵.

Wiederum ist somit, wie schon bei der Vorfeldermittlung, festzustellen, daß eine grundlegende Entscheidung, durch welche sich den verfassungsrechtlichen Anforderungen am besten Rechnung tragen ließe, aufgeschoben oder vermieden wird. Statt dessen wird – aus beiden Richtungen - eine verschleierte Aufweichung des Trennungsgebots vollzogen, die den historischen Erfahrungen in keiner Weise gerecht wird.

Vorzuziehen wäre auch hier de lege ferenda eine systematische Lösung, die jedenfalls verdeckte Maßnahmen im Vorfeld der zureichenden tatsächlichen Anhaltspunkte ausschließen müßte, um das Rechtsstaatsprinzip zu achten.

5) Zwischenergebnis: BKA-Streife und Trennungsgebot

Nach alldem ist festzuhalten, daß das zu prüfende BKA-Vorgehen -im eingrifflosen Bereich- insoweit mit dem Rechtsstaatsprinzip vereinbar ist. Die historischen Erfahrungen werden nicht mißachtet.

E. Ermächtigungsgrundlagen der Maßnahmen mit Eingriffsqualität

Neben dem Vorliegen einer Aufgabenzuweisungsnorm ist für die Maßnahmen mit Eingriffsqualität noch eine Ermächtigungsgrundlage zur Rechtfertigung des Grundrechtseingriffs erforderlich.

²⁷⁴ Rublack, Terrorismusbekämpfungsgesetz, DuD 2002, S. 202 ff. (203)

²⁷⁵ Kollmann, Islamistischer Terrorismus – eine Herausforderung für die internationale Staatengemeinschaft, <<http://www.bdk.de/magazin/januar-2002.php3>> (S. 6)

I. Bayern

Es wird diskutiert, ob für die Internet-Streifentätigkeit Art. 31 oder 33 BayPAG heranzuziehen ist²⁷⁶: Art. 33, die Ermächtigung zur Datenerhebung mit technischen Mitteln, erfordert anders als die allgemeine Regelung in Art. 31 BayPAG das Vorliegen einer konkreten Gefahr²⁷⁷.

Nach der hier vertretenen Auffassung kann es auf eine Subsumtion unter diese Eingriffsgrundlagen jedoch gar nicht mehr ankommen: Könnte eine Befugnisnorm zwar ggf. über die fehlende Aufgabenzuweisungsnorm hinweghelfen, ist jedoch aufgrund der Annahme der fehlenden Länder-Gesetzgebungskompetenz für den Bereich der Vorfeldermittlung jeder landesrechtlichen Regelung der Rechtsboden entzogen. Die bayerische Streife ist demnach insgesamt rechtswidrig.

II. BKA-Streife

Für das Vorgehen des BKA muß hingegen für die Maßnahmen, für welche die Eingriffsqualität bejaht wurde, namentlich für die IRC-Teilnahme ohne Nennung der Ermittlereigenschaft im Nutzernamen, eine Ermächtigungsgrundlage gesucht werden.

Einer Ansicht nach ist eine solche Eingriffsgrundlage – auch für das verdecktes Vorgehen - in **§ 7 II BKAG** vorhanden²⁷⁸: § 7 BKAG greift auch im Rahmen der Strafverfolgungsvorsorge, wie sich aus der amtlichen Begründung zum BKAG ergibt²⁷⁹. Die Norm stelle eine Generalklausel für die Datenverarbeitung zur Erfüllung der Zentralstellenaufgabe dar.

Dem ist schon der Wortlaut von § 7 II BKAG entgegenzuhalten: Ein „Ersuchen um Auskünfte und Anfragen“ setzt ein Vorgehen im Wege des Dialogs

²⁷⁶ Stadler, Anlaßunabhängige Überwachung des Internet, <<http://www.afs-rechtsanwaelte.de/internetstreife.htm>>

²⁷⁷ Kant, Internet-Streifen, Bürgerrechte & Polizei 1/2002, S. 29 ff. (36)

²⁷⁸ Zöller, Verdachtslose Recherchen und Ermittlungen im Internet, GA 2000, S. 563 ff. (574)

²⁷⁹ Soiné, Datenverarbeitung für Zwecke künftiger Strafverfahren, CR 1998, S: 257 ff. (261); BT-Drucksache 13/1550, S. 25 (für § 8)

voraus²⁸⁰. Das BKA darf somit lediglich offen Daten bei nicht-öffentlichen Stellen erheben²⁸¹: Die Behördeneigenschaft ist somit deutlich zu machen.

Überdies ist ferner - trotz der jüngsten Befugnisserweiterung im Terrorismusbekämpfungsgesetz - problematisch, inwieweit sich exekutive Informationserhebungsmaßnahmen noch im Rahmen der Zentralstellenaufgabe des BKA halten²⁸². Einer Ansicht nach muß sich das BKA als Koordinierungsstelle auf Sammlung und Auswertung konzentrieren (§ 7 I); die Datenerhebung (§ 7 II) dagegen bleibe primär Aufgabe der Länderpolizeien²⁸³. Diese Ansicht findet auch einen Anknüpfungspunkt in der Gesetzesbegründung: Der Gesetzgeber ging davon aus, daß die Informationen dem BKA „regelmäßig ... von den Polizeien des Bundes und der Länder angeliefert“²⁸⁴ werden.

Dagegen ist der internetspezifische länderübergreifende Charakter der Cyber-Kriminalität als Argument einzuwenden. Grundsätzlich scheint die Koordinierungsarbeit der Zentralstelle daher im vorliegenden Rahmen erforderlich: Das Vorgehen hat allein diese Unterstützungsfunktion der Arbeit der Länderpolizeien zum Ziel; unmittelbar nach Identifizierung der Verantwortlichen erfolgt die Weiterleitung.

Wird bei der Internetermittlung jedoch durch eine Verschleierung der Ermittlereigenschaft und deshalb fehlender Überschaubarkeit eine Eingriffsqualität erreicht, so kann dies schon wegen des nicht-offenen Vorgehens in § 7 II BKAG keine Rechtfertigung finden²⁸⁵.

Die dargestellte Ermittlungsmaßnahme im IRC ist damit, jedenfalls in der derzeit praktizierten nicht-offenen Vorgehensweise, rechtswidrig.

²⁸⁰ Germann, Gefahrenabwehr und Strafverfolgung im Internet, S. 517

²⁸¹ Kant, Internet-Streifen, Bürgerrechte & Polizei 1/2002, S. 29 ff. (35)

²⁸² Ahlf in Ahlf / Daub / u.a., BKAG, § 2, Rn. 33

²⁸³ Stadler, Anlaßunabhängige Überwachung des Internet,

<<http://www.afs-rechtsanwaelte.de/internetstreife.htm>>

²⁸⁴ BT-Drucksache 13/1550, S. 24

²⁸⁵ BT-Drucksache 14/5555, 18. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz vom 13.03.01, S.105

F. Vorgehen zu Identifizierung des Verantwortlichen

Im Anschluß an die Internetstreifenfötigkeit nehmen die Ermittler Maßnahmen zur Identifizierung des Verantwortlichen vor, indem sie beim Zugangsprovider die Identität eines Nutzers erfragen: Wie bereits dargestellt (S. 12,13) kann der Zugangsprovider technisch das (temporäre) Pseudonym auch einer dynamischen IP-Adresse aufdecken. Solange die Logfiles noch nicht gelöscht sind, kann der Provider seinen entsprechenden Kunden identifizieren.

Zur Bestimmung der Eingriffsgrundlage ist zunächst die Natur des jeweiligen Datums zu bestimmen. Kommunikationsdaten lassen sich in Bestands- und Verbindungsdaten unterteilen. Definitionen dieser Begriffe finden sich in der TDSV²⁸⁶.

Bestandsdaten sind (gem. § 2 Nr. 3 TDSV) die Daten, die zur Begründung eines Vertragsverhältnisses über TK-Dienste einschließlich dessen inhaltlicher Ausgestaltung erforderlich sind.

Verbindungsdaten sind (gem. § 2 Nr. 4 TDSV) die Daten, die bei der Bereitstellung und Erbringung von Telekommunikationsdiensten anfallen.

I. § 89 VI TKG

Ob vorliegend Regelungen über Bestandsdaten oder Verbindungsdaten anzuwenden sind, ist bereits heftig umstritten: Das BKA²⁸⁷ beruft sich im Zusammenhang mit den Recherchen beim Zugangsprovider auf § 89 VI TKG²⁸⁸. Nach § 89 VI TKG haben die Anbieter von Telekommunikationsdienstleistungen auf Ersuchen von Strafverfolgungsbehörden diesen im Einzelfall eine Auskunft über alle **Bestandsdaten** des Anschlußinhabers zu erteilen, soweit dies für die Aufgabenerfüllung der anfragenden Stellen erforderlich ist²⁸⁹.

²⁸⁶ Holznagel / Enaux / Nienhaus, Grundzüge des Telekommunikationsrechts, S. 184

²⁸⁷ Aufgrund der festgestellten Rechtswidrigkeit der bayerischen Internetstreife soll hier nur noch auf das BKA eingegangen werden.

²⁸⁸ Meseke, Ermittlung und Fahndung im Internet, in BKA (Hrsg.), Festschrift für Herold, S. 505 ff. (523)

²⁸⁹ Holznagel / Enaux / Nienhaus, Grundzüge des Telekommunikationsrechts, S. 191

Eingewandt wird hiergegen, bei der als Identifizierungsmerkmal dienenden dynamischen IP-Adresse handele es sich um ein Verbindungsdatum²⁹⁰.

In der Tat muß bei IP-Adressen differenziert werden: Die dynamischen IP-Adressen fallen allein bei den einzelnen Kommunikationsvorgängen an und sind daher als Verbindungsdatum zu sehen. Nur statische IP-Adressen sind bereits als Vertragsbestandteil denkbar und bleiben konstant, so daß diese als Bestandsdaten zu sehen sind²⁹¹.

Die Anwendung einer Regelung zur Auskunft über Bestandsdaten wird jedoch teilweise auch damit begründet, daß „im Ergebnis nur Bestandsdaten herausgegeben werden sollen“²⁹².

Zwar werden in der Tat Name und Anschrift des Kunden herausgegeben, welche selbst unzweifelhaft Bestandsdaten sind. Abzustellen ist jedoch für die Ermächtigungsgrundlage auf das zur Identitätsbestimmung von den Behörden vorgelegte Datum, also die IP-Adresse: *Zu dieser* sollen Angaben gemacht werden. Datenschutz und Speicherfristen setzen stets an diesem die Aufdeckung des Pseudonyms ermöglichenden Datum an, nicht an den herauszugebenden Daten: Wäre die dynamische IP-Adresse gelöscht, so könnten erst gar keine Bestandsdaten ermittelt werden. Somit ist die Zuordnung dynamischer IP-Adressen zu konkreten Nutzern als Erhebung von Verbindungsdaten einzuordnen und § 89 VI TKG unanwendbar²⁹³.

Die Provider erheben ferner zu Recht noch einen grundlegenden Einwand gegen die Heranziehung von § 89 TKG: Das TKG ist gar nicht auf den Zugangsprovider anwendbar. Die Zugangsprovider erbringen *keinen* Telekommunikationsdienst, sondern einen **Teledienst** i.S.v. § 2 II Nr. 3 TDG. Entsprechend ist der Teledienstedatenschutz im TDDSG maßgeblich²⁹⁴. Das

²⁹⁰ Weichert, Cyber-Crime-Bekämpfung und Datenschutz, DaNa 2/2001, S. 5 ff. (7)

²⁹¹ Bär, Auskunftsanspruch über Telekommunikationsdaten nach den neuen §§ 100g, 100h StPO, MMR 2002, S. 358 ff. (359)

²⁹² Graf, Befugnisse und Grenzen der Ermittlungsbehörden, DPoIB1 4/2001, S. 6 ff. (8)

²⁹³ Weichert, Cyber-Crime-Bekämpfung und Datenschutz, DaNa 2/2001, S. 5 ff. (7)

²⁹⁴ BT-Drucksache 14/5555, 18. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz vom 13.03.01, S.105

TDDSG enthielt im Entwurfsstadium eine Auskunftspflichtung für Teledienste, die jedoch aus datenschutzrechtlichen Gründen gestrichen wurde.²⁹⁵ Erkundigungsbefugnisse gegenüber Telediensten hinsichtlich der sog. Teledienstenutzungsdaten hat nun erstmals das Terrorismusbekämpfungsgesetz den Nachrichtendiensten eingeräumt, nicht aber dem BKA. Diese Entscheidung des Gesetzgebers darf nicht mit der Argumentation unterlaufen werden, das TKG sei auch anwendbar, weil bei jeder Abwicklung von Telediensten öffentliche Leitungen benutzt würden.

Liegen noch keine zureichenden tatsächlichen Anhaltspunkte einer Straftat vor, kommt auch die neue Regelung des § 100 g StPO schon mangels Anfangsverdachts nicht in Betracht.

II. § 7 II BKAG

Zu denken ist jedoch wiederum an § 7 II BKAG: Seit der Befugnisweiterung im Rahmen des Terrorismusbekämpfungsgesetzes kann das BKA ohne vorherige Koordination und Absprache mit den Ländern offen Informationen erheben, soweit dadurch vorhandene Sachverhalte ergänzt werden sollen. Als solch vorhandener Sachverhalt können die im Rahmen der Internetstreife gewonnenen Informationen zu inkriminierten Angeboten gesehen werden, so daß § 7 II BKAG eine geeignete Grundlage für das Ersuchen um Auskunft beim Zugangsprovider darstellt.

Hinzuweisen bleibt jedoch darauf, daß auch bei Identifizierung des Rechners unter Umständen noch ungeklärt ist, welche Person aus einem Kreis mehrerer auf diesen Rechner Zugriffsberechtigter für die betreffende Benutzung verantwortlich war.²⁹⁶ Dies erfordert klassische offline-Ermittlungsarbeit.

²⁹⁵ Bär, Aktuelle Rechtsfragen bei strafprozessualen Eingriffen in die Telekommunikation, MMR 2000, S. 472 ff. (479)

²⁹⁶ Janovsky, Internet und Verbrechen, Kriminalistik 1998, S. 500 (503)

G. Rechtmäßigkeit vor dem Hintergrund möglicher grenzüberschreitender Ermittlung

Aufgrund der Grenzüberschreitung und Internationalität des Internets ist die Überprüfung der Rechtmäßigkeit noch nicht mit der Feststellung abgeschlossen, daß zumindest das eingriffslose Vorgehen des BKA im Inland rechtmäßig ist.

I. Prinzip der formellen Territorialität

Auch wenn die BKA-Ermittler von Deutschland aus agieren, stellt sich die Frage, ob sie nicht durch ihre online-Maßnahmen bereits die Gebietshoheit eines fremden Staates berühren: Die völkerrechtlich geschützte innere Souveränität eines Staates umfaßt auch alle Dinge, die sich auf dem Staatsgebiet befinden.²⁹⁷ Sie erstreckt sich damit auf jene „**physikalischen Pfeiler** (Server, Netzknoten)“²⁹⁸, die das Internet tragen.

Wie zentral diese Frage ist, zeigt erneut ein Blick in die Fallzahlen des BKA: Von den 1086 Fällen im Jahr 2001 waren **78 %** Auslandsfälle. Der Schwerpunkt liegt dabei, mit 577 Vorkommnissen (= 61 % der Auslandsfälle), in den USA. Die Ermittlungstätigkeit hatte also in der weit überwiegenden Zahl der Bearbeitungen Bezug zu fremdem Territorium.

Nicht identisch mit dieser Problematik ist die vorliegend weitgehend ausgeklammerte Frage der Anwendbarkeit deutschen Strafrechts. Vielmehr kann eine Ermittlungsmaßnahme auf fremdem Territorium ebenso gegen das Völkerrecht verstoßen, wenn sich das Ermittlungsverfahren gegen einen deutschen Staatsbürger richtet.

Somit wirft ein deutschsprachiges rechtswidriges Angebot, das von einem deutschen Staatsbürger ins Netz gestellt wurde, bisweilen dieselbe Frage auf: Der USA-Schwerpunkt der entdeckten Inhalte bedeutet keinesfalls, daß die für

²⁹⁷ Spatscheck / Alvermann, Internet-Ermittlungen im Steuerstrafprozeß, wistra 1999, S. 333 ff. (335)

²⁹⁸ Dix, Internationale Aspekte in: Bäumler (Hrsg.), E-Privacy, S. 93 ff. (93)

die Inhalte Verantwortlichen auch tatsächlich dort ansässig sind. Vielmehr ist die Ursache die große Zahl von Internet-Service-Providern mit Sitz und Servern in den USA, gerade auch die überwältigende Mehrheit der Free-Webpace-Anbieter.

Im Rahmen eines solchen Free-Webpace-Services wird kostenloser Speicherplatz auf einem Host-Server zur Verfügung gestellt. Der Server finanziert sich selbst durch Werbung, die im Angebot plaziert wird. Da keine Bestandsdaten zur Abrechnung benötigt werden, beschränkt sich die Anmeldung des Kunden mitunter auf eine nicht überprüfte online-Registrierung. Wo der Verantwortliche sich tatsächlich aufhält, bleibt zunächst ebenso unklar wie seine wahre Identität. Wer ein rechtswidriges Angebot online veröffentlichen will, wird dies somit bevorzugt im Rahmen dieser Free-Webpace-Dienste tun. So erklärt sich der US-Schwerpunkt des ZaRD-Fallaufkommens.

Zur Beurteilung der Rechtmäßigkeit der dargestellten Ermittlungsmaßnahme ist nach dem Gesagten somit noch zu klären, ob in der anlaßunabhängigen Recherche ein Verstoß gegen das sog. Prinzip der formellen Territorialität liegt.

Relevant ist diese Frage auch aus dem Grund, daß diese allgemeine Regel des Völkerrechts gemäß Art. 25 GG Bestandteil des Bundesrecht ist. Jeder Verstoß gegen das sog. Prinzip der formellen Territorialität ist damit zugleich ein Verstoß gegen das innerdeutsche Recht²⁹⁹.

Die völkerrechtlichen Regeln stehen gemäß Art. 25 II GG im Rang über dem einfachen Recht. Einer Ansicht nach kann deshalb ein Verstoß gegen das Territorialprinzip auch zum Beweisverwertungsverbot hinsichtlich der Ermittlungsergebnisse führen³⁰⁰: Denn ein subjektives Recht des Einzelnen ergebe sich vorliegend daraus, daß im Anwendungsbereich von Rechtshilfeabkommen diese Abkommen unmittelbare Eingriffsbefugnisse

²⁹⁹ Germann, Gefahrenabwehr und Strafverfolgung, S. 641

³⁰⁰ Spatscheck / Alvermann, Internet – Ermittlungen im Steuerstraßprozeß, wistra 1999, S. 333 ff. (335)

gegen den Einzelnen begründen, ihn also unmittelbar betreffen. Ein Verstoß gegen die Abkommen berühre somit auch die Rechtsposition des Beschuldigten.

Auf das hoch umstrittene Feld der Beweisverwertungsverbote kann im Rahmen dieser Arbeit aber nur hingewiesen werden.

II. Eingriff in die Gebietshoheit eines fremden Staates

Ein Eingriff in den fremden Hoheitsbereich liegt vor, wenn sich die Ermittlungsmaßnahme unmittelbar im Gebiet des betreffenden Staates tatsächlich auswirkt³⁰¹. Die Rechtswidrigkeit liegt in der Anmaßung, die eigene Hoheitsgewalt auf fremdem Staatsgebiet ohne vorherige Zustimmung auszuüben³⁰².

Eine solche Anmaßung stellt auch ohne Zwangsmaßnahmen oder Gewalteinwirkung einen Eingriff dar³⁰³.

III. Einordnung der Internetstreife

1) Streifengang

Eine klassische Streifenfahrt im Ausland wäre eindeutig ein Eingriff in die Gebietshoheit des fremden Staates³⁰⁴. Tatsächlich sind in diesem Zusammenhang jedoch Unterschiede zwischen der realen und der virtuellen Streifenfahrt von Belang, die im Inland noch ohne rechtliche Relevanz waren:

Zwar ist die Tatsache, daß die Ermittler selbst im Fall der Internetstreife im Inland verbleiben, unerheblich: Wie erwähnt erstreckt sich die innere Souveränität auch auf sämtliche Sachen, somit auch die Server im Staatsgebiet. Wird auf diese direkt zugegriffen, so liegt bereits darin ein Eingriff in die innere Souveränität des fremden Staates³⁰⁵.

³⁰¹ Ipsen, Völkerrecht, § 23, Rn. 6

³⁰² Seidl-Hohenveldern / Stein, Völkerrecht, Rn. 1506

³⁰³ Sieber: in Hoeren / Sieber (Hrsg.), Handbuch Multimedia Recht, S. 736

³⁰⁴ Kudlich, Strafprozessuale Probleme des Internet, JA 2000, S. 227 ff. (228)

³⁰⁵ Derksen, Bekämpfung von Rechtsradikalismus und Rassismus im Internet, ZFIS 1999, S. 150 ff. (155)

Auch steht der Annahme eines Eingriffs nicht von vornherein entgegen, daß im Inland das Vorgehen nicht als Eingriff gewertet wird. Maßgeblich ist, ob die Maßnahme im betroffenen Land einen Hoheitsakt darstellt³⁰⁶. Es wäre also die Beurteilung des betroffenen Staates heranzuziehen.

Für die Internetstreife wird bisweilen der Vergleich herangezogen, wie bei dem Abonnement einer ausländischen Zeitung ordne sich die Behörde hier völlig der fremden Gebietshoheit unter. Es handele sich bei der Internet-Recherche um schlicht-hoheitliches informationelles Handeln.³⁰⁷ Etwas anderes ergebe sich erst für die Maßnahmen mit Eingriffscharakter, so beim IRC³⁰⁸.

Zwar scheint die Informationsgewinnung über ausländische Zeitungen kein passendes funktionales Äquivalent zu sein: Die Behörde greift bei der Streife online auf Server im Ausland zu und nimmt nicht nur Informationen im Inland auf.

Im Ergebnis ist der Ablehnung einer Anmaßung fremder Hoheitsgewalt jedoch zuzustimmen. Die Online-Streife unterscheidet sich von ihrem Offline-Äquivalent insbesondere durch folgendes Phänomen, welches im übrigen auch für vergleichbare Maßnahmen mit Eingriffscharakter *de lege ferenda* gelten würde:

Die Behörde ist sich bei der Internetstreife zu Beginn ihrer Tätigkeit sehr häufig nicht bewußt, in fremdem Territorium zu handeln. So lassen schon generische Top-Level-Domains, welche anders als die Länderkürzel den Inhalt der Seite charakterisieren, keinen eindeutigen Schluß auf die Herkunft der Seite zu³⁰⁹. Ebenso verhält es sich zum Beispiel, wenn nur eine e-mail-Adresse aus dem Usenet als erster Ansatzpunkt zur Verfügung steht. Im übrigen werden Angebote im Internet regelmäßig auf einer Vielzahl von Servern „gespiegelt“, kopiert bereitgehalten, um den Zugriff zu beschleunigen³¹⁰. Auch dies kann den Schluß auf den Standort behindern.

³⁰⁶ Ipsen, Völkerrecht, § 23, Rn. 7

³⁰⁷ Soiné, Strafverfolgung, Polizei und Internet, *Polizeispiegel* 2001, S. 167 ff. (169)

³⁰⁸ Germann, *Gefahrenabwehr und Strafverfolgung*, S. 653

³⁰⁹ (.com;.net;.org;.gov;.mil;.edu;.int:)Köhler / Arndt, *Recht des Internet*, Rn. 11

³¹⁰ Hilgendorf, *Die Neuen Medien und das Strafrecht*, *ZStW* 2001, S. 650 ff. (666)

In diesen Fällen des Zweifels über den Ort ihres Handelns wäre die Behörde gänzlich an der Ermittlung gehindert, wenn sie stets befürchten müßte, damit das Völkerrecht zu verletzen³¹¹. Dies ist *nicht* Sinn und Zweck des formellen Territorialitätsprinzips.

Ein Vergleich aus der realen Welt findet sich im Bereich des Rundfunks über geostationäre Satelliten: Aus technischen Gründen reicht deren Sendekegel zwangsläufig über die Landesgrenzen hinaus (sog. Spill-over-Effekt)³¹². Wenn die Einwirkung auf den fremden Staat sich als unvermeidliche Folge einer Tätigkeit darstellt, deren Ziel die Änderung eines Zustands im eigenen Gebiet ist, soll keine verbotene Verletzung fremder Gebietshoheit vorliegen.

Dieser (umstrittene) Gedanke wird nun bereits auch für Fragen des Internationalen Deliktsrechts im Internet herangezogen³¹³. Er kann auch die Problematik der Internetstreife mit Auslandsbezug klären. Solange die Behörde unbewußt auf fremden Territorium agiert, kann dies jedenfalls nicht als rechtswidriger Eingriff in die Hoheitsmacht eines fremden Staates gewertet werden. Die BKA-Streife verstößt somit bei der Streifentätigkeit, die im Inland als rechtmäßig erachtet wurde, auch nicht gegen das Völkerrecht.

2) Anfrage beim Zugangs-Provider

Anders als bei der Streife stellt sich die Situation bei der Providieranfrage dar: Fordert die Behörde einen ausländischen Provider zur Herausgabe von Daten auf, so greift sie – in diesem Fall auch bewußt – in fremdes Hoheitsrecht ein.

Dem vorgelagert ist aber bereits das Problem, daß ausländische Provider gar nicht den Auskunftsansprüchen unterliegen, die gegenüber deutschen Providern bestehen³¹⁴. Es kommt hier somit nur der Weg der internationalen Rechtshilfe in Betracht.

³¹¹ Germann, Gefahrenabwehr und Strafverfolgung, S. 646

³¹² Seidl-Hohenveldern / Stein, Völkerrecht, Rn. 1284

³¹³ Köhler / Arndt, Recht des Internet, Rn. 536

³¹⁴ Graf, Befugnisse und Grenzen der Ermittlungsbehörden, DPoIb1 4/2001, S. 6 ff. (8)

IV. Probleme der Rechtshilfe und angestrebte Lösung

Rechtshilfe (im engeren Sinne) ist die Unterstützung für ein strafrechtliches Verfahren eines anderen Staates³¹⁵. Das Verfahren der internationalen Rechtshilfe gestaltet sich noch immer äußerst zeitaufwendig.

Die Inanspruchnahme von Rechtshilfe durch die Ermittlungsbehörden ist nicht im Europäischen Rechtshilfeübereinkommen geregelt, sondern dem innerstaatlichen Strafprozeßrecht zuzuordnen. Mangels anderer Regelungen kommt die analoge Anwendung der StPO in Betracht, auf die in § 77 IRG verwiesen wird³¹⁶. Die Behörde darf infolge der analogen StPO-Anwendung somit nur für solche strafprozessualen Maßnahmen ein Ersuchen stellen, die sie im Inland selbst hätte vornehmen dürfen.

Auch die *Beweisverwertung* richtet sich nach dem deutschen Recht. Für die Rechtmäßigkeit der *Datenerhebung* aber zieht die h.M. das Prinzip des „lex fori“, anerkannt im Internationalen Zivilprozeßrecht, heran. Es ist danach die Rechtmäßigkeit der Beweiserhebung nach dem Recht des Eingriffsortes maßgeblich und ggf. ausreichend für die Verwertbarkeit der Daten im hiesigen Strafverfahren³¹⁷. Probleme ergeben sich hier jedoch, wenn am Eingriffsort eine Eingriffsgrundlage, z.B. für den Zugriff auf Netzwerke, (noch) nicht vorgesehen ist. Es kommt dann zur Ablehnung des Rechtshilfeersuchens.

Angesichts der Kurzlebigkeit einiger Daten im Internet droht auch aufgrund der langen Bearbeitungszeit der Rechtshilfe häufig der endgültige Verlust von Beweismaterial³¹⁸. Gerade Angebote im Free-Webpace-Bereich wechseln mitunter täglich ihren Standort, um der Verfolgung zu entgehen.

Verbesserung schafft hier nun die Möglichkeit einer „**Preservation Order**“³¹⁹. Um einer Vernichtung der Daten zuvorzukommen, wird deren Sicherung

³¹⁵ Soiné, Fahndung via Internet, NStZ 1997, S. 166 ff. (167)

³¹⁶ Vassilaki, Strafverfolgung der grenzüberschreitenden Internet-Kriminalität, CR 1999, S. 574 ff. (578)

³¹⁷ Vassilaki, Strafverfolgung der grenzüberschreitenden Internet-Kriminalität, CR 1999, S. 574 ff. (578)

³¹⁸ Schuster, Die Grenzen polizeilicher Ermittlungen, in: Bäumler (Hrsg.): E-Privacy, S. 77 ff. (85)

³¹⁹ Meseke, Ermittlungen im Internet, Kriminalistik 2000, S. 245 ff. (247)

beantragt, die Daten daraufhin gleichsam „eingefroren“. Eine Herausgabe erfolgt dann jedoch erst nach einem positiv beschiedenen Abschluß des Rechtshilfeverfahrens.

Derartige Verbesserungen der internationalen Zusammenarbeit sind auch ein großes Ziel im Rahmen der „Convention on Cybercrime“. Diese am 08.11.2001 verabschiedete Konvention des Europarats sieht in den Art. 26 ff. engere Kooperations- und Beistandspflichten vor, die über die gängige Rechtshilfe hinausgehen: Bei Dringlichkeit werden auch Anfragen per E-mail und Fax möglich. Jeder Vertragsstaat soll ferner eine Zentralstelle für den Kontakt im Rahmen dieser Anfragen einrichten, Art. 27 der Konvention.³²⁰ Gem. § 3 BKAG wird auch in diesem Rahmen das BKA zuständig sein.

Die Konvention ist im übrigen nicht unumstritten, besonders aufgrund ihrer übereilten Verabschiedung nach dem 11. September 2001³²¹. Jedoch tritt sie ohnehin erst in Kraft, wenn mindestens fünf Staaten, davon 3 Mitgliedsstaaten sie ratifiziert haben. Bislang taten dies nur Albanien und Kroatien³²².

H. Zusammenfassung und Schlußbetrachtung

I. Zusammenfassung

Auch wenn es technisch möglich ist, das Internet umfassender zu überwachen und den Cyberspace zu einem „sichereren Ort“ zu machen als die reale Welt³²³: Die Internetermittlung muß sich an denselben rechtlichen Grenzen messen lassen wie die polizeiliche Offline-Arbeit. Daß das Netz kein rechtsfreier Raum ist, gilt auch für die Internet-Ermittlungsmaßnahmen selbst.

Aufgrund der hier vertretenen Einschränkung des Eingriffsbegriffs ist die Eingriffsqualität nur für die Teilnahme an IRC und Usenet, bei der die Ermittlereigenschaft verschleiert wird, bejaht worden.

³²⁰ Kugelmann, Die „Cybercrime“-Konvention, DuD 2001, S. 215 ff. (221)

³²¹ Marberth-Kubicki, Internet und Strafrecht, (I. 2b) cybercrime convention)
<<http://www.ag-strafrecht.de/aufsatzkubik.htm>>

³²² <<http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=185>>

³²³ Rötzer, Das Recht auf Anonymität, in: Bäumler (Hrsg.): E-Privacy, S. 27 ff. (32)

Zu prüfen war jedoch für alle Maßnahmen das Vorliegen einer Aufgabenzuweisungsnorm: Aufgrund des Fehlens einer Präventivwirkung ist die Internetstreife eine allein repressive Maßnahme. Deshalb wurde die Gesetzgebungskompetenz der Länder verneint: Für den rein repressiven Bereich hat der Bundesgesetzgeber durch die StPO abschließend von seiner konkurrierenden Gesetzgebungskompetenz Gebrauch gemacht.

Dies führt de lege lata zur Rechtswidrigkeit der Internetstreife durch die bayerische Polizei: Das BayPAG bietet für die Vorfeldtätigkeit keine Rechtsgrundlage.

Hinsichtlich der Tätigkeit des BKA wurde eine Aufgabenzuweisungsnorm für die Vorfeldermittlung im Rahmen der Zentralstellenfunktion bejaht. Auch wurde insoweit Vereinbarkeit mit dem Trennungsgebot festgestellt. Im eingriffslosen Bereich ist die BKA-Tätigkeit auch mit dem Prinzip der formellen Territorialität vereinbar und greift nicht in die Gebietshoheit fremder Staaten ein.

Jedoch konnte für die Maßnahmen mit Eingriffscharakter aufgrund des nicht-offenen Vorgehens keine Eingriffsgrundlage in § 7 II BKAG gesehen werden.

Ein rechtsstaatliches Dilemma wurde deutlich: Ein verdecktes Vorgehen der Polizei im Vorfeld des Anfangsverdachts wurde als mit dem Trennungsgebot nicht vereinbar bewertet. Auch de lege ferenda ist somit die verdeckte anlaßunabhängige Ermittlung im IRC nicht in rechtsstaatlicher Form denkbar. Verdeckte Tätigkeit im Vorfeld muß im Rechtsstaat den Nachrichtendiensten vorbehalten und auf den Bereich des Staatsschutzes beschränkt bleiben.

II. Schlußbetrachtung:

Besonders betroffen von der Internetstreife ist nicht die eigentliche Zielgruppe der Ermittler: Es kommt nicht zur Verhinderung, sondern zur Verlagerung der Kriminalität in weniger kontrollierbare Bereiche.

Vermeiden läßt sich dieser Verdrängungseffekt nur durch Totalüberwachung: In einigen totalitären Regimen ist zu diesem Zweck schon heute der Staat der einzige Zugangs-Provider.

Daß das Szenario der Totalüberwachung auch in einer Demokratie keine Überdramatisierung ist, läßt sich tendenziell schon heute in der Offline-Welt beobachten: Im Umkreis der CCTV³²⁴-überwachten britischen Großstädte rüsten nun auch die kleineren Orte ihre Straßen mit Kameras aus, um nicht Ausweichstandort für Kriminelle zu werden.³²⁵

Als erster zum Schweigen gebracht wird durch ein sich ausbreitendes Klima des Panopticons der redliche, datenschutzbewußte Bürger. Bereits heute ist die Sorge um den Schutz der Privatsphäre einer der Hauptgründe, nicht am Leben im Internet teilzunehmen.

In der Vermutung der Rechtstreue seiner Bürger unterscheidet sich der Rechtsstaat vom Polizeistaat.³²⁶

Vor jedem weiteren Schritt des Gesetzgebers ins Vorfeld des Anfangsverdachts ist deshalb die Warnung des Bundesverfassungsgerichts im Volkszählungsurteil zu bedenken:

Ein Verzicht auf die Ausübung der Kommunikationsgrundrechte wird „nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“³²⁷

³²⁴ (Closed Circuit Television): Lloyd, Legal Aspects of the Information Society, S. 42 f.

³²⁵ Bleyenberg, Das Internet als Panopticon, (6. Die Überwachung von Staat und Betrieb), <<http://www.uni-muenster.de/PeaCon/zurawski/panopticum/interpan.htm>>

³²⁶ WeBlau, Vorfelddermittlungen, S. 337

³²⁷ BVerfGE 65, 1 (43)