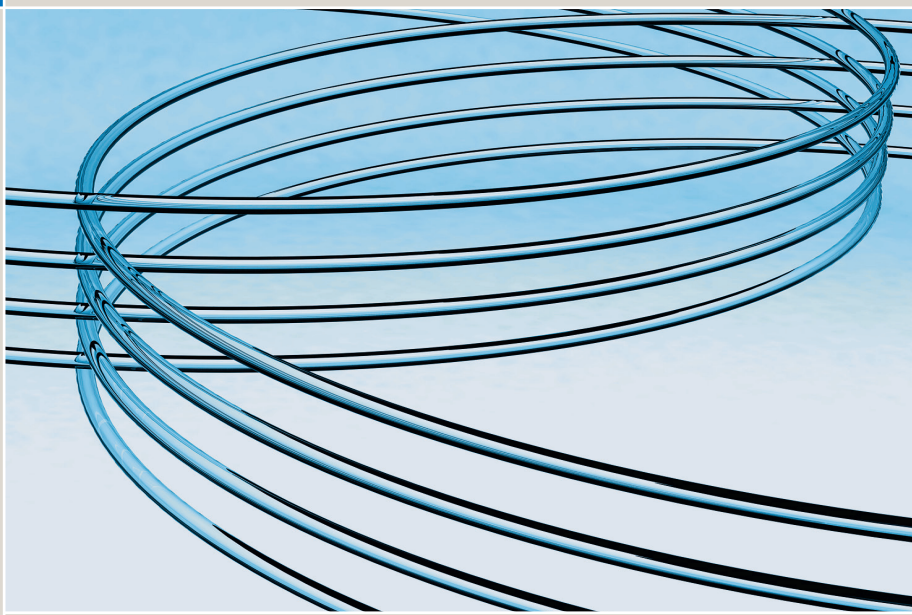
22

BIEMANN

Schriften zum Recht der Inneren Sicherheit



»Streifenfahrten« im Internet

Die verdachtsunabhängigen Ermittlungen der Polizei im virtuellen Raum

BOORBERG

„Streifenfahrten“ im Internet

Die verdachtsunabhängigen Ermittlungen der Polizei im virtuellen Raum

Dr. Jens Biemann

BOORBERG

Bibliografische Information der Deutschen Nationalbibliothek | Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über www.dnb.de abrufbar.

ISBN 978-3-415-05104-1 E-ISBN 978-3-415-05224-6

Satz: Thomas Schäfer, www.schaefer-buchsatz.de | Druck und Bindung: e. kurz + co druck und medientechnik gmbh, Kernerstraße 5, 70182 Stuttgart

Richard Boorberg Verlag GmbH & Co KG | Scharrstraße 2 | 70563 Stuttgart
Stuttgart | München | Hannover | Berlin | Weimar | Dresden
www.boorberg.de

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2012 von der Rechtswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg im Breisgau als Dissertation angenommen. Gesetze, Rechtsprechung und Schrifttum sind im Wesentlichen auf dem Stand von Dezember 2012.

Mein besonderer Dank gilt Herrn Prof. Dr. Thomas Würtenberger, der diese Arbeit mit sehr wertvollen fachlichen Ratschlägen und viel Verständnis betreute. Für die zügige Erstellung des Zweitgutachtens danke ich Herrn Prof. Dr. Walter Perron.

Besonders bedanken möchte ich mich bei meinen Freunden und meiner Familie, die mich stets vorangetrieben und damit erheblich zum Erfolg dieser Arbeit beigetragen haben. Stellvertretend seien Thomas Beisken LL.M., Henrik Siemer, Christoph Boeminghaus sowie meine Brüder Michael Biemann und Prof. Dr. Torsten Biemann genannt.

Mein größter Dank gebührt zweifelsohne meinen Eltern Hubert und Ingrid Biemann, die mich bedingungslos in meinem Leben und auch bei dieser Arbeit unterstützten. Ihnen ist diese Arbeit gewidmet.

Düsseldorf, Mai 2013 *Jens Biemann*

Inhaltsverzeichnis

A.
Einleitung

Staatliche Maßnahmen mit Bezug zum Internet wecken regelmäßig, so hat sich zumindest in der jüngeren Vergangenheit beispielsweise bei der Vorratsdatenspeicherung und der Online-Durchsuchung gezeigt, das besondere Interesse der Öffentlichkeit. Die große Angst vor der staatlichen Datengier und den möglichen Grundrechtseingriffen dominiert dabei die gesellschaftliche Diskussion. Dass für eine effektive Gefahrenabwehr und Strafverfolgung staatliche Stellen allerdings in hohem Maße auf Daten angewiesen sind, wird insoweit leicht verdrängt.

Die utopischen Selbstregulierungsvorstellungen des Internet, die sich einen Raum ohne staatliche Einflussnahme wünschen, gehen an der Realität vorbei. Dies stellte unlängst auch Deutschlands oberster Datenschützer, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar, fest, indem er deutlich machte, dass Selbstregulierungsmechanismen die Persönlichkeitsrechte im Internet nicht gewährleisten können[1]. Das „Ob" einer staatlichen Beobachtung des Internet steht damit außer Frage. Vielmehr bedarf das „Wie" der staatlichen Maßnahmen einer genaueren Betrachtung.

Seit nunmehr über 15 Jahren bewegen sich Polizisten auf ihren Streifenfahrten durch das Internet. Ihre Arbeitsmethoden und Aufgabenbereiche mussten sich immer wieder den stetigen Veränderungen des Internet sowie dem sich wandelnden Nutzerverhalten anpassen. In der Öffentlichkeit werden die Ermittlungsmaßnahmen der Polizei im virtuellen Raum kaum wahrgenommen. Dies mag daran liegen, dass der Nutzer im Regelfall, selbst wenn sein Verhalten im Internet beobachtet wird, dies nicht bemerkt. Die Polizeistreifen verhalten sich damit bei ihrer Suche nach rechtswidrigen Inhalten und strafbaren Handlungen unauffällig. Erst wenn konkrete Verdachtsmomente für eine Gefahr oder eine Straftat bestehen, wird der Nutzer dies wahrscheinlich durch die staatlichen Maßnahmen spüren.

Im Rahmen dieser Arbeit soll untersucht werden, ob sich die verdachtsunabhängigen Ermittlungen der Polizei im Internet innerhalb des gesetzlichen Rahmens bewegen. Dabei wird bewusst auf eine Betrachtung der polizeilichen Maßnahmen verzichtet, die dann eingeleitet werden können, wenn sich konkrete Verdachtsmomente, sei es zur Gefahrenabwehr oder zur Strafverfolgung, ergeben. Diese Arbeit will gerade die verdachtsunabhängigen

1 Vgl. die Meldung der vom Deutschen Bundestag eingesetzten „Enquete-Kommission Internet und digitale Gesellschaft" vom 21.02.2011, abzurufen unter *http://www.bundestag.de/dokumente/textarchiv/2011/33500340_kw08_pa_schaar/index.html.*

Ermittlungen der Polizei in den Kommunikationsdiensten und sonstigen Bereichen des Internet beleuchten, die jeden Nutzer treffen können.

In einem ersten Teil wird zunächst die präventive Nutzung des Internet durch die Polizei dargestellt. Im Rahmen dessen werden auch die derzeitigen Tätigkeiten der Polizei bei ihren virtuellen Streifenfahrten vorgestellt. Anschließend werden die technischen Grundlagen des Internet erläutert, um dann die unterschiedlichen Internetdienste, die auch bei der rechtlichen Bewertung eine Rolle spielen, darzustellen. Da aus rechtlicher Sicht nicht alle Daten eine Grundrechtsrelevanz aufweisen, muss die genaue Bedeutung personenbezogener Daten erläutert werden. Im Anschluss werden kurz wesentliche gesellschaftliche Entwicklungen aufgezeigt, die durch das Medium Internet verursacht wurden, und damit zusammenhängende Gefahren erläutert. Der einleitende Teil der Untersuchung wird mit einer kurzen Darstellung der möglichen Maßnahmen der Polizei zur Datenerhebung und Datenverarbeitung im Internet abgeschlossen.

Den Schwerpunkt der Arbeit bildet die rechtliche Überprüfung der verdachtsunabhängigen Ermittlungen der Polizei im virtuellen Raum. Die Maßnahmen der Polizei müssen sich an den verschiedenen Grundrechten messen. Dabei spielt insbesondere das Recht auf informationelle Selbstbestimmung eine wesentliche Rolle. Insoweit muss geprüft werden, ob die in dem Volkszählungsurteil des Bundesverfassungsgerichts[2] entwickelten Grundsätze auch für das sich stets verändernde und weiterentwickelnde Internet anzuwenden sind. Besonderes Augenmerk liegt dabei auf der genauen Unterscheidung und Kategorisierung der unterschiedlichen Internetdienste, um eine praxistaugliche Einordnung vornehmen zu können, in welchen Fällen die Polizei bei ihren verdachtsunabhängigen Ermittlungen im Internet in Grundrechte eingreift. Im Rahmen dessen werden auch neuere Internetdienste, so beispielsweise Soziale Netzwerke wie Facebook, mit ihren Besonderheiten beleuchtet.

Da Grundrechtseingriffe einer gesetzlichen Rechtfertigung bedürfen, wird im Anschluss geprüft, ob die geltenden Gesetze eine ausreichende Grundlage für die untersuchten Ermittlungen der Polizei im Internet darstellen. Abschließend werden die neuen Herausforderungen für den Datenschutz betrachtet, die insbesondere durch den stetig wachsenden gesellschaftlichen Einfluss und die Ausbreitung des Internet auf immer mehr Lebensbereiche bedingt sind. Die in den 1980er Jahren entwickelten Grundsätze des Rechts auf informationelle Selbstbestimmung können heute nicht mehr in der Stringenz und Schärfe gehalten werden. Aus diesem Grund schließt die Arbeit mit dem Versuch, ein Recht auf virtuelle Selbstbestimmung zu entwickeln, welches sich den neuen Umständen des Internet-Zeitalters stellen kann.

2 BVerfGE 65, 1.

B.
Die präventive Nutzung des Internet durch die Polizei

Staatlichen Stellen stehen verschiedene Möglichkeiten zur Verfügung, das Internet zu präventiven Zwecken zu nutzen. Im Folgenden soll dargestellt werden, in welchem Umfang die Polizei das Internet zu präventiven Zwecken tatsächlich verwendet. Die Nutzung des Internet durch die Polizei zu repressiven Zwecken[3] soll dabei ebenso wenig betrachtet werden wie die Maßnahmen zur Gefahrenabwehr, die nicht auf eine direkte Nutzung des Internet selbst zurückzuführen sind, wie beispielsweise Beseitigungsanordnungen[4], Telekommunikationsüberwachungsmaßnahmen[5] und Online-Durchsuchungen[6].

3 Zur Nutzung des Internet zu repressiven Zwecken siehe *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 633 ff.; *Singelnstein*, NStZ 2012, 593 ff.; *Kochheim*, Verdeckte Ermittlungen im Internet, Stand: März 2012, abzurufen unter *http://cyberfahnder.de*; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl., 2012, Rdnr. 758 ff.; *Bär*, MMR 1998, 463 ff.; *Gehde*, DuD 2003, 496 ff.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000; *Valerius*, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, 2004.

4 Zu den Beseitigungsanordnungen und Sperrungen siehe *Sieber/Nolde*, Sperrverfügungen im Internet, 2008; *Schöttle*, K&R 2007, 366 ff.; *Höhne*, jurisPR-ITR 24/2010, Anm. 2; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000; *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, 2001. Für die Realisierbarkeit von Sperrungen und Filtern siehe auch *Schneider*, MMR 2004, 18 ff.

5 Siehe vertiefend zur Telekommunikationsüberwachung *Marberth-Kubicki*, Computer- und Internetstrafrecht, 2. Aufl., 2010, S. 189 ff.; *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, 2009, S. 270 ff. (insb. S. 314 ff.); für die E-Mail-Überwachung siehe zum Zugriff beim Diensteanbieter *Neuhöfer*, Der Zugriff auf serverbasierte gespeicherte E-Mails beim Provider, 2011; zur Gefahrenabwehr siehe *Hsieh*, E-Mail-Überwachung zur Gefahrenabwehr, 2011.

6 Siehe vertiefend zur sog. Online-Durchsuchung *Gudermann*, Online-Durchsuchung im Lichte des Verfassungsrechts, 2010; *Soiné*, NVwZ 2012, 1585 ff.; *Stadler*, MMR 2012, 18 ff.; *Herrmann/Soiné*, NJW 2011, 2922 ff.; *Roggan*, Online-Durchsuchung, 2008; *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 99 ff.; *Leisner*, NJW 2008, 2902 ff.; *Volkmann*, DVBl 2008, 590 ff.; *Britz*, DÖV 2008, 411 ff.; *Kutscha*, NJW 2008, 1042 ff.; *Böckenförde*, JZ 2008, 925 ff.; *Bartsch*, CR 2008, 613 ff.; *Hornung*, CR 2008, 299 ff.; *Stögmüller*, CR 2008, 435 ff.; *Heckmann*, in: Kluth u. a., FS Rolf Stober, 2008, S. 615 ff.; *Bär*, MMR 2008, 325 ff.

I. Polizeilicher Aufgabenbereich

Der polizeiliche Aufgabenbereich lässt sich nach herkömmlicher Auffassung in zwei große Aufgabenkategorien aufteilen: Die präventiv-polizeiliche Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung auf der einen Seite steht neben der repressiven Verfolgung von Straftaten und Ordnungswidrigkeiten auf der anderen Seite („Dualismus polizeilicher Aufgaben“)[7]. Für die polizeiliche Gefahrenabwehr gelten die Aufgaben- und Befugnisnormen in den Polizeigesetzen, während die Strafprozessordnung und das Ordnungswidrigkeitengesetz grundsätzlich für die repressiven Tätigkeitsbereiche der Polizei einschlägig sind[8].

Die Gefahrenabwehr hat die Aufgabe, von dem Einzelnen und dem Gemeinwesen Gefahren abzuwehren, durch die die öffentliche Sicherheit oder Ordnung bedroht wird, und Störungen der öffentlichen Sicherheit oder Ordnung zu beseitigen, soweit es im öffentlichen Interesse geboten ist[9]. Die polizeiliche Gefahrenabwehr ist als verfassungsrechtliche Pflicht des Staates zum Schutz der Funktionsfähigkeit staatlicher Institutionen sowie zum Schutz des Einzelnen bei der Ausübung seiner grundrechtlichen Freiheiten zu qualifizieren[10]. Dies bedeutet, dass der Staat beispielsweise Gefahren für Grundrechte einzelner Bürger im Rahmen seiner Möglichkeiten grundsätzlich beseitigen muss.

Neben den auf den ersten Blick scheinbar leicht abgrenzbaren beiden klassischen Aufgabenbereichen der Polizei gibt es weitere Aufgabenkategorien, die nicht immer eindeutig der Gefahrenabwehr oder der Strafverfolgung zugeordnet werden können[11]. Durch die Übertragung immer neuer Aufgaben im Rahmen der Ausdehnung des freiheitlich-rechtsstaatlichen Sicherheitsauftrags, wie beispielsweise durch Maßnahmen zur vorbeugenden Bekämpfung von Straftaten und zur Vorbereitung auf die Gefahrenabwehr, hat sich die klassische Aufteilung der Aufgabenbereiche nachhaltig geändert[12]. Zudem werden der Polizei durch die moderne Technik Einsatzmittel zur Verfügung gestellt, die neue Möglichkeiten der Gefahrenabwehr und Verbrechensbekämpfung bieten[13]. Insbesondere bei Maßnahmen im

7 Vgl. beispielsweise *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 6. Aufl., 2010, § 7, Rdnr. 7 ff.

8 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 178.

9 Vgl. z. B. § 1 Abs. 1 Satz 1 PolG BW.

10 *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 23.

11 Vgl. z. B. *Denninger*, in: Lisken/Denninger, HbPolR, 5. Aufl., 2012, Kap. D, Rdnr. 1 ff.

12 Hierzu zählen z. B. Maßnahmen zur Datenerhebung und Datenverarbeitung, vgl. *Ruder/Schmitt*, Polizeirecht, 7. Aufl., 2011, Rdnr. 204 ff.; vgl. insgesamt zur Aufgabenerweiterung der Polizei Zöller, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, 2002, S. 77 ff.

13 Vgl. *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 1, Rdnr. 4; vgl. insgesamt zum Wandel des Gefahrenbegriffs im Polizeirecht *Pils*, DÖV 2008, 941 ff.; *Kugelmann*, DÖV 2003, 781 ff.

Vorfeld eines konkreten Tat- oder Gefahrenverdachts ist die Einordnung nicht immer unumstritten[14]. Problematisch ist für diese Vorfeldmaßnahmen, dass die althergebrachten Abgrenzungen für den präventiven Bereich mit dem Gefahren- und Störerbegriff und für den repressiven Bereich mit den Grundbegriffen „Anfangsverdacht" und „Beschuldigter" einer bestimmten Straftat noch keine genauen Ergebnisse liefern können[15]. Aus diesem Grund schlägt beispielsweise Denninger die „Dreiheit der Polizeiaufgaben" vor, bei der neben Gefahrenabwehr und Strafverfolgung die Prävention tritt, die Aufgaben der Straftatenverhütung, der Verfolgungsvorsorge und der Sicherheitsvorsorge (der Vorbereitung auf die Gefahrenabwehr) umfassen soll[16]. Nach allgemeiner Ansicht umfasst aber die Aufgabe der Gefahrenabwehr auch polizeiliche Vorsorgemaßnahmen, die der Verhütung künftiger Straftaten dienen, als wesentlicher Bestandteil einer vorbeugenden Bekämpfung von Straftaten[17]. Davon eingeschlossen sind Maßnahmen zur Verhütung und Verhinderung von zu erwartenden Straftaten, Maßnahmen zur Vorsorge für die Verfolgung von künftigen Straftaten und Vorbereitungshandlungen, um künftige Gefahren abwehren zu können[18].

Ausgehend vom „Dualismus polizeilicher Aufgaben" können nicht immer alle Maßnahmen, gerade im Vorfeld eines konkreten Gefahren- oder Tatverdachts, genau einem der beiden Aufgabenbereiche alleinig zugesprochen werden[19]. Diese sog. doppelfunktionalen Maßnahmen sind kumulativ dem Recht der Gefahrenabwehr und der Strafverfolgung zuzuordnen[20]. Für die Frage, ob die Polizei zur Gefahrenabwehr nach dem Polizeigesetz oder als Ermittlungsbehörde auf dem Gebiet der Strafrechtspflege tätig geworden ist, muss die Maßnahme funktional betrachtet werden, wobei entscheidend das Schwergewicht des polizeilichen Handelns und der damit verbundene

14 Vgl. dazu *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 178 ff.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 243 ff.; *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 10 ff.

15 Vgl. *Denninger*, in: Lisken/Denninger, HbPolR, 5. Aufl., 2012, Kap. D, Rdnr. 2; *Ruder/Schmitt*, Polizeirecht, 7. Aufl., 2011, Rdnr. 204.

16 *Denninger*, in: Lisken/Denninger, HbPolR, 5. Aufl., 2012, Kap. D, Rdnr. 5; vgl. dazu auch *Albers*, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, 2001, S. 252 ff.

17 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 179; *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., 2008, § 17, Rdnr. 21 ff.; *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 1, Rdnr. 4a ff.

18 *Ruder/Schmitt*, Polizeirecht, 7. Aufl., 2011, Rdnr. 204.

19 Die Entnahme einer Gewässerprobe durch die Polizei kann beispielsweise neben der Gefahrenabwehr gleichzeitig der Verfolgung von Umweltstraftaten dienen, vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 188 ff. mit weiteren Beispielen.

20 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 188 ff.

Zweck sind[21]. Die Beurteilung richtet sich dabei nach der Perspektive eines objektiven Beobachters, wie sich für diesen das polizeiliche Handeln seinem Gesamteindruck nach darstellt[22]. Als Sonderfall besteht die Möglichkeit, dass gleichzeitig Maßnahmen der Gefahrenabwehr und Strafverfolgung getroffen werden. Die Maßnahmen stützen sich dann auch auf mehrere Rechtsgrundlagen[23].

Um die polizeilichen Maßnahmen zur verdachtsunabhängigen Ermittlungen im Internet einer Aufgabenkategorie zuordnen zu können, soll zunächst die Vorgehensweise der Polizei kurz dargestellt werden. Die ermittelnden Beamten durchsuchen Webseiten oder Webforen nach etwaigen rechtswidrigen Inhalten, wie beispielsweise kinderpornografischen Bildern oder Videoaufnahmen[24]. Ferner beteiligen sich die Polizisten aktiv in Kommunikationsdiensten, indem sie eigene Beiträge verfassen und mit anderen Nutzern dieser Dienste kommunizieren. Die Beamten handeln dabei, zumindest anfangs, verdachtsunabhängig, also ohne konkrete Verdachtsmomente. Im Rahmen dieser Arbeit wird auch nicht näher auf die sich aus einem möglichen Anfangsverdacht ergebenden weiteren Ermittlungsmaßnahmen eingegangen, da diese nicht mehr den verdachtsunabhängigen Ermittlungen im eigentlichen Sinne zuzurechnen sind, sondern eigenständige polizeiliche Maßnahmen darstellen[25].

Zu prüfen ist nun, welcher Aufgabenkategorie die genannten Maßnahmen zuzuordnen sind. Entscheidend sind dafür das Schwergewicht des polizeilichen Handelns und der damit verbundene Zweck aus der Sicht eines objektiven Beobachters. Ausgangspunkt der verdachtsunabhängigen Ermittlungen ist das Fehlen einer konkreten Gefahr[26]. Sie setzen also im Vorfeld

21 BVerwGE 47, 255, 265; *Knemeyer*, Polizei- und Ordnungsrecht, 11. Aufl., 2007, Rdnr. 122; *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 1, Rdnr. 5; *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 6. Aufl., 2010, Rdnr. 15; *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 189 m. w. N.; a. A. *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 423, der vor allem die Gesichtspunkte zur Bestimmung des Schwerpunktes für zu unklar hält.

22 *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 189.

23 Beispielsweise die erkennungsdienstliche Behandlung eines Ausländers, vgl. *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 1, Rdnr. 5; *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 191.

24 Das BKA bezeichnet seine Maßnahmen als „ständige, systematische, anlassunabhängige, deliktsübergreifende Recherche in Datennetzen, insbesondere im Internet, nach strafrechtlich relevanten Inhalten“, vgl. die Informationen zur Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) unter *http://www.bka.de/*.

25 Zu unterscheiden sind dann die Maßnahmen der Gefahrenabwehr, wie z. B. die Löschung einer Webseite mit rechtswidrigen Inhalten, von den Maßnahmen der Strafverfolgung, wie etwa die weiteren Ermittlungsmaßnahmen gegen einen bestimmten Beschuldigten.

26 Eine konkrete Gefahr kann definiert werden als eine „Sachlage, die bei ungehindertem, nach Prognose der Polizei zu erwartendem Geschehensablauf in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einem Schaden führen kann“, *Würtenberger/Heckmann*, Polizeirecht,

konkreter Gefahren an[27]. Die Polizisten ergreifen selbst die Initiative, um konkrete Gefahren aufzuspüren. Dabei richten sich die Maßnahmen auch nicht gegen bestimmte Personen, sondern es kann grundsätzlich jeden treffen. Ziel der verdachtsunabhängigen Ermittlungen ist es, als ersten Schritt einen Gefahrenverdacht zu schöpfen[28]. Erst in den nächsten Schritten kämen dann weitere Ermittlungsmaßnahmen bis hin zur Löschung oder Sperrung einer Webseite oder gegebenenfalls die Einleitung eines Ermittlungsverfahrens in Betracht. Bei ihrer Verdachtssuche stellt die staatliche Stelle schon bevor sie einen Anlass hat, eine konkrete Gefahr zu vermuten, die elementaren Voraussetzungen künftiger Gefahrenabwehr sicher, indem sie sich die Möglichkeit eröffnet, eine eventuelle Gefahrensituation erstmals zur Kenntnis zu nehmen[29]. In diesem frühen Stadium ihrer Ermittlungen liegt damit eine Maßnahme der Gefahrenvorsorge vor, die der Gefahrenabwehr zuzurechnen ist[30].

Für dieses Ergebnis spricht zudem das zeitliche Nacheinander polizeilicher Maßnahmen[31]. Die polizeiliche Generalklausel für die Strafverfolgung gemäß §§ 161, 163 StPO kann dann einen Eingriff rechtfertigen, wenn ein entsprechender Anfangsverdacht im Sinne des § 152 Abs. 2 StPO[32] für eine Straftat vorliegt. Dieser Anfangsverdacht ist zwar die am wenigsten intensivste Verdachtsstufe[33], jedoch erfordert ein Anfangsverdacht konkrete

6. Aufl., 2005, Rdnr. 411. Vgl. zu ähnlichen Definitionen einer konkreten Gefahr z. B. *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 6. Aufl., 2010; *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., 2008, § 6, Rdnr. 17 ff.; *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 69.

27 Vgl. insgesamt dazu *Wulff*, Befugnisnormen zur vorbeugenden Verbrechensbekämpfung in den Landespolizeigesetzen, 2003, S. 5 ff.

28 Siehe auch zu Maßnahmen der Verdachtsgewinnung im Lichte der Rechtsprechung des Bundesverfassungsgerichts *Bull*, Grundsatzentscheidungen zum Datenschutz bei den Sicherheitsbehörden, in: Möllers/van Ooyen, Bundesverfassungsgericht und Öffentliche Sicherheit, 2011, 65, 86 ff.

29 Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 252, der diese Vorfeldmaßnahmen als „Gefahrenabwehrvorsorge" bezeichnet.

30 Im Ergebnis ebenso *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 252; wohl auch *Bär*, MMR 1998, 463, 465; *Zöller*, GA 2000, 563, 570; *Graf*, DRiZ 1999, 281, 285. Im „analogen" Leben werden Polizeistreifen auch als Maßnahmen der Gefahrenvorsorge eingestuft, vgl. *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 1, Rdnr. 4a.

31 Vgl. insgesamt dazu *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 185; kritisch dazu *Wick*, Gefahrenabwehr – vorbeugende Verbrechensbekämpfung – Legalitätsprinzip, DRiZ 1992, 217, 221 ff.

32 § 152 Abs. 2 StPO begründet die Pflicht der Staatsanwaltschaft, „wegen aller verfolgbaren Straftaten einzuschreiten, sofern zureichende tatsächliche Anhaltspunkte vorliegen".

33 Die intensiveren Verdachtsstufen sind der „hinreichende Tatverdacht" und der „dringende Tatverdacht".

Tatsachen oder zumindest Indizien für eine Tatbegehung[34]. Für die verdachtsunabhängigen Ermittlungen der Polizei im Internet liegt dieser Anfangsverdacht gerade noch nicht vor, da selbst Indizien für eine Tatbegehung regelmäßig fehlen. Zwar sind auch Vorermittlungen zur Klärung der Frage, ob auf Grund vorliegender tatsächlicher Anhaltspunkte die Einleitung eines Ermittlungsverfahrens veranlasst ist, zulässig[35]. Jedoch müssen für Vorermittlungen tatsächliche Anhaltspunkte für eine Straftat bestehen[36]. Aus diesem Grund sind die verdachtsunabhängigen Ermittlungen der Polizei im Internet nicht als Vorermittlungen im strafprozessualen Sinne zu qualifizieren. Die polizeilichen Maßnahmen im Internet könnten allerdings Vorfeldermittlungen sein, die dazu dienen, solche tatsächlichen Anhaltspunkte für eine Tatbegehung erst zu gewinnen[37]. In strafprozessualer Hinsicht sind solche Vorfeldermittlungen aber mangels Anfangsverdachts unzulässig[38]. In diesem frühen verdachtsunabhängigen Ermittlungsstadium können polizeiliche Maßnahmen in zeitlicher Hinsicht noch nicht der Aufklärung von Straftaten und somit der Strafverfolgung dienen, sondern der Verhinderung und Unterbindung von Straftaten[39]. Damit sind die verdachtsunabhängigen Ermittlungen der Polizei im virtuellen Raum Maßnahmen zur Gefahrenabwehr.

II. Polizeistreifen im Internet – die verdachtsunabhängigen Ermittlungen der Polizei

Mit den „virtuellen Streifenfahrten“ versucht die Polizei, einige Bereiche der Kriminalität im Internet zu verhindern beziehungsweise einzuschränken. Diese Aufgabe nehmen die Polizeibehörden nicht erst seit kurzem wahr, sondern erfüllen sie vielmehr bereits seit über 15 Jahren. In dieser Zeit konnten die ermittelnden Beamten einerseits mit den technischen und gesellschaftlichen Entwicklungen des Internet wachsen. Andererseits müssen sich die Behörden immer wieder auf neue, teilweise kaum vorhersehbare Veränderungen des Internet einstellen und diese bei ihrer Arbeit berücksichtigen.

34 Vgl. *Beulke*, StPO, 10. Aufl., 2008, Rdnr. 114; *Meyer-Goßner*, StPO, 53. Aufl., 2010, § 152, Rdnr. 4.

35 Vgl. *Lange*, DRiZ 2002, 264; siehe insgesamt zu Vorermittlungen *Haas*, Vorermittlungen und Anfangsverdacht, 2003; *Lange*, Vorermittlungen, 1999.

36 Vgl. *Wolter*, in: SK-StPO, Vor § 151, Rdnr. 156b; *Pfeiffer*, StPO, 5. Aufl., 2005, § 152, Rdnr. 1c.

37 Siehe insgesamt zu Vorfeldermittlungen *Artzt*, Die verfahrensrechtliche Bedeutung polizeilicher Vorfeldermittlungen, 2000; *Weßlau*, Vorfeldermittlungen, 1989; *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, 2002, insb. S. 77 ff.

38 *Meyer-Goßner*, StPO, 53. Aufl., 2010, § 152, Rdnr. 4a.

39 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 185 m. w. N.; kritisch *Sproß*, NVwZ 1992, 642, 644 ff.

1. Überblick über die Geschichte der Polizeistreifen im Internet

Schon im Jahre 1989 hatte die „Arbeitsgemeinschaft der Leiter der Landeskriminalämter mit dem Bundeskriminalamt“ (AG Kripo) versucht, eine Lösung für das Problem der pornografischen und sonstigen jugendgefährdenden Schriften im Bildschirmtext (Btx) zu finden[40]. Die Übernahme dieser Aufgabe durch eines der Landeskriminalämter – insbesondere durch das LKA Baden-Württemberg – scheiterte zunächst an der Kostenfrage[41].

Im Jahre 1993 wurde auf der 128. Tagung der AG Kripo beschlossen, dass schließlich das Landeskriminalamt Baden-Württemberg in einem Pilotprojekt die Aufgaben einer zentralen Auswertungsstelle für kinderpornografische Medien übernehmen sollte. Im Vorfeld war festgestellt worden, dass zunehmend auch die Neuen Medien zur Verbreitung kinderpornografischer Bilder und Schriften genutzt wurden. Im Abschlussbericht des Landeskriminalamtes Baden-Württemberg vom November 1995 wurde dementsprechend empfohlen, in jedem LKA eine Ansprechstelle für Kinderpornografie einzurichten[42].

Die ersten Polizeistreifen wurden ab Anfang 1995 eingesetzt, um den virtuellen Raum zu überwachen[43]. Sowohl Beamte des Landeskriminalamtes Bayern als auch Beamte des Polizeipräsidiums München (Kommissariat 343) führen seitdem verdachtsunabhängige Ermittlungen im Internet durch[44]. Zu Beginn der Überwachung waren insbesondere die Mailbox-Szene und das Netz Datex-J Ziele der Ermittler[45].

Der damalige Innenminister von Bayern, Günther Beckstein, hatte gefordert, dass auch in den anderen Bundesländern polizeiliche Stellen zur Internetrecherche eingerichtet werden sollten[46]. Mit Beschluss der Innenminis-

40 Vgl. insgesamt zur Geschichte der Polizeistreifen im Internet *Siegert*, Das Internet – Grundlagenwissen für die Polizei, 2002, S. 230 ff. Die Ausarbeitung der Geschichte der Polizeistreifen im Internet von Siegert erfolgte anhand von verschiedenen behördlichen Unterlagen, zu denen der Verfasser keinen Zugang hatte, da diese fast ausschließlich VS-NfD (Verschlusssache – Nur für den Dienstgebrauch bestimmt) sind.

41 Vgl. *Siegert*, Das Internet – Grundlagenwissen für die Polizei, 2002, S. 231.

42 Vgl. insgesamt dazu *Siegert*, Das Internet – Grundlagenwissen für die Polizei, 2002, S. 231 ff.

43 Siehe dazu auch *Bär*, MMR 1998, 463, 464 ff.; *Kant*, CILIP 71 (1/2002), 29 ff.; *Siegert*, Das Internet – Grundlagenwissen für die Polizei, 2002, S. 231; *Steinle*, Die Polizei 2004, 296, 299; *Zöller*, GA 2000, 563, 567 ff. Vereinzelt wurden auch verdachtsunabhängige Ermittlungen in Berlin und Baden-Württemberg durchgeführt, vgl. *Siegert*, Das Internet – Grundlagenwissen für die Polizei, 2002, S. 231.

44 Siehe dazu *www.polizei.bayern.de/schutz/kriminal.index.htm*. Schon im ersten Jahr der Polizeistreifen im Netz wurden allein 172 Fälle mit dem Anfangsverdacht für einen Tatbestand der Verbreitung von Kinderpornografie aufgedeckt, vgl. Süddeutsche Zeitung vom 30.01.1997, Münchener Zeitung vom 30.01.1997, *Grassmann*, Die Welt vom 27.08.1997.

45 So Kriminalhauptkommissar Rainer Richard von der Kripo München in CHIP 5/2003, Internet-Fahnder – Verbrecherjagd im Internet, S. 214.

46 *Kant*, CILIP 71 (17/2002), 29.

terkonferenz auf ihrer 153. Sitzung am 19./20. November 1998 wurde hingegen das Bundeskriminalamt beauftragt, die anlassunabhängigen Recherchen im Internet künftig zentralisiert für das gesamte Bundesgebiet wahrzunehmen[47]. Die Einrichtung einer Zentralstelle beim Bundeskriminalamt war deshalb zweckmäßig, da das Bundeskriminalamt originär eine Zentralstellenfunktion hat[48]. Außerdem sollten so Aufgabenüberschneidungen und doppelte Bearbeitungen überwiegend vermieden werden. Durch einen effektiveren Mittel- und Personaleinsatz sollten zudem die Kosten geringer gehalten werden. Im Januar 1999 wurde daraufhin eine „Zentralstelle für anlassunabhängige Recherchen in Datennetzen" (ZaRD) beim Bundeskriminalamt eingerichtet[49]. Die ZaRD ist ein Bestandteil des beim Bundeskriminalamt in der Abteilung KI eingerichteten „Technischen Servicezentrums für Informations- und Kommunikationstechnik" (TeSIT).

Neben den Ermittlern in Bayern und beim Bundeskriminalamt surfen seit Anfang des Jahres 2005 Beamte des Landeskriminalamtes Baden-Württemberg (Arbeitsbereich Internet-Recherchen AIR) verdachtsunabhängig durch das Internet[50].

Auch andere Landeskriminalämter, wie Rheinland-Pfalz (Zentralstelle für Internetkriminalität, ZFI, seit 2006), Niedersachsen (Anlassunabhängige Recherche in Datennetzen, AuR, seit 2006), Nordrhein-Westfalen (SG 34.3 Zentrale Internet Recherche, ZIR, seit 2007), Hessen (SG 323 IUK/Task Force Internet, TFI, seit 2007) und Sachsen (LKA Sachsen, seit 2011), verfügen mittlerweile über spezielle Rechercheeinheiten, die im Internet nach strafbaren Inhalten suchen[51]. Bund und Länder haben außerdem mittlerweile eine gemeinsame „Koordinierungsgruppe für anlassunabhängige Recherchen im Internet" (KaRIn) eingerichtet[52]. Die Gesamtzahl aller betei-

47 Auch der damalige Bundesinnenminister Otto Schily signalisierte auf einer Tagung des Bundeskriminalamtes, dass die anlassunabhängigen Recherchen im Internet zukünftig zentralisiert vom Bundeskriminalamt durchgeführt werden sollten. Dieser Vorschlag Schilys geht auf eine vom Land Nordrhein-Westfalen initiierte Bundesratsinitiative zurück, die sich für eine Zentralstelle beim Bundeskriminalamt ausgesprochen hatte. Damit sollte insbesondere Bayern künftig keine Möglichkeit mehr geboten werden, die anderen Länder in Fragen der technischen Ausrüstung und Medienkompetenz zu deklassieren. Siehe dazu *www.heise.de/newsticker/meldung/3225*.

48 Zur Zentralstellenfunktion des BKA siehe *www.bka.de/*. Vgl. zum Aufgabenwandel des BKA Abbühl, Der Aufgabenwandel des Bundeskriminalamtes, 2010, sowie zur weiteren Zentralisierung auf das BKA Roggan, NJW 2009, 257 ff.

49 Weitergehende Informationen zur ZaRD sind zu finden unter *www.bka.de/*.

50 Gestartet haben zunächst lediglich fünf Beamte, siehe dazu *www.heise.de/newsticker/meldung/55971*, *www.lka-bw.de/*.

51 Vgl. BT-Drs 17/5835 vom 16.05.2011, S. 2, sowie *http://www.polizei-beratung.de/themen-und-tipps/sexualdelikte/kinderpornografie/polizeiliches-einschreiten.html*.

52 Vgl. BT-Drs 17/5835 vom 16.05.2011 sowie den Vortrag des Präsidenten des Bundeskriminalamtes, *Jörg Ziercke*, auf der BKA-Herbsttagung 2007, abzurufen unter *www.bka.de/*.

ligten Internet-Fahnder wurde 2007 auf rund 350 Beamte geschätzt[53]. Die Mitarbeiterzahl in den einzelnen Zentralstellen von Bund und Ländern lag 2011 zwischen 4 und 45 Mitarbeitern[54].

Die ermittelnden Beamten der Zentralstelle Internetrecherche des Landeskriminalamts Nordrhein-Westfalen haben 2009 über 1.100 Strafverfahren initiiert, wovon rund 500 Kinder-, Jugend-, Gewalt- und Tierpornografie betrafen[55]. 229 Verfahren waren der politisch motivierten Kriminalität zuzurechnen. Den illegalen Handel mit Medikamenten und Betäubungsmitteln hatten 388 Verfahren zum Gegenstand.

Die Polizeibehörden nutzen bei der Suche nach rechtswidrigen Inhalten eigene Suchmaschinen. Dazu wurde etwa das Internet-Ermittlungstool „INTERMIT“ entwickelt. Bei diesem Internet-Ermittlungstool handelt es sich im Kern um eine Meta-Suchmaschine, mit der „weitgehend automatisiert und systematisch das Internet nach verbotenen Inhalten wie etwa rechtsextremistischen oder kinderpornografischen Seiten“ durchsucht werden kann[56]. Danach gleicht es über das Programm PERKEO diese Bilder mit der Datenbank ab, um so bereits bekannte kinderpornografische Inhalte aufzuspüren[57]. Das Programm PERKEO wird ständig in Zusammenarbeit mit dem Bundeskriminalamt erweitert[58].

Für die Terrorismusbekämpfung arbeiten die Polizeibehörden und Nachrichtendienste im „Gemeinsamen Terrorismusabwehrzentrum“ (GTAZ) zusammen[59]. Die Polizeibehörden und Nachrichtendienste sind dabei zwar räumlich auf demselben Gelände angesiedelt, jedoch entsprechend dem Gebot der Trennung von Nachrichtendiensten und Polizei[60] in unterschiedlichen Gebäuden untergebracht. Das „Gemeinsame Internetzentrum“ (GIZ) wird in erster Linie von Vertretern der Sicherheitsbehörden des Bundes gebildet. Die Sicherheitsbehörden werten im Rahmen ihrer Aufgabenerfüllung auch die Inhalte des Internet aus[61]. Dabei werden die Beamten mit großer Wahrscheinlichkeit auch verdachtsunabhängig im Internet ermitteln. Das GTAZ und das GIZ sind allerdings keine eigenen Behörden und die

53 Der Spiegel, 30/2007, 26, 27.

54 Vgl. BT-Drs 17/5835 vom 16.05.2011, S. 2.

55 Vgl. insgesamt dazu das Lagebild Computerkriminalität 2009 des Landeskriminalamtes NRW, S. 5.

56 Pressemitteilung des BSI vom 16.05.2001, zitiert bei Kant, CILIP 71 (1/2002), 29, 34.

57 Zu den Möglichkeiten und Grenzen solcher Spezialsoftware wie PERKEO vgl. *König*, Kinderpornographie im Internet, 2004, S. 231 ff.

58 *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 981.

59 Vgl. insgesamt dazu die Ausführungen unter *http://www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/Sicherheit/Terrorismus/GTAZ.html*; *Weisser*, NVwZ 2011, 142 ff.

60 Vgl. zum Gebot der Trennung von Polizei und Nachrichtendiensten *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 101.

61 Vgl. dazu den 23. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die Jahre 2009 und 2010 vom 12.04.2011, S. 53.

dort tätigen Mitarbeiter unterstehen der Aufsicht und den Weisungen der Behörden, denen sie angehören[62]. Daher ergeben sich im Rahmen dieser Arbeit keine Besonderheiten für die Mitarbeiter der Polizeibehörden, insbesondere des Bundeskriminalamtes, die auch für das GTAZ und GIZ tätig sind.

Nach dem Vorbild des GTAZ wurde im November 2012 das „Gemeinsame Extremismus- und Terrorismusabwehrzentrum" (GETZ) eingerichtet[63]. Ein Teil der Zusammenarbeit zwischen Polizei und Verfassungsschutz auf Bund- und Länderebene betrifft die koordinierte Internetauswertung[64]. Ziel des GETZ ist die Bündelung des Fachwissens der Behörden sowie ein möglichst vollständiger und rascher Informationsfluss, ohne dabei Zuständigkeits- oder Befugnisfragen zu berühren[65].

2. Begriffsbestimmung

Nachdem die Geschichte der virtuellen Polizeistreifen kurz dargestellt wurde, bleibt nun zu klären, was eigentlich die Polizeistreifen im Internet genau unternehmen und wie dies einzuordnen ist. Das Bundeskriminalamt sowie auch die weiteren Landeskriminalämter verwenden für ihre verdachtsunabhängigen Ermittlungen im Internet regelmäßig den Begriff „anlassunabhängige Recherchen". Der Begriff „Recherche" ist in der polizei- und strafrechtlichen Terminologie nicht verwurzelt, weshalb der Begriff „Recherche" eher ungeeignet ist, einen Vorgang, bei dem nach strafbaren Inhalten gesucht wird, lediglich verharmlosend als „Recherche" zu bezeichnen. Soweit in dieser Arbeit „verdachtsunabhängige Ermittlungen" erwähnt werden, stehen diese als Synonym für „anlassunabhängige Recherchen".

Mit Streifenfahrten oder Streifengängen im „analogen" Bereich zeigt die Polizei ihre Präsenz und bietet sich als Ansprechpartner für den Bürger an. Mit den Polizeistreifen soll einerseits eine gewisse Abschreckung erzeugt werden, um Straftaten vorzubeugen und dem Bürger ein Gefühl der Sicherheit zu vermitteln. Andererseits soll mit der Polizeipräsenz erreicht werden, dass nach oder während einer Straftat oder Gefahrensituation schnell und effektiv reagiert werden kann.

Die Polizeistreifen im Internet verfolgen sehr ähnliche Ziele. Die Ermittlungen der ZaRD beim Bundeskriminalamt umfassen die „ständige, systematische, anlassunabhängige, deliktsübergreifende, nicht extern initiierte

62 Vgl. dazu *http://www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/Sicherheit/Terrorismus/GTAZ.html*.

63 Siehe dazu *http://www.bmi.bund.de/DE/Nachrichten/Dossiers/GETZ/getz_node.html*; siehe insgesamt dazu BT-Drs 17/11857.

64 Siehe die Presseinformation des Bundesamtes für Verfassungsschutz zum Start des GETZ vom 15.11.2012, S. 3, abzurufen unter *http://www.verfassungsschutz.de*.

65 Vgl. Presseinformation des Bundesamtes für Verfassungsschutz zum Start des GETZ vom 15.11.2012, S. 1, abzurufen unter *http://www.verfassungsschutz.de*.

Suche nach strafbaren Inhalten im Internet und Online-Diensten, einschließlich der Weiterverfolgung von dabei festgestellten, strafrechtlich relevanten Sachverhalten mit Beweissicherung bis zur Feststellung der Verantwortlichen und/oder der örtlichen Zuständigkeiten von Polizei und Justiz“[66]. Die folgenden Punkte sind die wesentlichen Elemente in der Aufgabenerledigung bei der ZaRD[67]:

– ständige, systematische, anlassunabhängige, deliktsübergreifende Recherche in Datennetzen, insbesondere im Internet, nach strafrechtlich relevanten Inhalten
– Prüfung auf strafrechtliche Relevanz
– Beweiserhebung, -sicherung und -dokumentation
– Verfolgung dieser Straftaten bis zur Ermittlung der örtlich zuständigen Polizeibehörde und entsprechende Abgabe des Vorgangs
– Koordination der Recherchetätigkeit mit den entsprechenden Dienststellen der Landeskriminalämter
– Informationsaustausch und Zusammenarbeit mit anderen öffentlichen und privaten Stellen und Einrichtungen
– Öffentlichkeitsarbeit
– Beteiligung an Aus- und Fortbildungsmaßnahmen

Wesentliches Element der Arbeit der Polizeibehörden ist, dass sie in der Regel verdachtsunabhängig agieren. Zu Beginn ihrer Maßnahme besteht gerade noch kein konkreter Verdacht einer bestimmten Gefahr oder gegen eine bestimmte Person. Zwar reagieren die Behörden auch auf Strafanzeigen oder Hinweise aus der Bevölkerung. Dies wird im Rahmen dieser Arbeit aber nicht genauer untersucht, da bei den genannten Fällen in der Regel keine verdachtsunabhängigen Ermittlungen mehr vorliegen. Soweit bereits ein Anfangsverdacht besteht oder Tatsachen für eine konkrete Gefahr vorliegen, handeln die Polizeibeamten nicht mehr verdachtsunabhängig.

Bei ihren verdachtsunabhängigen Ermittlungen surfen die Polizisten durch das Internet. Sie sind beispielsweise in Tauschbörsen, Chats, Webforen, Blogs, auf Videoplattformen und in Sozialen Netzwerken[68] unterwegs. Hauptaugenmerk beim Bundeskriminalamt liegt auf kinderpornografischen

66 Siehe dazu die Information zur Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) unter *www.bka.de/*.

67 Laut eigener Auskunft unter *www.bka.de/*.

68 Vgl. z. B. die Pressemitteilung des Ministeriums für Inneres und Kommunales des Landes Nordrhein-Westfalen vom 01.03.2011, abzurufen unter *http://www.mik.nrw.de/presse-mediathek/aktuelle-meldungen/archiv/archiv-meldungen-im-detail/news/spezialisierte-lka-ermittler-spueren-erfolgreich-internet-kriminalitaet-auf-innenminister-jaeger.html*. Nach Auskunft der Bundesregierung auf eine Kleine Anfrage ermitteln die Polizeibehörden des Bundes und insbesondere das BKA jedoch nicht anlassunabhängig in den Sozialen Netzwerken, vgl. BT-Drs 17/6587, S. 2. Siehe insgesamt dazu den 23. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die Jahre 2009 und 2010 vom 12.04.2011, S. 86.

Inhalten, die ungefähr 80 Prozent der Fälle ausmachen sollen[69]. Ferner suchen die Polizisten nach sonstigen jugendgefährdenden Inhalten, wie etwa gewaltverherrlichenden Videos oder Computerspielen. Außerdem fahnden die Ermittler nach rechtsextremistischen Inhalten, Beleidigungen, Verbreitung von fremdenfeindlichen Symbolen oder Verabredungen zum Handel mit Betäubungsmitteln[70]. Auch terroristische Aktivitäten und Hacker-Angriffe werden im Internet verfolgt. Zusätzlich sucht die Polizei nach Indizien für bevorstehende Amokläufe, Bombenbau-Anleitungen und sonstigen strafbaren Inhalten[71].

69 Der Spiegel, 30/2007, 26, 27. Vgl. zu den Folgen für den virtuellen Bereich durch die Umsetzung der europäischen Richtlinie über die Bekämpfung der Kinderpornografie *Gercke*, ZUM 2012, 625, 627 m. w. N.

70 Vgl. insgesamt dazu *Henrichs/Wilhelm*, Kriminalistik 2010, 30 ff.

71 Vgl. Der Spiegel, 30/2007, 26 ff.

C.
Die Grundlagen des Internet

I. Die Entstehung des Internet

Das Internet ist ein weltumspannendes Netz der Netzwerke, bei dem die Netzwerke untereinander kommunizieren können. Das im Jahr 1969 ursprünglich als militärisches Kommunikationsnetzwerk konzipierte ARPANET (Advanced Research Projects Agency Network) entwickelte sich in den Folgejahren hin zu einem weltweiten Netzwerk, welches heute insbesondere zu zivilen Zwecken genutzt wird[72].

Am 1. Januar 1983 wurde das gesamte Netzwerk auf das Transmission Control Protocol und das Internet Protocol (TCP/IP) umgestellt. Die Einführung des noch heute gültigen TCP/IP-Standard ebnete dem Internet als verbundener Satz von Netzwerken, die im speziellen den TCP/IP-Standard anwenden, den Weg zum Massenmedium[73].

Ein weiterer wesentlicher Meilenstein für die rasante Entwicklung des Internet war das Domain Name System (DNS). Während man vorher auf der Benutzerebene als Rechneradresse eine Kombination aus Zahlen verwenden musste, konnte nun die Adressierung über symbolische Rechnernamen erfolgen. Eine Adresse wie beispielsweise „shell.de“ lässt sich einfacher eingeben und merken als ein Zahlencode.

Das Projekt ARPANET wurde im Jahre 1990 eingestellt. Zur selben Zeit wurde das WWW (World Wide Web) als vernetztes Hypertext-Projekt für die internationale Zusammenarbeit im Bereich der Hochenergie-Physik am European Laboratory for Particle Physics (CERN) entwickelt[74]. Durch das WWW und die Entwicklung von Navigationssoftware konnten die verschiedenen Internetdienste unter einer einheitlichen gemeinsamen Benutzeroberfläche vereint werden. Diese enorme Vereinfachung der Handhabung führte zu einer unaufhaltsamen Verbreitung des Internet weltweit. Das Internet ist mittlerweile ein weltweiter Zusammenschluss einer unbekannten Anzahl von Rechnern und Netzwerken verschiedener Größenordnung. Die

72 Vgl. zur Geschichte des Internet auch die Darstellungen bei *Finke*, Die strafrechtliche Verantwortung von Internet-Providern, 1998, S. 3 ff.; *Hoeren*, Grundzüge des Internetrechts, 2. Aufl., 2002, S. 9 ff.; *Soiné*, NStZ 1997, 166 ff.; *Haft/Eisele*, JuS 2001, 112 ff.; *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, 1999, S. 15 ff.; vgl. zur Gesetzgebungsgeschichte des Internet *Géczy-Sparwasser*, Die Gesetzgebungsgeschichte des Internet, 2003.

73 Mit der Einführung des TCP/IP-Standards etablierte sich für das ARPANET und die mit ihm verbundenen Netzwerke, die nach diesen Konventionen miteinander kommunizierten, die Bezeichnung „Internet“, s. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 33.

74 Das Projekt wurde 1989 von Robert Cailliau und Tim Berners-Lee vorgeschlagen und 1990 realisiert, vgl. *Haft/Eisele*, JuS 2001, S. 113.

dezentrale Organisationsstruktur des Internet ohne einen Hauptrechner garantiert ein unabhängiges Bestehen dieses Netzes der Netzwerke. Mittlerweile nutzen weltweit über zwei Milliarden Menschen das Internet[75]. Vor ungefähr zwölf Jahren waren es erst ca. 360 Millionen Internet-Nutzer weltweit[76].

II. Die technischen Grundlagen des Internet

Auf der ganzen Welt gibt es eine Vielzahl von Netzen, die unterschiedliche Hard- und Software benutzen. Um diese verschiedenen Netze effizient zu nutzen, ist es notwendig, dass die Netze miteinander verbunden werden können. Dies setzt voraus, dass verschiedene, meist miteinander nicht kompatible Netze zusammengeschlossen werden. Das geschieht vorwiegend mit Geräten namens Gateways, die die für Hardware und Software erforderliche Übersetzung übernehmen und die Verbindung herstellen. Man bezeichnet eine Gruppe miteinander verbundener Netze als Internetworks oder Internet[77].

Bei dem öffentlichen Internet handelt es sich um ein weltweites Computernetzwerk, bei dem Millionen von Computern in aller Welt miteinander verbunden sind. Das Internet stellt somit einen speziellen Fall eines Internetworks dar. Die meisten der Computergeräte, die über das Internet miteinander verbunden werden, sind Desktop-PCs und mobile Endsysteme (Notebooks, Mobiltelefone etc.) und sogenannte „Server", auf denen Informationen, wie beispielsweise WWW-Seiten und E-Mail-Nachrichten, gespeichert sind und übertragen werden können[78]. Seit einiger Zeit werden aber auch nicht traditionelle Computergeräte, wie beispielsweise Web-Fernseher, Personenrufsysteme (Pager) und selbst Toaster an das Internet angeschlossen. Im Internet-Jargon bezeichnet man all diese Geräte als Hosts oder Endsysteme[79].

1. Die Netz-Software

Bei der Konzeption der ersten Rechnernetze wurde vorwiegend auf die Hardware geachtet. Die Netz-Software spielte nur eine untergeordnete Rolle. Heute ist die Netz-Software hochstrukturiert, weshalb ihre Bedeutung für Rechnernetze enorm gewachsen ist. Um die Komplexität bei der Datenüber-

75 Am 30.06.2012 nutzten ca. 2,4 Milliarden Menschen weltweit das Internet, Quelle: *www.internetworldstats.com*.

76 Am 31.12.2000, Quelle: *www.internetworldstats.com*.

77 Der Terminus „Internetwork" bezeichnet im allgemeinen Sinne den Zusammenschluss von Netzwerken. Der Terminus „Internet" meint hingegen das weltweite Internet.

78 Vgl. *Kurose/Ross*, Computernetzwerke, 4. Aufl., 2008, S. 23.

79 Man nennt sie Hosts, weil sie sozusagen die Wirte für Anwendungsprogramme wie Web-Browser oder Serverprogramme sind.

tragung zwischen unterschiedlichen Rechnersystemen zu systematisieren, sind die meisten Netze als mehrere übereinander liegende Schichten oder Ebenen aufgebaut[80]. Hierbei unterscheiden sich Anzahl, Bezeichnung, Inhalt und Funktion der einzelnen Schichten von Netz zu Netz. Die Schichten haben immer den Zweck, den jeweils höheren Schichten bestimmte Dienste zur Verfügung zu stellen, diese Schichten aber von Einzelheiten, wie die Dienste angeboten oder implementiert werden, abzuschirmen[81]. Die Datenkommunikation wird dadurch also portioniert.

Das TCP/IP-Referenzmodell[82] bildet mit seinen vier Schichten und seinen vielfältigen Protokollen heutzutage die Basis für das Internet. Benannt ist das TCP/IP-Referenzmodell nach den zwei wichtigsten Protokollen TCP (Transmission Control Protocol) und IP (Internet Protocol)[83]. Es gibt heute eigentlich nur wenige Anwendungsbereiche, in denen das komplexere sogenannte ISO-OSI-Referenzmodell noch gefordert ist[84].

2. Die Adressierung im Internet

Im Internet wird eine Adressierungsstruktur benutzt, um eine möglichst effiziente Vermittlung der zu übertragenden Pakete über mehrere Teilnetzwerke hinweg zu gewährleisten. Die Internetadressen geben darüber Auskunft, wer der betreffende Netzteilnehmer ist, wo er sich befindet und über welche Übertragungswege er erreichbar ist. Eine solche IP-Adresse besteht nach dem derzeit noch hauptsächlich verwendeten IPv4[85] aus 4 Bytes (32 Bits), durch die jedes Endsystem (Host) im Internet global eindeutig identifiziert werden kann[86]. IP-Adressen werden oft als Folge von 4 Dezimalzahlen ange-

80 Vgl. zu Netzwerkprotokollen beispielsweise *Peterson/Davie*, Computernetze, 4. Aufl., 2008, S. 19 ff.; *Stein*, Taschenbuch Rechnernetze und Internet, 2. Aufl., 2004, S. 25 ff.

81 Diese hierarchischen Schichtenmodelle folgen daher dem Julius Cäsar zugesprochenen Prinzip des *Divide et impera!* (lat. für: Teile und herrsche!). Bei den Schichtenmodellen ist die Kommunikation zur besseren Gliederung und zur Erstellung eines modularen Systems in funktionale Elemente aufgeteilt.

82 Teilweise wurde dieses Referenzmodell auch als DoD-Referenzmodell bezeichnet, da es vor über zwanzig Jahren vom US Department of Defense (DoD) entwickelt wurde. Weiterführendes zum TCP/IP-Referenzmodell ist beispielsweise zu finden bei *Hein*, TCP/IP, 6. Aufl., 2002; *Santifaller*, TCP/IP und ONC/NFS, 4. Aufl., 1998.

83 Vgl. ausführlich dazu z. B. *Tanenbaum*, Computernetzwerke, 4. Aufl., 2003, S. 54 ff.

84 Das ISO-OSI-Referenzmodell wurde 1983 von der „International Standard Organisation" (ISO) beschlossen. „OSI" steht für „Open Systems Interconnection". Vgl. insgesamt dazu beispielsweise *Tanenbaum*, Computernetzwerke, 4. Aufl., 2003, S. 54 ff. In der Praxis gab es allerdings nur wenige erfolgreiche Umsetzungen dieses Modells, vgl. *Sieber*, in: Hoeren/Sieber, Hdb. Multimedia-Recht, Teil 1, Rdnr. 41.

85 Internet Protocol Version 4 (IPv4).

86 Jede Adresse besteht dabei aus zwei Teilen: der Netzidentifikation (Net-ID) und der Benutzeridentifikation (Host-ID oder User-ID). Es gibt fünf verschiedene Klassen von Internetadressen, nämlich A, B, C, D und E. Diese unterscheiden sich durch die Länge der Felder Netzidentifi-

geben, die durch Punkte getrennt sind[87]. Auf Grund des enormen Wachstums des Internet und der Vielzahl neuer, multimedialer Anwendungen wurde Anfang der neunziger Jahre klar, dass das InternetProtocol in wesentlichen Punkten überarbeitet werden muss[88]. Im Rahmen dieser Überarbeitung wird der Adressraum erweitert, da dieser ansonsten den Anforderungen der Zukunft nicht gerecht werden kann. Mit der Umstellung der Adresslänge von 32 Bits auf 128 Bits erhöht sich die Anzahl der möglichen Adressen auf 2^{128} (entspricht 10^{38} Adressen). Der Übergang von IPv4 zu IPv6 kann allerdings nur schrittweise über einen langen Zeitraum erfolgen[89].

3. Das Domain-Name-System

Zur leichteren Handhabung wird jeder Internetadresse ein Name zugeordnet. Hierfür wurde das Domain-Name-System (DNS) entwickelt[90]. Das ab 1986 eingesetzte DNS ist eine verteilte Datenbank, die die Abbildung von Host-Namen zu IP-Adressen bereitstellt[91].

Der Adressname gliedert sich im DNS wie bei der numerischen Schreibweise in einen Benutzeridentifikationsteil (Host-ID oder User-ID) und einen Netzidentifikationsteil (Net-ID), der als Domain-Name bezeichnet wird. Zu jeder Domain gibt es in der Regel mindestens eine Sub-Domain. Diese Sub-Domains sind der Hauptdomäne (Top-Level-Domain) hierarchisch untergeordnet[92]. Der Domain-Name besteht somit aus einer Top-Level-Domain (der am weitesten rechts befindliche Name) sowie aus Sub-Domains[93].

Die Top-Level-Domains sind in zwei große Bereiche, nämlich Allgemeines (Generic) und Länder (Countries), unterteilt. Allgemeine Domains sind beispielsweise *com (commercial)*, *edu (educational)*, *net (Netzbetreiber und*

kation bzw. Benutzeridentifikation. Eine Aufstellung der fünf Klassen von Internetadressen wird dargestellt von *Kyas/Campo*, Internet professionell, 2. Aufl., 2001, S. 83.

87 Dotted decimal notation. Beispielsweise 194.148.652.73.

88 Eine ganze Reihe von Arbeitsgruppen der IETF (Internet Engineering Task Force) beschäftigte sich aus diesem Grund seit 1992 mit Verbesserungsvorschlägen. Auf der Jahrestagung der IETF im Juli 1994 wurde schließlich die neue Version des Internet-Protocol IPv6 (oder auch IPng= next generation) verabschiedet. Die Details zum IPv 6 sind beispielsweise zu finden bei *Braun*, IPnG: Neue Internet-Dienste und virtuelle Netze, 1999, S. 55 ff.

89 Vgl. z. B. *Kurose/Ross*, Computernetzwerke, 4. Aufl., 2008, S. 399 ff.; *Peterson/Davie*, Computernetzwerke, 4. Aufl., 2008, S. 325.

90 Vertiefend zum DNS siehe *Meinel/Sack*, WWW, 2004, S. 578 ff.; *Kurose/Ross*, Computernetze, 4. Aufl., 2008, S. 160 ff.

91 Bei dem DNS handelt es sich eigentlich um einen Internetdienst. Auf Grund der engen Verflechtung zur Adressierung im Internet wird allerdings schon an dieser Stelle das DNS beschrieben.

92 Eine anschauliche Darstellung des DNS in Baumform befindet sich in Tanenbaum, Computernetzwerke, 4. Aufl., 2003, S. 633.

93 Ein Beispiel für einen Domain-Namen ist „*yahoo.de*“. Die einzelnen Adressteile werden beim DNS durch einen Punkt unterteilt.

-anbieter), *int (internationale Organisationen)* und *museum (Museen)*. Bei den geographischen Top-Level-Domains für Länder gibt es zum Beispiel *de (Deutschland)*, *us (USA)*, *jp (Japan)* oder *uk (Großbritannien)*. Die Sub-Domains sind grundsätzlich frei wählbar[94]. Insbesondere im kommerziellen Bereich hat sich daher durchgesetzt, einfach den Firmen- oder Produktnamen als Sub-Domain-Namen zu verwenden, soweit dieser noch nicht besetzt ist[95].

Die Vergabe der Top-Level-Domains wird zentral von der ICANN (Internet Corporation for Assigned Names and Numbers) durchgeführt[96]. Die Verwaltung einer Top-Level-Domain und die Vergabe von Domains unterhalb dieser Top-Level-Domain werden von einer dediziert zuständigen Organisation wahrgenommen. In Deutschland ist das DENIC e.G. (Deutsches Network Information Center) für die Top-Level-Domain „*de*“ verantwortlich[97]. Generell gilt, dass eine neue Domain immer nur mit Zustimmung der nächsthöheren Domain eingerichtet werden kann. Damit kann jedes Unternehmen, das im Besitz einer Domain ist, vollkommen frei eine Hierarchie dieser Domain untergeordneter Sub-Domains selbst gestalten[98].

4. Die verschiedenen Internetdienste

Der eigentliche Sinn und Zweck des Internet besteht in den zur Verfügung gestellten Anwendungen, die auf den Diensten, die das Internet bereitstellt, basieren[99]. Der Begriff Internetdienste fasst alle Dienste (Anwendungen) zusammen, die im Schichtenmodell oberhalb von TCP/IP eingeordnet sind[100]. In den frühen Jahren des Internet, in denen nur einige wenige das neue Medium Internet nutzten, waren drei grundlegende Dienste für die Nutzung des Internet ausreichend: Die Versendung von elektronischen Nachrichten (E-Mail), die Übertragung von Dateien (File Transfer Protocol, FTP) und die Fernbedienung von Computern über das Internet (Telnet).

Ende der achtziger Jahre mussten neue, leistungsstärkere Benutzerschnittstellen geschaffen werden, um die stetig wachsende Informationsflut, die durch rasch wachsende Benutzerzahlen und exponentiell ansteigende

94 Vgl. zum Domainrecht beispielsweise *Viefhues*, in: Hoeren/Sieber, Hdb. Multimedia-Recht, Teil 6.1.

95 Beispielsweise *„audi.de“*, *„focus.de“*.

96 Siehe zur Rechtsnatur, Struktur und Aufgaben der ICANN *Keber*, in: Dörr/Kreile/Cole, Hdb. Medienrecht, 2. Aufl., 2011, Kap. M, Rdnr. 14 ff.

97 Siehe zu den neu zu vergebenden Top-Level-Domains im Jahr 2011 *Maaßen/Hühner*, MMR 2011, 148 ff.

98 Ein Unternehmen kann beispielsweise für jede Abteilung Sub-Domains anlegen.

99 Eine umfassende Darstellung der Internetdienste in technischer Hinsicht ist zu finden bei *Kurose/Ross*, Computernetzwerke, 4. Aufl., 2008, S. 125 ff.; *Stein*, Taschenbuch Rechnernetze und Internet, 2. Aufl., 2004, S. 419 ff.

100 Vgl. *Stein*, Taschenbuch Rechnernetze und Internet, 2. Aufl., 2004, S. 419.

Datenmengen forciert wurde, zu bewältigen. So sind unabhängig voneinander WAIS (Wide Area Information Server), ein System, das die einfache Volltextsuche in weltweit verteilten Datenbeständen ermöglicht, und Archie, ein internetweites Dateiensuchsystem, entstanden. Außerdem waren mittels IRC (Inter Relay Chat) interaktive Diskussionsrunden per Computertastatur möglich und dank Gopher konnte das Internet auf der Basis von verschachtelten Verzeichnisstrukturen durchkämmt werden. Für all diese Dienste waren aber unterschiedliche Bedienoberflächen notwendig. Wenn jemand die verschiedenen Dienste im Internet nutzen wollte, musste er bis Anfang der neunziger Jahre eine Vielzahl von unterschiedlichen Programmen mit ebenso vielen unterschiedlichen Bedienoberflächen benutzen. Im Jahre 1993 erfolgte dann der Durchbruch des WWW (World Wide Web), der heute im Internet üblichen Benutzeroberfläche, mit der per Mausklick das gesamte Internet durchforscht werden kann. Die dafür entwickelten Programme werden Internet-Browser oder WWW-Browser genannt[101].

Im Folgenden werden insbesondere die Internetdienste dargestellt, die im Rahmen dieser Arbeit eine besondere Relevanz haben. Die weiteren Internetdienste werden vorgestellt, soweit sie in der Praxis besonders häufig genutzt werden.

4.1 Electronic Mail Service (E-Mail)

Der wohl älteste populäre und heute neben dem WWW meistgenutzte Dienst im Internet ist die elektronische Post, der sogenannte Electronic Mail Service (E-Mail)[102]. E-Mail ist ein Kommunikationsmittel zwischen zwei oder mehreren Personen, das neben reinem textbasierten Informationsaustausch die Übertragung multimedialer Dateien gestattet[103]. Letztendlich handelt es sich bei einer E-Mail um eine Nachbildung der herkömmlichen Briefpost auf der Basis moderner, digitaler Kommunikationsmittel. Bei einem E-Mail-Dienst handelt es sich um eine einfache Art der asynchronen Kommunikation[104]. Die ersten E-Mail-Systeme existierten bereits kurz nach dem Start des ARPANET und bestanden lediglich aus einem Dateitransferprogramm zusammen mit der Konvention, dass die erste Zeile jeder zu versendenden Nachricht mit der Adresse des Empfängers zu starten hat. Heute gehört E-Mail als Kommunikationsmedium sowohl geschäftlich als auch

101 *Tim Berners-Lee* programmierte den ersten WWW-Browser mit dem Namen World Wide Web auf einem NeXT-Rechner. Weihnachten 1990 fertiggestellt, wurde das Programm bereits ab März 1991 im Kernforschungszentrum CERN eingesetzt. Damit begann der Siegeszug des WWW.

102 Ausführlicher wird der Electronic Mail Service behandelt bei *Kurose/Ross*, Computernetze, 4. Aufl., 2008, S. 146 ff.; *Tanenbaum*, Computernetzwerke, 4. Aufl., 2003, S. 640 ff.

103 *Gergen*, Internetdienste, 2002, S. 91.

104 Vgl. *Kurose/Ross*, Computernetze, 4. Aufl., 2008, S. 146.

privat zu den am häufigsten verwendeten Diensten. Bereits im Jahr 1995 wurden in Deutschland etwa 6 Milliarden elektronische Sendungen (Fax, E-Mail) über Datennetze und etwa 9 Milliarden Postbriefe über herkömmliche Wege transportiert. Schon im Jahr 2000 hatte sich dieses Verhältnis umgekehrt. Nach Schätzungen der Post AG wurden mehr als 13 Milliarden elektronische Sendungen gegenüber 6 Milliarden herkömmlichen Briefsendungen verschickt[105]. Die E-Mail-Zahlen aus dem Jahr 2010 dürften die enorme Verbreitung von E-Mail-Diensten verdeutlichen: 2010 wurden weltweit ca. 107 Billionen E-Mails versandt[106]. Davon waren allerdings fast 90 Prozent sogenannte Spam-Nachrichten, also hauptsächlich Werbe-Mails[107].

Elektronische Nachrichten können abgespeichert werden, an große Gruppen adressiert werden, an andere Personen weitergeleitet werden, Multimediadokumente (z. B. Bild-, Ton- oder Videodateien) enthalten oder weiterverarbeitet werden.

Neben all diesen Vorteilen hat das E-Mail-System aber auch Nachteile. Es gibt verschiedene Möglichkeiten, ein E-Mail-System für Attacken auf Personen oder Unternehmen zu missbrauchen. So können beispielsweise Viren über E-Mails importiert werden oder Spam-Nachrichten (unaufgeforderte Werbung) Kosten für ein Unternehmen verursachen, da ein Mitarbeiter eine gewisse Zeit benötigt, um diese Spam-Nachrichten zu bearbeiten bzw. zu löschen[108]. Zudem ist es auch möglich, E-Mail-Adressen beim Versand zu fälschen[109].

Das Prinzip eines E-Mail-Systems basiert auf zwei Komponenten, nämlich dem User Agent (UA) und dem Message Transfer Agent (MTA)[110]. Als User Agents werden Systeme bezeichnet, mit denen der Anwender Nachrichten erzeugen, editieren, lesen, senden und empfangen kann[111]. Message Transfer Agents sind für den Transport der Nachrichten vom Sender zum Bestimmungsort verantwortlich. Damit die Nachrichten ihr Ziel erreichen, müssen oftmals mehrere MTAs zusammenarbeiten. Hierzu wird ein spezielles Kommunikationsprotokoll, nämlich das Simple Mail Transfer Protocol (SMTP)

105 Die Zahlen stammen aus *Kyas/Campo*, Internet professionell, 2. Aufl., 2001, S. 135.

106 Vgl. SPIEGEL ONLINE vom 18.01.2011, *http://www.spiegel.de/netzwelt/web/0,1518,740121,00.html*.

107 Vgl. SPIEGEL ONLINE vom 18.01.2011, *http://www.spiegel.de/netzwelt/web/0,1518,740121,00.html*.

108 Weitere Möglichkeiten für E-Mail-Attacken auf Personen oder Unternehmen sind Mailbomben, anonyme Belästigungsmails oder das unberechtigte Verwenden des Mailservers. Eine Darstellung der Missbrauchsmöglichkeiten ist zu finden bei *Janowicz*, Sicherheit im Internet, 2002, S. 114 ff.; *Gergen*, Internetdienste, 2002, S. 127 ff.

109 Siehe dazu *Sieber*, in: Hoeren/Sieber, Hdb. Multimedia-Recht, Teil 1, Rdnr. 114.

110 Ein System, das die zwei grundlegenden Komponenten UA und MTA enthält, wird als Message Handling System (MHS) bezeichnet.

111 Der UA könnte letztlich auch als E-Mail-Editor bezeichnet werden. Als Beispiel sei der multimediale Alleskönner Microsoft Outlook genannt.

genutzt[112]. Um die verschiedenen E-Mails zu speichern, benötigt ein Anwender eine Art Briefkasten, der Mailbox genannt wird. Der Anwender kann dann die eingegangenen E-Mails über einen E-Mail-Client aus der Mailbox abrufen. Um den unberechtigten Zugriff auf die Mailbox zu verhindern, muss sich der Anwender gegenüber seinem elektronischen Postfach über Benutzeridentifikation und Passwort ausweisen[113].

Für die verdachtsunabhängigen Ermittlungen der Polizei im virtuellen Raum sind E-Mails in der Regel irrelevant, da E-Mails der gezielten Kommunikation mit einem oder mehreren Adressaten dienen. Die Postfächer, in denen die Nutzer ihre E-Mails speichern, sind zudem nicht öffentlich zugänglich.

4.2 File Transfer Protocol (FTP)

In den Zeiten, als es noch keine Computernetzwerke gab, konnten Daten zwischen verschiedenen Rechnern nur mit transportablen Speichermedien wie beispielsweise Disketten oder Magnetbändern ausgetauscht werden. Zur Zeit des ARPANET wurde das auch heute noch verbreitete File Transfer Protocol (FTP) entwickelt. Mit dem FTP können im Internet Dateien sämtlicher Art (Text-, Bild-, Video-, Ton-, Programmdateien etc.) zwischen zwei Rechnern übertragen werden. Das FTP arbeitet nach dem Client/Server-Modell. Ein FTP-Server stellt dabei Dateien zur Verfügung, die über einen FTP-Client angefordert werden können. Im Vergleich zu anderen Internetdiensten, wie E-Mail oder HTTP, arbeitet das FTP effektiver und zuverlässiger, da es speziell für diese Aufgabe optimiert wurde[114].

4.3 World Wide Web (WWW)

Das WWW ist heutzutage der Internetdienst, der das Internet am stärksten prägt[115]. Durch das WWW scheinen dem Nutzer schier unbegrenzte Möglichkeiten zur Gestaltung offenzustehen. Schon zu Beginn der neunziger Jahre standen dem Benutzer durch das WWW Daten vom anderen Ende der Welt mit einem Mausklick zur Verfügung. Aus Sicht des Benutzers besteht das WWW aus einer scheinbar unendlich großen weltweiten Sammlung von Dokumenten, die Seiten (Pages) oder Webseiten genannt werden.

Mit dem WWW konnten sich aber auch die Inhalte im Internet ändern. Was bis dahin aus dem Netz kam, war textbasiert, bestenfalls aufgelockert mit einigen einfachen Grafiken. Webseiten hingegen gestatten eine fast beliebige Formatierung und die Einbindung von komplexen Grafiken, Fotos oder Videos. Der Hauptgrund für die enorme Verbreitung des WWW ist der

112 Das SMTP ist eine vereinfachte Version eines früheren Transportprogrammes, dem Mail Transfer Protocol (MTP).

113 Die Benutzeridentifikation wird auch User-ID oder Benutzername genannt.

114 *Sieber*, in: Hoeren/Sieber, Hdb. Multimedia-Recht, Teil 1, Rdnr. 131.

115 Vertiefend zum WWW beispielsweise *Kurose/Ross*, Computernetze, 4. Aufl., 2008, S. 125 ff.; *Meinel/Sack*, WWW, 2004; *Tanenbaum*, Computernetzwerke, 4. Aufl., 2003, S. 664 ff.

geradezu revolutionäre Bedienkomfort. Praktisch alle neu im Internet hinzukommenden Daten werden heute in WWW-konformer Darstellung aufbereitet. Ein sehr großer Teil des Internet besteht daher heute aus WWW-Dokumenten, da viele bestehende Informationsarchive in dieses Format umgewandelt wurden. Dies führt dazu, dass für viele das WWW gleichbedeutend mit dem Internet ist.

Die Funktionsweise des WWW basiert auf dem Prinzip des Hypertext[116]. Bei den Hypertextdokumenten handelt es sich um Textdateien, die über Schlüsselwörter, die sogenannten Hyperlinks, mit einem oder mehreren anderen Dokumenten vernetzt sind[117]. Die Hyperlinks sind in besonderer Weise aus dem übrigen Text hervorgehoben. Wenn man nun einen solchen Hyperlink aktiviert (beispielsweise durch einen Mausklick), wird man automatisch zum betreffenden Dokument geführt. So ist es möglich, von einem Dokument zum nächsten zu gelangen und dabei Dokumente, die sich an völlig unterschiedlichen Orten im Internet befinden, aufzurufen. Auf diese Art und Weise durchziehen vernetzte WWW-Hypertextdokumente wie ein virtuelles Spinnengewebe das gesamte Internet[118]. Es können aber nicht nur Textdateien miteinander verbunden werden. Sämtliche multimedialen Dateien können mittels Hypertext miteinander vernetzt werden[119].

Um einen unkomplizierten und schnellen Abruf von Dateien zu erreichen, sind gewisse Standards notwendig. Die Architektur des WWW basiert auf den drei Standards HTML (Hypertext Markup Language), HTTP (Hypertext Transport Protocol)[120] und URL (Uniform Resource Locator). Jeder Seite wird ein URL zugewiesen, der als weltweiter Name gilt. Ein URL besteht aus drei Teilen:

- das Protokoll (auch Schema genannt), das benutzt werden muss, um auf das betreffende Objekt zugreifen zu können,
- die Internetadresse und Portnummer des Serversystems, auf dem sich die Seite befindet,
- der Pfad und ein eindeutiger Name der spezifischen Seite (normalerweise der Dateiname).

116 Hypertext ist eine seit den sechziger Jahren bekannte Methode, um zusammengehörende Dokumente miteinander zu verbinden. Es bestehen sehr starke Ähnlichkeiten zur Arbeitsweise des menschlichen Gehirns.

117 Ein Hyperlink, oder kurz Link, kann man auch als Zeiger zu einer anderen Webseite bezeichnen.

118 Ein Beispiel für die Funktionsweise des WWW: In einem Artikel über den Börsengang eines Unternehmens ist der Name des Unternehmens hervorgehoben. Wenn man diesen anklickt, wird man auf die Homepage des Unternehmens geführt.

119 So können beispielsweise auch Ton-, Bild- oder Videodateien über Hyperlinks erreicht werden. Diese Dokumente werden dann Hypermediadokumente genannt.

120 Genauere Informationen zum HTTP bieten z. B. *Kurose/Ross*, Computernetze, 4. Aufl., 2008, S. 125 ff.; *Tanenbaum*, Computernetzwerke, 2003, S. 706 ff.

Das Format eines URL ist demnach

Zugriffsmethode://Server-Name[Port:]/Inhaltsverzeichnis/Dateiname.

Mittels der verschiedenen URL ist es möglich, unkompliziert und zielsicher durch das Internet zu surfen.

HTML ist die Sprache, in der Webseiten geschrieben werden[121]. Damit können Benutzer Webseiten erstellen, die Text, Grafik und Hyperlinks auf andere Webseiten enthalten. Bei HTML handelt es sich um eine sogenannte Markup-Sprache[122]. Das HTTP ist das Standardübertragungsprotokoll im WWW[123]. Durch das HTTP werden Milliarden von Einzeldokumenten, also einzelnen Webseiten, koordiniert[124].

4.3.1 Öffentlich zugängliche Inhalte des WWW

Für die verdachtsunabhängigen Ermittlungen der Polizei im virtuellen Raum ist das WWW mit seinen Webseiten der wichtigste Internetdienst. Ein Großteil der Webseiten des WWW ist öffentlich zugänglich. Diese Bereiche unterliegen keiner Zugangsbeschränkung. Nutzer können sie ohne Registrierung oder sonstige Berechtigung unbeschränkt besuchen. Die Polizei kann diese Inhalte, wie jeder andere Nutzer auch, grundsätzlich frei aufrufen. Die Polizisten können beispielsweise Webseiten im Internet abrufen, die Informationen zu Unternehmen, Vereinen oder sonstigen Gruppen enthalten. Angebote von Zeitschriften und Zeitungen oder sonstige frei zugängliche Inhalte von Presseorganen können die staatlichen Stellen ebenfalls einsehen. Für die Arbeit der Polizei können zum Beispiel die Kommentarfunktionen zu Artikeln relevant sein. Durch die Kommentarfunktionen können Leser des Artikels – oft ohne vorherige Registrierung und Angabe ihres Klarnamens – den Inhalt des Artikels kommentieren. Die Polizei kann außerdem private Webseiten und Blogs aufrufen, soweit diese ohne Zugangsbeschränkungen einsehbar sind.

4.3.2 Geschützte Inhalte des WWW

Neben den öffentlich zugänglichen Bereichen des WWW sind bestimmte Webseiten nur einem beschränkten Nutzerkreis zugänglich. Hierbei kann es sich beispielsweise um Mitgliederbereiche auf Webseiten, bestimmte Webforen oder um Soziale Netzwerke handeln. Der Modus der Zugangsbeschränkung ist dabei unterschiedlich ausgestaltet. In der Regel wird einem Nutzer nur dann Zutritt zum geschützten Bereich gewährt, wenn er den richtigen Benutzernamen und das zugehörige Passwort eingibt.

---

121 Weiterführendes zu HTML ist zu finden bei *Meinel/Sack*, WWW, 2004, S. 805 ff.

122 HTML selbst wurde aus dem Standard SGML (Standard Generalized Markup Language) entwickelt und ähnelt anderen Markup-Sprachen wie beispielsweise LaTex oder troff.

123 Genauere Informationen zum HTTP bieten z. B. *Kurose/Ross*, Computernetze, 4. Aufl., 2008, S. 125 ff.; *Tanenbaum*, Computernetzwerke, 2003, S. 706 ff.

124 *Sieber*, in: Hoeren/Sieber, Hdb. Multimedia-Recht, Teil 1, Rdnr. 80.

In den meisten Fällen erfolgt die Registrierung, um einen geschützten Bereich einsehen zu können, über die Angabe eines frei gewählten Benutzernamens oder einer Benutzeridentifikation und einer E-Mail-Adresse. Im Anschluss wird automatisch an die angegebene E-Mail-Adresse das Passwort für den Abruf der geschützten Inhalte gesandt. Alternativ wird häufig vom Nutzer verlangt, dass er bereits bei der Registrierung ein eigenes Passwort auswählt. Um dies zu authentifizieren, erhält er im Anschluss eine E-Mail mit einem Link, den er abrufen muss. Danach ist sein Zugang freigeschaltet.

Die Erteilung der Zugangsberechtigung kann auch auf viele weitere Weisen erfolgen[125]. Die meisten Zugangsberechtigungssysteme verlangen allerdings keine Verifizierung der Angaben des Nutzers. Der Diensteanbieter überprüft nicht, ob der gegebenenfalls anzugebende Name, die Anschrift oder die E-Mail-Adresse des Nutzers wahrheitsgemäß sind.

Einige Diensteanbieter sehen besondere Schutzmechanismen zur Identitätsfeststellung vor, um bestimmte Inhalte zu schützen. Durch besondere Registrierungsmaßnahmen wollen die Diensteanbieter die Identität der interessierten Nutzer verifizieren. Hierfür können sie beispielsweise Chipkarten, Ausweise, das sogenannte Post-Ident-Verfahren[126], biometrische Verfahren oder in Zukunft den elektronischen Personalausweis einsetzen[127]. Von dem interessierten Nutzer kann zum Beispiel gefordert werden, dass er seinen Personalausweis direkt oder eine beglaubigte Kopie vorzulegen hat. Der Diensteanbieter kann so, je nach Ausgestaltung des Authentifizierungsvorganges, den Namen des Nutzers und gegebenenfalls weitere Daten genau überprüfen. Daran anknüpfend kann er entscheiden, ob der interessierte Nutzer Zugang zu den geschützten Inhalten erhält.

Um kostenpflichtige Dienste abzurechnen, verlangen Diensteanbieter häufig die Angabe von Kreditkartendaten. Die interessierten Nutzer müssen hierfür etwa den Namen des Kreditkarteninhabers und des Kreditkartenunternehmens, die Kreditkartennummer, das Ablaufdatum und eventuell die Prüfziffer angeben.

4.4 Suchdienste

Die Ausbreitung des Internet sowohl bezüglich seiner Benutzer als auch der angebotenen Webseiten ist noch lange nicht abgeschlossen. Schon heute umfasst das Internet aber ein unvorstellbares Angebot an Informationen, die kanalisiert werden müssen. Um sich durch diese Informationsflut zu

125 Vgl. insgesamt *Böckenförde*, Die Ermittlung im Netz, 2003, S. 197 ff.

126 Bei dem Post-Ident-Verfahren muss der Empfänger des Briefes, welcher z. B. das Passwort enthält, beim Postamt seinen Personalausweis oder Reisepass vorlegen, um den Brief zu erhalten, vgl. dazu *Möller*, NJW 2005, 1605 ff.

127 *Schulz/Hoffmann*, CR 2010, 131, 132; vgl. auch *Böckenförde*, Die Ermittlung im Netz, 2003, S. 200 ff.

kämpfen, stehen dem Benutzer verschiedene Suchdienste, insbesondere Suchmaschinen und Kataloge zur Seite.

4.4.1 Suchmaschinen

Bei Suchmaschinen kann der Benutzer über eine Eingabemaske einen Begriff spezifizieren und nach kurzer Suche steht eine Auswahl an möglichen Zielen zur Verfügung[128]. Die möglichen Ziele werden in einer Liste von Links aufgeschlüsselt. Bei der Volltextsuche wird der gesamte Text des ausgewählten Bestands durchsucht. Wenn der gesuchte Begriff auftaucht, wird der Link angezeigt. Es hängt vom eingegebenen Begriff ab, ob das Suchergebnis brauchbar ist oder nicht. Bei wenig spezifischen Suchanfragen werden im Normalfall sehr viele Treffer (Suchergebnisse) gefunden. Der Benutzer hat dann die Aufgabe, diese eigenständig zu sichten. Um dem Anwender eine genauere Vorstellung davon zu geben, was ihn auf der im Suchergebnis angezeigten Webseite erwartet, wird ihm zusätzlich zum Link in den meisten Fällen noch eine kurze Erläuterung zum Kontext, in dem der gesuchte Begriff gefunden wurde, gegeben.

Suchmaschinen bestehen je nach Größe aus mehreren zehntausend bis vielen Millionen von registrierten URLs, die jeweils mit charakteristischen Stichworten ihrer zugeordneten Dokumente verknüpft sind. Die Effizienz und Qualität von Suchmaschinen hängt hauptsächlich von der Leistungsfähigkeit der Robot-Programme ab, die diese Datenbanken aufbauen beziehungsweise warten. Eine sehr leistungsfähige Suchmaschine speichert zu jedem URL den gesamten Text ab. Sie ist somit in der Lage, eine Volltextsuche über alle registrierten Dokumente durchzuführen. Dies bedeutet aber nicht, dass das Suchergebnis für den Benutzer das beste Resultat ist[129]. Oft ist es so, dass Links als Suchergebnis angezeigt werden, die zwar das angegebene Stichwort enthalten, thematisch aber einen völlig fremden Bereich behandeln. Für die Ordnung der Suchergebnisse nach ihrer Relevanz spielen verschiedene Faktoren eine Rolle, die unterschiedliche Manipulationen der Suchergebnisse ermöglichen[130].

Im Internet gibt es mittlerweile eine Vielzahl verschiedener Suchmaschinen, die bei der Stichwortsuche unterschiedliche Ergebnisse liefern können. Um ein Suchergebnis zu erhalten, wirken oftmals mehrere Rechner des Suchmaschinenanbieters zusammen. Bei dem Suchmaschinenanbieter *Goo-*

128 Die derzeit bekannteste Suchmaschine ist Google.

129 Siehe insgesamt zur datenschutzrechtlichen Problematik von Suchmaschinen, mit denen nach Personen gesucht werden kann, *Seidel/Nink*, CR 2009, 666, 668 ff.; *Weichert*, MR-Int 2007, 188; ders., „Suchmaschinen sind im Prinzip rechtswidrig", Handelsblatt vom 03.02.2008, abzurufen unter *http://www.handelsblatt.com/suchmaschinen-sind-im-prinzip-rechtswidrig/2918060.html*.

130 Siehe dazu *Sieber*, in: Hoeren/Sieber, Hdb. Multimedia-Recht, Teil 1, Rdnr. 106 ff.

gle können beispielsweise bei der Beantwortung einer einzigen Suchanfrage bis zu 1.000 Rechner mitwirken[131].

Die Polizei setzt im Rahmen ihrer verdachtsunabhängigen Ermittlungen regelmäßig Suchmaschinen ein. Die Suchmaschinen stellen insoweit eine Arbeitserleichterung für die Polizei dar, indem sie die – zumeist öffentlich zugänglichen – Inhalte des Internet auswerten. Ferner nutzt die Polizei auch eigene Suchmaschinen, wie beispielsweise das Internet-Ermittlungstool „INTERMIT“[132].

4.4.2 Kataloge

Kataloge (auch Internet-Verzeichnisse genannt) arbeiten anders als Suchmaschinen. Bei einem Katalog handelt es sich um einen Dienst mit vorsortierten Themen, der Begriffe in einem Kontext liefert[133]. Die thematische Zuordnung wird bei einem Katalog meist von einer Redaktion verwaltet. Sie bietet zu den verschiedenen Kategorien Links an, die den Benutzer auf andere Webseiten führen, auf denen dann vertiefende Informationen zum gesuchten Thema zu finden sind. Bei manchen Katalogen wird für die Einordnung einer Webseite ein Robot-Programm verwendet, welches eine Webseite analysiert und anhand von Schlüsselwörtern beurteilt, in welcher Kategorie eine Seite einzuordnen ist. Es besteht für die Ersteller von Webseiten auch die Möglichkeit, ihre Seite bei einem Katalog direkt für eine bestimmte Kategorie anzumelden. Zusätzlich sind noch Moderatoren damit beschäftigt, laufend Korrekturen in den verschiedenen Kategorien vorzunehmen. Diese Moderatoren können auch bestimmte Webseiten in den verschiedenen Kategorien weit nach oben stellen, um die Anwender schnell auf die wichtigsten Seiten zu lenken. Hierbei besteht allerdings die Gefahr, dass der Moderator den Anwender bei seiner Suche beeinflusst.

4.5 Diskussions- und Kommunikationsforen

Im virtuellen Raum gibt es eine Vielzahl an Möglichkeiten, mit anderen zu diskutieren und zu kommunizieren[134]. Wenn man nur mit einer bestimmten Person kommunizieren möchte, wird dies häufig über ein E-Mail-System geschehen. Für Diskussionen, die mit vielen verschiedenen Personen durchgeführt werden sollen, gibt es unterschiedliche Möglichkeiten. Der News-Dienst (auch als Usenet oder Internet-News bezeichnet) verfügt über Tausende von Diskussionsforen, an denen der Benutzer teilnehmen kann. Vergleichbar mit dem News-Dienst sind die Mailing-Listen, die es auch zu den unterschiedlichsten Themen gibt. Bei Mailing-Listen und dem News-

131 *Reppesgaard*, Das Google-Imperium, 2008, S. 95.

132 Siehe dazu bereits oben unter B.II.1.

133 Weiterführendes zu Katalogen liefern *Kyas/Campo*, Internet professionell, 2. Aufl., 2001, S. 448 ff.; *Gergen*, Internetdienste, 2002, S. 289 ff.

134 Grote verweist bereits 1999 auf die „Vielfalt der Kommunikationsformen und -inhalte im Internet“, *Grote*, KritV 1999, 27, 29 ff.

Dienst handelt es sich um asynchrone Dienste. Mittlerweile dominieren allerdings Webforen das Internet. Eine Kommunikation mittels schriftlicher Nachrichten in Echtzeit erlaubt beispielsweise der Internet Relay Chat (IRC).

Diskussions- und Kommunikationsforen sind für die verdachtsunabhängigen Ermittlungen der Polizei im virtuellen Raum ein wesentliches Überwachungsgebiet. Die Polizisten durchsuchen beispielsweise Chats und Webforen insbesondere nach kinderpornografischen, jugendgefährdenden oder rechtsextremistischen Inhalten[135]. Die Diskussions- und Kommunikationsforen im Internet sind bezüglich ihres Zugangs unterschiedlich ausgestaltet. Neben öffentlich zugänglichen Foren sind viele nur nach einer vorherigen Registrierung einsehbar[136]. Teilweise unterscheiden die Foren auch danach, ob ein Nutzer selbst Beiträge verfassen möchte oder lediglich ein stiller Mitleser ist. Nur in den Fällen, in den der Nutzer selbst Beiträge veröffentlichen und sich aktiv an der Kommunikation beteiligen möchte, muss er sich vorher registrieren. Staatliche Behörden können folglich als stille Mitleser die öffentlich zugänglichen Inhalte dieser Foren ohne vorherige Registrierung erfassen.

4.5.1 News-Dienst

Der News-Dienst des Internet besteht aus einer Vielzahl von Diskussionsforen, die nach Themen in verschiedene Newsgroups unterteilt sind[137]. Er dient dem öffentlich zugänglichen Meinungsaustausch und ist vergleichbar mit einem schwarzen Brett. Die von den Mitgliedern der Newsgroups verfassten Artikel werden nicht automatisch an diese verteilt, sondern zentral auf sogenannten News-Servern gespeichert. Der Anwender kann nun selbst entscheiden, welche Beiträge er lesen möchte. Es liegt also keine passive Informationszuweisung vor, sondern eine aktive Informationsbeschaffung[138]. Um sich weltweit in Diskussionsgruppen auszutauschen, wird nicht nur ein einzelner Server in den Datenaustausch eingebunden, sondern es existiert ein globales Netz von Servern, die untereinander die Beiträge der Benutzer austauschen und den einzelnen Newsgroups zuweisen. Damit die Mitglieder einer Newsgroup jederzeit frühere Artikel lesen und die Entwicklung einer Diskussion verfolgen können, werden die Diskussionsbeiträge in chronologischer und thematischer Ordnung für einen gewissen Zeitraum archiviert. Man unterscheidet grundsätzlich moderierte Newsgroups, in denen ein Moderator entscheidet, welcher Beitrag veröffentlicht wird, von

135 Vgl. Der Spiegel, 30/2007, 26 ff.

136 Vgl. zu den Möglichkeiten der Registrierung die obigen Ausführungen zu geschützten Inhalten im WWW unter Ziffer 4.3.2.

137 Einen News-Dienst liegt das Network News Transfer Protocol (NNTP) zu Grunde. Dieses Protokoll setzt auf TCP als Transportdienst auf. Vertiefend zum News-Dienst siehe *Meinel/Sack*, WWW, 2004, S. 640 ff.; *Kyas/Campo*, Internet professionell, 2. Aufl., 2001, S. 181 ff.

138 *Gergen*, Internetdienste, 2002, S. 141.

unmoderierten Newsgroups, in denen jeder Anwender unzensiert seinen Beitrag der Masse eröffnen kann.

4.5.2 Mailinglisten

Neben den Newsgroups sind Mailing-Listen eine weitere Möglichkeit, weltweit über jegliche Themen in einer Gruppe zu diskutieren[139]. Die Funktionsweise der Mailing-Listen ist sehr einfach konzipiert und baut auf dem E-Mail-System auf. Jede Interessengruppe besitzt eine zentral geführte Verteilerliste, die die E-Mail-Adressen aller Teilnehmer enthält. Wenn nun ein Mitglied der Diskussionsrunde einen Beitrag verfasst hat, sendet er diesen an die Verwaltungsadresse der entsprechenden Mailing-Liste. Von dort aus wird dann der Beitrag an alle Teilnehmer, die in der Verteilerliste geführt werden, weitergeleitet. Mailinglisten spielen mittlerweile allerdings keine große Rolle mehr.

4.5.3 Internet Relay Chat (IRC)

Bei dem Internet Relay Chat (IRC) handelt es sich um einen Dienst, der zum Austausch von schriftlichen Nachrichten in Echtzeit konzipiert ist[140]. Im Unterschied zum E-Mail-Dienst, der grundsätzlich auf eine asynchrone Kommunikation zwischen Einzelpersonen abzielt, ist der IRC von Anfang an für Zwecke der Gruppenkommunikation vorgesehen[141]. Der IRC ist als Client/Server-Anwendung konzipiert und sieht eine gleichzeitige Teilnahme vieler verschiedener Anwender an einem Server vor. Die IRC-Server sind über das Internet miteinander verbunden und bilden so ein großes IRC-Netzwerk. Auf vielen tausend verschiedenen Kanälen (Channels) finden Diskussionen und Gespräche, sogenannte Chats, in Echtzeit statt[142]. In Echtzeit bedeutet, dass die von einem Benutzer eingegebene Nachricht so schnell wie möglich zum zentralen Server gesendet wird und dieser die Nachricht möglichst schnell an die anderen Teilnehmer weitergibt. Es ist daher beim Chatten möglich, direkt auf die Nachricht eines anderen Teilnehmers zu antworten[143]. So kann eine gesprächsähnliche Kommunikation über Tastatureingaben stattfinden. Unter den Chats gibt es öffentliche, also für alle Nutzer frei verfügbare, und private, zu der nicht jeder Nutzer zuge-

139 Weitere Informationen zu Mailing-Listen geben z. B. *Kyas/Campo*, Internet professionell, 2001, 2. Aufl., S. 189 ff.

140 Die Finnen *Jarkko Oikarinen* und *Jyrki Kuoppala* haben diesen Dienst 1988 entwickelt. Weiterführendes zum IRC bieten *Sieber*, in: Hoeren/Sieber, Hdb. Multimedia-Recht, Teil 1, Rdnr. 119 ff.; *Meinel/Sack*, WWW, 2004, S. 639 ff.

141 IRC wird deshalb auch als Telekonferenz-System bezeichnet.

142 Mehr zu Chats ist zu finden bei *Fix*, Generation Chat, 2001; *Beißwenger*, Chat-Kommunikation, 2001; *Husmann*, Chatten im Internet Relay Chat (IRC), 1998.

143 Die Teilnahme an einem Chat, also an einem Gespräch oder einer Diskussion, wird „chatten" genannt. Das Chatten ist letztlich durch den Film „Das Netz" besonders bekannt geworden.

lassen wird. Die privaten Chats sind vergleichbar mit einem (virtuellen) Gespräch im engen Kreis.

Immer mehr Menschen treffen sich im Netz, um über die Tastatur miteinander zu plaudern. Man kann rund um die Uhr mit Teilnehmern aus der ganzen Welt zu fast jedem Thema chatten. Die gängigste Sprache für Chats ist Englisch. Aber es gibt heute wohl kaum ein Land, in dem nicht auch zumindest ein Chat in der Landessprache existiert. Für einige Menschen ist die virtuelle Chat-Welt zu einer Art Nebenwelt geworden, die immer stärker die Realität verdrängt[144]. Bei einer so intensiven Beschäftigung mit einer virtuellen Welt bilden sich eigene Verhaltensregeln, die für Chats unter dem Begriff „Chattiquette“ zusammengefasst sind[145]. Außerdem möchte im Netz der Chatter zumindest vorerst anonym bleiben. Daher gibt er sich ein Pseudonym, welches im Chat-Jargon als „Nickname“ oder kurz „Nick“ bezeichnet wird.

4.5.3.1 Chattiquette

Für Chats gibt es viele geschriebene und ungeschriebene Verhaltensregeln. Die geschriebenen Verhaltensregeln kann man auf fast jedem Server nachlesen. Es ist etwa untersagt, sexistische oder beleidigende Aussagen zu machen. Außerdem ist links- oder rechtsextremistische Propaganda verboten. Zu den ungeschriebenen Regeln gehören oftmals Regelungen, die auch im realen Leben existieren. Man sollte keine fremde Kommunikation unfreundlich und direkt stören, man sollte auf gestellte Fragen antworten und man sollte niemanden belästigen.

Eine Besonderheit der Chats ist die Sprache, mit der kommuniziert wird. Um die Kommunikation effizienter zu machen, haben sich eine ganze Menge an Abkürzungen und Symbolen eingebürgert, die Gefühle und häufige Aussprüche ausdrücken[146]. Für Teilnehmer an Chats ist es wichtig, diese Sprache, den sogenannten Chat-Slang, zu beherrschen, da es sonst oftmals schwierig ist, den Gesprächen zu folgen.

Nicht immer sind alle Teilnehmer eines Chats an wirklichen Gesprächen oder Diskussionen interessiert. Es wird häufig, gerade in öffentlichen Chats, Teilnehmer geben, die stören oder beleidigen wollen. Für diese Fälle der verbalen Entgleisung gibt es eine Art Aufpasser, den Channel-Operator oder Moderator. Dieser kann Störer aus einem Chat zeitweise oder ganz entfernen.

144 Die großen Online-Dienste bieten eigenständige Chat-Welten an. Die Teilnahme an diesen Chats erfordert eine Mitgliedschaft. Dafür wird dem Chatter von einfachen Chat-Oberflächen bis zu Virtual-Reality-Clients alles geboten.

145 „Chattiquette“ ist im Grunde die Etikette im Chat.

146 So steht z. B. „CWYL“ für „chat with you later“ oder „IMHO“ für „in my humble opinion“.

4.5.3.2 Nickname

Jeder Chatter verwendet zu seiner Identifikation einen frei wählbaren, jeweils eindeutigen Namen als Pseudonym, der „Nickname“ oder kurz „Nick“ genannt wird. Die Auswahl eines geeigneten Nicknames ist nicht ganz unwichtig. Über einen interessanten Nickname, der vielleicht ein besonderes Hobby oder besondere Interessen hervorhebt, kann man leichter zu denjenigen Chattern Kontakt aufnehmen, die ähnliche Interessen haben. Viele Nicknames sagen so schon etwas über den Teilnehmer aus, wobei diese Aussage natürlich nicht wahr sein muss, da die Nicks frei wählbar sind[147].

4.5.4 Instant-Messaging- und Konferenzdienste

Instant-Messaging- und Konferenzdienste setzen verschiedene Kommunikationsmethoden kombiniert ein[148]. Sie vereinen beispielsweise eine Chatfunktion mit Möglichkeiten der Datenübertragung, der Sprachtelefonie und der Schaltung von Videokonferenzen[149]. Mit diesen Internetdiensten können kleine Gruppen, deren Teilnehmer bestimmt sind, kommunizieren.

4.5.5 Webforen

Bei einem Webforum handelt es sich um ein Internetforum auf einer Webseite, also als Teil des World Wide Web. Die Webforen haben in den letzten Jahren die meisten anderen Internetforen, wie beispielsweise den News-Dienst, verdrängt. Zum News-Dienst bestehen ansonsten keine wesentlichen Unterschiede. Allerdings setzen die meisten Webforen eine vorherige Registrierung voraus, wodurch sich auch langfristige elektronische Gemeinschaften bilden können. Die Nutzer handeln in den Webforen zumeist unter Nicknames. Als Mittel der Identitätsbildung können sich die Nutzer beispielsweise Benutzerbilder und Signaturen geben.

4.5.6 Soziale Netzwerke

In den letzten Jahren haben Soziale Netzwerke wie StudiVZ, Facebook oder Xing eine immer größere Bedeutung in der virtuellen Welt gewonnen. Facebook hat beispielsweise weltweit Ende 2011 bereits über 840 Millionen Nutzer, davon über 20 Millionen Nutzer aus Deutschland, gehabt[150]. Mit den Sozialen Netzwerken bieten die Anbieter den Nutzern virtuelle Kommunikationsplattformen zur Kontaktpflege und Selbstdarstellung an[151]. In diesen Netzwerken können die Nutzer sich interaktiv beteiligen. Nachdem sie ein

147 Hinter dem Nickname „Jenny21J“ könnte eine Frau, die 21 Jahre alt ist, stehen. Es könnte aber auch ein 80jähriger Mann diesen Nickname gewählt haben.

148 Häufig genutzt wird beispielsweise ICQ.

149 Vgl. insgesamt dazu *Sieber*, in: Hoeren/Sieber, Hdb. Multimedia-Recht, Teil 1, Rdnr. 127 ff.

150 Vgl. *http://de.statista.com/statistik/daten/studie/70189/umfrage/nutzer-von-facebook-in-deutschland-seit-2009/*.

151 Vgl. insgesamt dazu *Henrichs/Wilhelm*, Kriminalistik 2010, 30 ff.

persönliches Profil mit ihren persönlichen Daten[152], Vorlieben und weiteren Angaben angelegt haben, können sie sich beispielsweise mit anderen Nutzern „befreunden". Dadurch herrscht eine virtuelle Verknüpfung zwischen diesen Freunden, so dass der Kontakt untereinander besonders leicht gepflegt werden kann. Die sogenannten „Freunde" in Sozialen Netzwerken müssen sich weder nahe stehen noch überhaupt kennen, wobei die Entwicklung aktuell eher dahin geht, nur bekannten Nutzern Einsicht in das persönliche Profil zu gewähren[153].

Über die Sozialen Netzwerke können die Nutzer zudem Nachrichten, gegebenenfalls mit Anhängen, versenden und empfangen, Fotos auf ihrer Profilseite einpflegen, die Beiträge anderer kommentieren, sich in virtuelle Gästebücher von anderen Nutzern eintragen und über Recherchetools andere Nutzer aufspüren. Soziale Netzwerke bieten ihren Nutzern sich stetig weiterentwickelnde Funktionen an, um sich zu vernetzen, miteinander zu kommunizieren und Daten unterschiedlichster Formate auszutauschen. Im Gegensatz zu anderen Webforen handeln die Nutzer in Sozialen Netzwerken häufig unter ihrem Klarnamen. Allerdings wird der Wahrheitsgehalt der Inhalte und Daten vor ihrer Veröffentlichung nicht überprüft, womit besondere Gefahren einhergehen[154].

Inwieweit die Polizei im Rahmen ihrer verdachtsunabhängigen Ermittlungen im virtuellen Raum Soziale Netzwerke überwacht, wird durch die staatlichen Quellen unterschiedlich beantwortet. Nach Angaben der Bundesregierung auf eine Kleine Anfrage ermitteln die Polizeibehörden des Bundes – insbesondere das BKA – nicht verdachtsunabhängig in Sozialen Netzwerken[155]. Im Rahmen der Strafverfolgung setzte das BKA in einem Zeitraum von Sommer 2009 bis Sommer 2011 in sechs Ermittlungsverfahren „virtuelle" Verdeckte Ermittler ein[156].

Für die Landesbehörden gibt es anderslautende Auskünfte, nach denen auch in Sozialen Netzwerken verdachtsunabhängig ermittelt wird[157]. Über die erhebliche Relevanz Sozialer Netzwerke für polizeiliche Ermittlungen besteht aber Einigkeit, weshalb sich beispielsweise die Kommission Kriminalitätsbekämpfung (KKB) der AG Kripo seit 2010 mit den Möglichkeiten

152 Vgl. beispielsweise zu den datenschutzrechtlichen Problemen Sozialer Netzwerke *Erd*, NVwZ 2011, 19 ff.

153 *Graf*, in: Beck´scher Online-Kommentar StPO, § 100a, Rdnr. 32e.

154 Vgl. zu den besondere Gefahren Sozialer Netzwerke für Kinder und Jugendliche *Jandt/Roßnagel*, MMR 2011, 637 ff.; vgl. zur Gefahr von Aufrufen zur Lynchjustiz und organisiertem Mobbing in Sozialen Netzwerken *Ostendorf/Frahm/Doege*, NStZ 2012, 529 ff.

155 Vgl. BT-Drs 17/6587, S. 2.

156 BT-Drs 17/6587, S. 5.

157 Vgl. z. B. die Pressemitteilung des Ministeriums für Inneres und Kommunales des Landes Nordrhein-Westfalen vom 01.03.2011, abzurufen unter *http://www.mik.nrw.de/presse-mediathek/aktuelle-meldungen/archiv/archiv-meldungen-im-detail/news/spezialisierte-lka-ermittler-spueren-erfolgreich-internet-kriminalitaet-auf-innenminister-jaeger.html*.

polizeilicher Recherchen in Sozialen Netzwerken befasst und die AG KaRIn mindestens zweimal pro Jahr in regelmäßigen Arbeitstagungen neue Erkenntnisse und Entwicklungen in Sozialen Netzwerken austauscht[158]. Die Polizei Hannover nutzt sogar bei Ermittlungen ein eigenes Facebook-Profil, auf dem sie Fotos von Verdächtigen zeigt und nützliche Hinweise sammelt[159].

4.6 Audio- und Videokommunikation

Während durch den IRC schriftliche Nachrichten in Echtzeit ausgetauscht werden können, besteht heute auch die Möglichkeit, multimediale Angebote in Echtzeit (Realtime) zu nutzen[160]. Durch die stetig steigende Bandbreite können sehr große Audio-, Video- oder Bilddateien in annehmbarer Zeit übertragen werden. Kontinuierliche Medienanwendungen, wie beispielsweise Internet-Telefonie, Internet-Radio, Videokonferenzen oder interaktive Spiele, gewinnen immer mehr an Bedeutung. Gerade der Einfluss der Internet-Telefonie[161] wächst stetig an, bei der für die Übertragung der Sprach- und Datenkommunikation auf die verschiedenen Protokolle des Internet zurückgegriffen wird. Wenn eine Multimedia-Datei über das Internet in Echtzeit bereits während des Übertragungsvorganges kontinuierlich wiedergegeben wird, bezeichnet man dies als Streaming. Dies wird durch eine Pufferung der übertragenen Daten vor der eigentlichen Darstellung erreicht.

4.7 File-Sharing-Systeme

Mit File-Sharing-Systemen können Nutzer über das Internet Daten austauschen. Die Besonderheit bei File-Sharing-Systemen ist, dass jeder Rechner gleichzeitig als Server und als Client agiert. Dieses dezentrale Datenverteilungssystem, bei dem sich die relevanten Daten in der Regel nicht nur auf einem Server, sondern gleichzeitig auf vielen Rechnern befinden, erleichtert die Verfügbarkeit der Daten für den Datenaustausch[162]. File-Sharing-Systeme werden insbesondere für den illegalen Austausch urheberrechtlich

158 Vgl. BT-Drs 17/6587, S. 3. Vgl. insgesamt zur erheblichen Relevanz Sozialer Netzwerke für die polizeilichen Ermittlungen *Henrichs/Wilhelm*, Kriminalistik 2010, 30 ff.

159 Süddeutsche.de vom 11.08.2011, abzurufen unter *http://www.sueddeutsche.de/digital/soziale-netzwerke-als-fahndungswerkzeug-mit-facebook-auf-verbrecherjagd-1.1130130*. Andere Bundesländer planen dies ebenfalls, was nicht unumstritten ist, siehe dazu *http://www.heise.de/newsticker/meldung/Facebook-Fahndung-in-Thueringen-umstritten-1777850.html*.

160 Zur Übertragung von digitalisierten Audio- und Videosignalen über das Internet wird als Übertragungsprotokoll das Real-Time Transport Protocol (RTP) genutzt. Weiterführend *Meinel/Sack*, WWW, 2004, S. 626 ff.

161 Internet-Telefonie wird auch als „IP-Telefonie" oder „Voice over IP (VoIP)" bezeichnet.

162 Vgl. insgesamt dazu *Sieber*, in: Hoeren/Sieber, Hdb. Multimedia-Recht, Teil 1, Rdnr. 139 ff.

geschützter Inhalte (z. B. Musik- und Videodateien oder Software) genutzt[163].

III. Internet und Gesellschaft

Das Internet hat sich innerhalb von wenigen Jahren von einem Medium, das vorwiegend von Wissenschaft und Forschung genutzt wurde, zu einem Massenmedium für jedermann entwickelt. Im Jahr 1991 machten noch Netzwerke von Universitäten und Forschungseinrichtungen Dreiviertel aller an das Internet angeschlossenen Netze aus. Dieser Anteil ist seitdem stetig gefallen. Mittlerweile ist das Internet ohne Zweifel ein weltumspannendes, globales Netz für alle. Während sich die Benutzerzahl in den letzten Jahren enorm vergrößert hat, fällt bei genauerer Betrachtung der weltweiten Verteilung der Benutzer im Internet auf, dass insbesondere die hochentwickelten Industrienationen den größten Einfluss auf diese Entwicklung gehabt haben[164]. In den nächsten Jahren ist allerdings damit zu rechnen, dass auch die anderen Länder weiter aufholen werden, so dass in nicht ferner Zukunft das Internet ein Netzwerk von allen Menschen für alle Menschen sein wird.

Indem das Internet nicht nur geographisch wächst, sondern auch bei den meisten Menschen immer größere Anteile des persönlichen Lebensraums einnimmt, verändern sich die Abhängigkeiten. Die Entwicklung zu einer Informationsgesellschaft mit all ihren Vor- und Nachteilen fördert die Abhängigkeit von der Informationstechnologie[165]. Indem Informationen und der Zugang zu Informationen sowohl in wirtschaftlicher als auch in gesellschaftlicher Hinsicht eine immer größere Rolle einnehmen, bedeutet der freie und gleichberechtigte Internetzugang ein wesentliches Recht für den Nutzer. Dieser mit dem modernen Begriff „Netzneutralität“ umschriebene Umstand wird voraussichtlich in den nächsten Jahren noch weiter an Einfluss gewinnen und zugleich für Verwirrung sorgen[166]. Netzneutralität bedeutet zwar den freien Zugang zu den Daten des Internet, aber ist nicht gleichzusetzen mit einem freien Internet ohne staatliche und wirtschaftliche Eingriffe.

Eine der bedeutenden gesellschaftlichen Entwicklungen der letzten Jahre war sicherlich der Transfer identitätsbezogener Elemente in das Internet[167]. Das Internet ist nicht mehr lediglich ein Medium zur Informationssuche, sondern es hat sich immer weiter zu einem Interaktionsmittel entfaltet, welches den Nutzer nicht berieseln will, sondern zum Mitwirken anregt. Diesen Fortschritt kann man allgemein als „Web 2.0“ zusammenfassen. Bei dem

163 Vgl. z. B. *Mühlberger*, GRUR 2009, 1022 ff.
164 Siehe dazu www.internetworldstats.com.
165 Vgl. *Gercke*, MMR 2008, 291, 292.
166 Vgl. zur Netzneutralität z. B. *v. Lucius*, NVwZ 2011, 218 ff.; *Spies*, MMR 2010, 585 ff.
167 *Gercke*, MMR 2008, 291, 292.

Web 2.0 handelt es sich nicht um einen eigenen Internetdienst, sondern vielmehr um eine neue Form der virtuellen Vernetzung zur Interaktion[168]. Der Kernbestandteil des Web 2.0 sind Kommunikationsplattformen zur Kontaktpflege, Selbstdarstellung und zum Informationsaustausch. Nutzer können, beispielsweise in den Sozialen Netzwerken, selbst Informationen eingeben, aktualisieren und verändern. Außerdem können Sie mit anderen Nutzern kommunizieren, Beiträge anderer kommentieren, bestimmten Gruppen beitreten oder auf bestimmte Inhalte im Internet hinweisen. Neben diesen Kommunikationsplattformen zeichnet sich das Web 2.0 durch weitere neue Angebotsformen aus[169], wie zum Beispiel virtuelle Spielwelten[170]. In diesen künstlichen Welten nehmen die Nutzer in Gestalt einer virtuellen Figur Kontakt zu anderen Nutzern auf. Im Gegensatz zu Sozialen Netzwerken entfernen sich die Nutzer noch weiter von der eigenen Realität, da sie in den virtuellen Welten anonym eine Identität annehmen können, die mit ihrem eigenen Leben nicht zusammenhängen muss. Sie können sich in den virtuellen Spielwelten also in der Form und Weise darstellen, wie sie es wollen.

Die virtuelle Selbstdarstellung spielt für einen wachsenden Teil der Menschen eine immer bedeutendere Rolle. Im Internet können sie ein Bild von sich aufzeigen, das nicht der Realität entsprechen muss. In den meisten Fällen wird ein anderer Nutzer die genannten Eigenschaften auch nicht verifizieren können, wenn er den Nutzer nicht persönlich kennt. Teil dieser Entwicklung ist sicherlich der Trend, im Internet ein Tagebuch zu führen und dieses der Allgemeinheit zu öffnen. Diese sogenannten Weblogs (oder kurz: Blogs) geben den Menschen die Möglichkeit, andere an ihrem Leben und ihren Erlebnissen, Einstellungen und Erfahrungen teilzuhaben[171].

Durch das Internet hat sich ferner das Kommunikationsverhalten der Menschen beschleunigt und verändert. Informationen werden in Sekunden um die Welt geschickt. Internetdienste wie Twitter bieten die Chance, eine große Zahl von Menschen direkt und grenzenlos zu informieren. Auf den ersten Blick unwichtige Begebenheiten können sich so zum globalen Gesprächsthema erheben. Andererseits können die Internetdienste, wie etwa auch die Sozialen Netzwerke, zum blitzartigen Austausch von Informationen genutzt werden. Eine Zensur oder ein Abfangen dieser Nachrichten ist, bedingt durch die technische Struktur des Internet, kaum möglich. Dadurch können diese Internetdienste selbst auf politische Entwicklungen einen immensen Einfluss ausüben[172].

168 Daher wird das Web 2.0 auch teilweise als „MitmachWeb“ bezeichnet.

169 Siehe dazu *Henrichs/Wilhelm*, Kriminalistik 2010, 30 ff.

170 Weiterführend dazu *Habel*, MMR 2008, 71 ff.

171 Siehe weiterführend zu Blogs *Kaufmann*, Weblogs – Rechtliche Analyse einer neuen Kommunikationsform, 2009.

172 Als Beispiel können etwa die politischen Entwicklungen in Tunesien Anfang 2011 genannt werden.

Neben den genannten Einflüssen nimmt das Internet selbstredend auch im Wirtschaftsleben eine stetig wachsende Bedeutung ein. Kaum ein Unternehmen kommt heute ohne eine Selbstdarstellung im Internet aus. Als bevorzugtes Kommunikationsmittel hat die E-Mail den Brief längst abgelöst.

Schlussendlich könnte hier die Aufzählung beinahe unbegrenzt fortgeführt werden. Im Ergebnis kann aber festgehalten werden, dass das Internet zum ständigen und beherrschenden Medium für die Menschen geworden ist. Welche Bedeutung das Internet für unsere Gesellschaft eingenommen hat, zeigt sich auch daran, dass der Bundestag eine eigene Enquete-Kommission „Internet und digitale Gesellschaft" eingerichtet hat[173].

IV. Gefahren im Internet

Das Internet bietet seinen Benutzern ein fast unendliches Spektrum an Informationen. Bei all diesen Nutzungsmöglichkeiten muss jedoch jedem klar sein, dass das Internet kein rechtsfreier Raum ist. Mit der Verbreitung des Internet ist eine Vielzahl neuer Rechtsprobleme entstanden, die zu einem großen Teil durch die geltenden Gesetze gelöst werden konnten. Ein Teil der Rechtsprobleme konnte aber nur durch neue Gesetze beziehungsweise Modifikationen bestehender Gesetze einheitlich geklärt werden. Der Gesetzgeber und die Rechtsprechung werden auch weiterhin gefragt sein, um die Gefahren des Internet zu minimieren, da immer wieder neue Nutzungsarten des virtuellen Raumes entdeckt werden und somit neuer Handlungsbedarf besteht. Nur wenn dem Medium Internet ein verlässliches rechtliches Instrumentarium zur Seite steht, wird die stets steigende wirtschaftliche Bedeutung des Internet nicht durch rechtliche Risiken oder rechtliche Hemmnisse behindert werden.

Bei den Gefahren im Internet wird man unterscheiden müssen zwischen dem deliktischen Handeln, bei dem der Computer als Werkzeug eingesetzt wird, und den Straftaten, die im virtuellen Raum als Tatort verübt werden[174]. Zur erstgenannten Gruppe mit dem Computer als Werkzeug zählen beispielsweise das Ausspähen von Daten (§ 202a StGB), das Abfangen von Daten (§ 202b StGB) oder die Computersabotage (§ 303b StGB)[175]. Eine große Bedrohung geht von Computerviren aus, die in unterschiedlichster

173 Näheres dazu ist zu finden unter *http://www.bundestag.de/internetenquete/index.jsp*.

174 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 544. Dementsprechend kann auch einerseits nach „Computerkriminalität" mit dem Computer als Werkzeug oder Ziel der Tat und andererseits nach „Internetkriminalität" mit den strafrelevanten Handlungen, die durch Nutzung des Internet begangen werden, differenziert werden, vgl. *Eisenberg*, Kriminologie, 6. Aufl., 2005, § 47, Rdnr. 65, 69; vgl. zur Internetkriminalität auch *Laue*, jurisPR-StrafR 13/2009, Anm. 2; *ders.*, jurisPR-StrafR 15/2009, Anm. 2; *Gercke*, ZUM 2010, 633 ff.

175 Vgl. insgesamt dazu *Gercke*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 84 ff.; *Ernst*, Hacker, Cracker & Computerviren, 2004.

Form auftreten können. Bei den Computerviren handelt es sich um Programme, die sich durch Selbstkopieren in Wirtsprogrammen verbreiten und Daten in einem Datensystem unberechtigt verändern, neue Daten hinzufügen oder den Datenfluss verändern[176].

Teilweise werden aber auch einfach Strafdelikte aus dem „analogen" Leben in den virtuellen Raum übertragen. Im Jahr 2007 waren beispielsweise über 70 Prozent der „mit Tatmittel Internet begangenen" Straftaten Betrugsdelikte[177]. In diesen Fällen fördern die technischen Entwicklungen des Internet keine wesentlichen neuen Rechtsprobleme, sondern die einfachen Möglichkeiten über Online-Shopping und Auktions-Plattformen[178] erleichtern den Nutzern die Tatbegehung[179]. Die Täter können so aus ihrer vertrauten Sphäre am heimischen Rechner Straftaten mit teilweise immensem Ausmaß begehen.

Neben den bereits aus der Vorzeit des Internet-Zeitalters bekannten Straftatbegehungsformen gibt es allerdings auch verschiedene, durch das neue Medium eröffnete Begehungsfelder. Beim sogenannten „Phishing" versuchen die Täter zumeist die Kontodaten mit den zugehörigen Zugangsdaten von den Opfern ausfindig zu machen. Dazu nutzen sie unterschiedliche Begehungsformen, wie beispielsweise die Vortäuschung der Webseite der Bank des späteren Opfers. Wenn das spätere Opfer nun seine vertraulichen Zugangsdaten auf der Webseite eingibt, spähen die Täter diese aus und nutzen sie für ihre Taten[180].

Ein wesentliches Element der Polizeiarbeit ist im Internet die Bekämpfung von verbotenen Inhalten. Zuvorderst wird, gerade auch durch die verdachtsunabhängigen Ermittlungen der Polizei im Internet, der Versuch unternommen, die Veröffentlichung von kinderpornografischen Inhalten weitestgehend einzudämmen. Neben diesen Inhalten werden auch andere illegale, etwa rechtsextremistische und gewaltverherrlichende Webseiten möglichst effektiv bekämpft, beispielsweise durch das Löschen oder Sperren dieser Webseiten[181]. Die globale Struktur des Internet erschwert den Behörden ihre notwendige Arbeit dabei jedoch enorm.

In Sozialen Netzwerken haben sich für die staatlichen Stellen neue und altbekannte Gefahren versammelt. Indem vor allem in Sozialen Netzwerken die Grenzen zwischen „CyberCrime" und realem Leben verschwimmen, ist dort der Staat zum Handeln aufgefordert[182]. Anlass zum polizeilichen Han-

176 Vgl. *Laue*, jurisPR-StrafR 13/2009, Anm. 2.
177 Vgl. *BKA* (Hrsg.), Polizeiliche Kriminalstatistik 2007, 2008, S. 243.
178 Insgesamt dazu *Dingler*, Betrug bei Online-Auktionen, 2008.
179 Vgl. *Laue*, jurisPR-StrafR 15/2009, Anm. 2.
180 Siehe zum „Phishing" *Brandt*, Zur Strafbarkeit des Phishing, 2010.
181 Vgl. dazu z. B. *Sieber/Nolde*, Sperrverfügungen im Internet, 2008.
182 Siehe zu den besonderen Gefahren für Kinder und Jugendliche in Sozialen Netzwerken *Jandt/Roßnagel*, MMR 2011, 637 ff.

deln in Sozialen Netzwerken und auch im gesamten Internet bieten zum Beispiel Beleidigungen, Betäubungsmitteldelikte, Stalking, Betrugsstraftaten, Sexualstraftaten (z. B. Vertrieb von kinderpornografischem Material), Urheberrechtsverletzungen, politisch motivierte Kriminalität, Vortäuschung von Straftaten, Verstöße gegen das Waffenrecht und Aufforderungen zu Straftaten[183].

Die mittlerweile nicht mehr ganz neuen Gefahren durch Terrorismus gehören zum Aufgabenbereich der Polizei[184]. Die grenzenlosen und anonymisierten Möglichkeiten des Internet bieten den Terroristen die Chance, ein weltumspannendes Netzwerk mit schnellen und einfachen Kommunikationsstrukturen aufzubauen. Daher gehen die Ermittlungen im Bereich terroristischer Aktivitäten im Internet auf Grund der technischen Struktur des Internet mit besonderen Herausforderungen an die staatlichen Stellen einher[185].

V. Personenbezogene Daten im Internet

Die Privatsphäre eines Menschen gehört zu den wesentlichen Elementen einer autonomen Lebensgestaltung. Jeder Mensch möchte, wenn auch in unterschiedlicher Intensität, grundsätzlich selbst über die Verwendung und Erhebung seiner persönlichen Daten entscheiden. Im heutigen Informationszeitalter werden personenbezogene Daten immer wichtiger und wertvoller[186]. Früher mussten der Bundesgerichtshof und das Bundesverfassungsgericht zumeist über die Vermarktung des allgemeinen Persönlichkeitsrechts durch Wort und Bild von Prominenten richten[187]. In heutiger Zeit haben die personenbezogenen Daten von „Normalbürgern" an immenser Bedeutung gewonnen, da sich das Konsumverhalten der Menschen durch die neuen Informations- und Kommunikationsmöglichkeiten geändert hat[188].

Um gezielter und effektiver für Produkte zu werben, ist es von Vorteil, Nutzerprofile über die potentiellen Kunden zu erstellen[189]. Wirtschaftlichen

183 Vgl. insgesamt dazu *Henrichs/Wilhelm*, Kriminalistik 2010, 30, 32 ff.

184 Vgl. beispielsweise die Novellierung des BKAG, dazu *Bäcker*, Terrorismusabwehr durch das Bundeskriminalamt, 2009.

185 Siehe insgesamt dazu *Gercke*, CR 2007, 62 ff.

186 Zur Bedeutung von personenbezogenen Daten als Wirtschaftsfaktor *Weichert*, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, S. 1463 ff.

187 Z. B. Paul Dahlke, Boris Becker, Emil Nolde, Caroline v. Monaco, Nena.

188 Zum Konsumverhalten im Internet bereits *Kepplinger/Engesser*, in: Gounalakis, Rechtshandbuch Electronic Business, 2003, S. 69 ff.

189 Beispielhaft ist hierfür die 4-Milliarden-Dollar-Klage eines Herstellers von Videos für Internet-Broadcasts gegen den Betreiber einer Suchmaschine, weil dieser nicht, wie vereinbart, Benutzerdaten seines Dienstes lieferte. Der Rechtsanwalt des Klägers formulierte deutlich: „Diese Daten sind die Internet-Währung". Nachzulesen auf *www.heise.de/newsticker/data/jk-30.12.99-000/*. Weiterführendes zu Nutzerprofilen bieten *Fröhle*, Web advertising, Nutzer-

Wert haben beispielsweise die Adressen von Kunden, die Bonität möglicher Vertragspartner oder Status, Konsumverhalten und Alter von Kunden. Einen wesentlichen Beitrag zur Ökonomisierung personenbezogener Daten hat die Verbreitung des Internet geleistet. Das Internet bietet mit seinem enormen Ausmaß eine fast unerschöpfliche Sammlung an Daten, die von den Nutzern aufgerufen werden können. Neben diesen abrufbaren Daten entstehen bei jeder Nutzung des Internet weitere Daten, wie beispielsweise Angaben über den Beginn und das Ende sowie den Umfang der jeweiligen Nutzung.

Es hat aber nicht nur eine quantitative Änderung des Gefahrenpotentials für personenbezogene Daten in einer zunehmend „informatisierten Gesellschaft“[190] stattgefunden. Auch qualitativ besteht eine neue Gefahrendimension, da Informations- und Kommunikationsdienste in der Regel in einem offenen Telekommunikationsnetz wie dem Internet genutzt werden, dessen Zugangsberechtigte der Nutzer weder kennt noch kontrollieren kann[191].

Ein Schutzbedürfnis der personenbezogenen Daten besteht nicht nur gegenüber privaten Unternehmen, sondern in zunehmendem Maße gegenüber den staatlichen Einrichtungen, die mit ihrer Datengier scheinbar einen gläsernen Internet-Nutzer erreichen wollen. Schlagwörter wie „Terrorgefahr“ oder „Verbrechensbekämpfung“ erscheinen als multifunktionale Werkzeuge zur Beschneidung der Freiheitsrechte und Befriedigung des staatlichen Kontrollbedürfnisses[192].

Um dem entgegenzuwirken, dient der Datenschutz dem Schutz des Persönlichkeitsrechts beim Umgang mit personenbezogenen Daten[193]. Die Datenschutzgesetze finden allerdings nur Anwendung, wenn es sich um personenbezogene Daten handelt[194]. Für das Internet ist prinzipiell kein neuer Begriff der „personenbezogenen Daten“ entstanden oder erforderlich[195]. Personenbezogene Daten sind gem. § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen[196] Person. Eine eindeutige Entscheidung zwischen

profile und Teledienstedatenschutz, 2003; *Lerch/Krause/Hotho/Roßnagel/Stumme*, MMR 2010, 454 ff.

190 *Pitschas*, DuD 1998, 139, 149.

191 *Moos*, Datenschutz im Internet, in: Kröger/Gimmy, Handbuch zum Internetrecht, 2002, S. 497, 498.

192 Siehe dazu *Bull*, RDV 2008, 47.

193 Vgl. § 1 Abs. 1 BDSG.

194 Vgl. z. B. § 1 Abs. 2 BDSG.

195 *Helfrich*, in: Hoeren/Sieber, Hdb. Multimedia-Recht, Teil 16.1, Rdnr. 32 ff.

196 Nur natürliche Personen unterliegen dem Schutz des BDSG. Die rechtspolitisch vehement diskutierte Frage, ob auch juristische Personen einbezogen werden sollten, spielt in der Praxis eine eher untergeordnete Rolle, da oftmals von Informationen über Gesellschaften und Vereine auf Personen geschlossen werden kann und damit auch diese Angaben als personenbezogene Daten zu behandeln sind. Vgl. hierzu *Dammann*, in: Simitis, BDSG, 2006, 6. Aufl., § 3, Rdnr. 17 ff.; *Gola/Schomerus*, BDSG, 11. Aufl., 2012, § 3, Rdnr. 11.

persönlichen und sachlichen Verhältnissen ist in vielen Fällen nicht möglich, allerdings auch nicht notwendig, da das Gesetz insoweit keine differenzierenden Vorgaben enthält[197]. Zu den Angaben über persönliche Verhältnisse zählen beispielsweise Identifikationsmerkmale (Name, Anschrift, Geburtsdatum etc.), äußere Merkmale (Geschlecht, Gewicht, Größe, Augenfarbe etc.) sowie innere Zustände (Meinungen, Werturteile, Überzeugungen etc.).

Als Angaben über sachliche Verhältnisse sind zum Beispiel die Vermögens- oder Eigentumsverhältnisse oder auch alle sonstigen Beziehungen zu Dritten und zur Umwelt zu klassifizieren[198]. Die Angaben müssen sich nicht zwingend unmittelbar auf eine bestimmte Person beziehen. Es reicht aus, wenn ein Bezug zu ihr hergestellt werden kann[199]. Damit ist eine Bezugsperson bestimmbar, wenn die Person zwar nicht unbedingt allein anhand der Daten identifiziert werden kann, sie allerdings mittelbar erkennbar und individualisierbar ist.

Die dezentralisierte Konzeption des Internet führt dazu, dass personenbezogene Daten regelmäßig nicht an einem Ort, sondern an vielen unterschiedlichen Stellen gespeichert werden. Beim Suchmaschinenanbieter *Google* wird beispielsweise vermutet, dass er weltweit mehr als eine Million Server in mindestens 13 Rechenzentren betreibt[200].

Da es personenbezogene Daten in vielfältiger Form gibt, können die unterschiedlichen Daten in verschiedene Datenkategorien unterteilt werden. Dabei kann insbesondere nach Bestandsdaten, Verkehrsdaten[201] und Inhaltsdaten differenziert werden.

Bestandsdaten sind nach der Definition in § 3 Nr. 3 TKG die Daten eines Teilnehmers, die „für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden“[202]. Die Bestandsdaten haben keinen besonderen Bezug zum jeweiligen Kommunikationsvorgang, sondern sind die Basisdaten, die für das Vertragsverhältnis erforderlich sind[203]. Zu den Bestandsdaten zählen beispielsweise Name und Anschrift des Nutzers, Kontoverbindung und Art des kontrahierten Dienstes[204]. Auf die Bestandsdaten kann die Polizei bei den verdachtsunabhängigen Ermittlungen im virtuellen

197 *Fröhle*, Web advertising, Nutzerprofile und Teledienstedatenschutz, 2003, S. 85; *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2008, S. 101, m. w. N.

198 *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2008, S. 101.

199 *Gola/Klug*, Grundzüge des Datenschutzrechts, 2003, S. 40 ff.

200 Vgl. *http://www.joergo.de/google.html*; *Ott*, MMR 2009, 158, 159.

201 Verkehrsdaten werden teilweise auch als Verbindungsdaten bezeichnet.

202 Vgl. dazu die ähnliche Bestimmung in § 14 Abs. 1 TMG zu Bestandsdaten.

203 *Gausling*, Verdachtsunabhängige Speicherung von Verkehrsdaten auf Vorrat, 2010, S. 10.

204 *Holznagel/Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl., 2011, § 3 TKG, Rdnr. 5.

Bereich grundsätzlich nicht zugreifen, da diese Daten beim Diensteanbieter gespeichert und daher nicht öffentlich zugänglich sind.

Verkehrsdaten sind die Daten eines an der Telekommunikation Beteiligten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (§ 3 Nr. 30 TKG). Im Unterschied zu Bestandsdaten beziehen sich Verkehrsdaten auf einen konkreten Telekommunikationsvorgang und geben Auskunft, von welchem Anschluss wann mit wem wie lange kommuniziert wurde[205]. Zu den Verkehrsdaten gehören beispielsweise die Rufnummer oder sonstige Kennung der jeweiligen Endeinrichtung, Zeitpunkt und Dauer der Verbindung, die übermittelten Datenmengen sowie sonstige zum Aufbau und zur Aufrechterhaltung sowie zur Entgeltabrechnung erforderliche Verkehrsdaten[206]. Diese Verkehrsdaten sind in der Regel nicht öffentlich zugänglich und können somit auch nicht von der Polizei im Rahmen ihrer verdachtsunabhängigen Ermittlungen abgerufen werden.

Bei den Inhaltsdaten handelt es sich um die Daten, mit denen sich der typische Nutzer des Internet zumeist befassen wird. Die Inhaltsdaten sind die Daten[207], die die eigentlichen Nachrichten und Informationen enthalten[208]. Zu den Informationen und Nachrichten, die ausgetauscht oder bereitgestellt werden, gehören beispielsweise der Text einer E-Mail, die Bilder und der Text einer Homepage, News-Artikel oder die Texte in einem Chat[209]. Die Inhaltsdaten sind für die Begutachtung dieser Arbeit besonders relevant, da sich die Polizei bei ihren verdachtsunabhängigen Ermittlungen im Internet zunächst wie ein gewöhnlicher nichtstaatlicher Nutzer verhält. Dadurch kann sie bei ihren Ermittlungen vorerst nur Inhaltsdaten erheben, also beispielsweise Daten aus Einträgen in Webforen oder bestimmte Texte oder Bilder auf Webseiten. In einem nächsten Schritt, wenn die staatliche Stelle beispielsweise einen rechtswidrigen Inhalt auf einer Webseite entdeckt hat, kann sie die zugehörigen Bestands- und/oder Verkehrsdaten zum Inhaltsanbieter beim Provider abfragen.

205 *Gausling*, Verdachtsunabhängige Speicherung von Verkehrsdaten auf Vorrat, 2010, S. 9.

206 Vgl. *Säcker*, in: ders., TKG, 2. Aufl., 2009, § 3, Rdnr. 96. Siehe dazu auch die Aufzählung in § 96 Abs. 1 Satz 1 TKG.

207 Die Begriffe „Daten“ und „Informationen“ werden zumeist synonym benutzt. Zur Unterscheidung von Daten und Informationen siehe *Albers*, Umgang mit personenbezogenen Informationen und Daten, in: *Hoffmann-Riem*, Grundlagen des Verwaltungsrechts, Bd. 2, 2008, § 22, Rdnr. 8 ff.

208 *Gundermann*, K&R 1998, 48 ff.; *Köhntopp/Köhntopp*, Datenspuren im Internet, CR 2000, 248, 250. Für den Begriff „Inhaltsdaten“ gibt es grundsätzlich keine gesetzliche Definition (Ausnahme: § 38b Abs. 6 Fernmeldeordnung, inzwischen aufgehoben).

209 Vgl. *Köhntopp/Köhntopp*, Datenspuren im Internet, CR 2000, 248, 250. Zur Frage, was Information eigentlich ist, bietet Hoeren einen interessanten Definitionsversuch, vgl. *Hoeren*, Zur Einführung: Informationsrecht, JuS 2002, S. 947 ff.

Neben den genannten Datenkategorien gibt es noch weitere Datengruppen[210]. Abrechnungsdaten werden zum Zwecke der Abrechnung mit dem Nutzer erhoben und werden in der Regel aus den Verkehrs- und Bestandsdaten sowie gegebenenfalls weiteren Daten abgeleitet. Bei den Standortdaten handelt es sich um Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben (vgl. § 3 Nr. 19 TKG)[211]. Durch mobile Endgeräte gewinnen Standortdaten eine stetig wachsende Bedeutung, etwa bei der Ortung von Personen[212].

Einen Sonderfall stellen IP-Adressen dar, bei denen die Eigenschaft als personenbezogenes Datum in verschiedener Hinsicht umstritten ist[213]. Zunächst ist danach zu differenzieren, ob es sich um statische oder dynamische IP-Adressen handelt. Eine statische IP-Adresse wird einem bestimmten Internetanschluss fest zugewiesen, womit eine dauerhafte Verknüpfung besteht. Bei jeder Nutzung des Internet wird daher immer dieselbe IP-Adresse genutzt[214]. Dem Großteil der Nutzer und insbesondere privaten Nutzern wird allerdings bei jeder neuen Einwahl jeweils eine neue IP-Adresse vom Access-Provider zugewiesen[215]. Diese sogenannten dynamischen IP-Adressen ermöglichen so eine effizientere Nutzung der nur begrenzt vorhandenen IP-Adressen.

Für die statischen IP-Adressen wird mittlerweile nach ganz herrschender Meinung die Eigenschaft als personenbezogene Daten angenommen, zumin-

210 Nicht näher eingegangen wird auf Nutzungsdaten im Sinne des § 15 TMG, die Daten aus mehreren verschiedenen Datenkategorien sein können, vgl. dazu *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl., 2011, § 15 TMG, Rdnr. 2 ff.

211 Der Begriff der „Standortdaten" wurde im Rahme der Umsetzung der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation, EK-DSRL), ABl. EG Nr. L 201 in das TKG eingefügt. Hierzu ausführlich *Ohlenburg*, MMR 2003, 82, 86; *dies.*, MMR 2004, 431, 436.

212 Siehe zum Einsatz des IMSI-Catchers beispielsweise *Harnisch/Pohlmann*, NVwZ 2009, 1328 ff.

213 Vgl. zum Streitstand z. B. *Meyerdierks*, MMR 2009, 8 ff.; *Voigt*, MMR 2009, 377, 378 ff.

214 Eine statische IP-Adresse kann daher auch zu den Bestandsdaten gezählt werden, vgl. *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 2005, 4. Aufl., S. 282.

215 Mit der Einführung von IPv6 gibt es allerdings ausreichend IP-Adressen, die eine statische Zuordnung fördern könnten, vgl. *Hoeren*, ZRP 2010, 251, 252 ff. Durch die Ausbreitung statischer IP-Adressen entstehen neue Gefahren für verschiedene Grundrechte, wie das Bundesverfassungsgericht zutreffend festgestellt hat. Den Gesetzgeber treffe insoweit eine „Beobachtungs- und gegebenenfalls Nachbesserungspflicht", BVerfG, 1 BvR 1299/05 vom 24.01.2012, Absatz 161.

dest soweit sie einer natürlichen Person zugeordnet werden können[216]. Zwar ist auch bei einer statischen IP-Adresse nicht unbedingt klar, welche natürliche Person sich nun genau zu dem betreffenden Zeitpunkt auf beispielsweise einer bestimmten Webseite befunden hat, da im Regelfall verschiedene Personen über eine statische IP-Adresse das Internet nutzen. Allerdings wird auch eine Telefonnummer den personenbezogenen Daten zugeordnet, obwohl nicht genau gesagt werden kann, wer ein Telefonat geführt hat[217]. Ebenso werden auch die Kfz-Kennzeichen zu den personenbezogenen Daten gezählt[218]. Auf den ersten Blick lässt sich der Halter eines Kraftfahrzeuges durch das Kfz-Kennzeichen nicht identifizieren. Die Zulassungsstelle kann aber die Auskunft zum Halter des Kraftfahrzeuges geben. Welche natürliche Person das Kraftfahrzeug beispielsweise bei einer Geschwindigkeitsüberschreitung geführt hat, kann auch nicht allein anhand der Halterauskunft exakt bestimmt werden. Dies wird auch für die Einordnung als personenbezogenes Datum nicht gefordert. Sowohl das Kfz-Kennzeichen als auch die Telefonnummer genügen zur genauen Identifikation des Halters bzw. Anschlussinhabers. Dass dabei gegebenenfalls eine Strafverfolgungsbehörde oder eine sonstige Behörde detailliertere Informationen benötigt, ist für diese Einordnung irrelevant. Es reicht aus, dass ein Personenbezug zwischen der Telefonnummer oder dem Kfz-Kennzeichen und einer bestimmten Person hergestellt werden kann[219]. Somit ist es für die grundsätzliche Qualifikation einer statischen IP-Adresse als personenbezogenes Datum unbeachtlich, dass unterschiedliche Personen den Internet-Zugang nutzen können.

Bezüglich der dynamischen IP-Adressen besteht insoweit Uneinigkeit. Der Anknüpfungspunkt für die verschiedenen Ansichten ist der Personenbezug der Daten. Ein personenbezogenes Datum setzt voraus, dass die betroffene natürliche Person bestimmt oder zumindest bestimmbar ist.

Nach der Theorie der absoluten Personenbezogenheit ist eine Person bestimmbar, wenn abstrakt für irgendjemanden, also nicht lediglich für denjenigen, der über die Daten verfügt, die Möglichkeit besteht, die Daten einer

216 *Schmitz*, in: Hoeren/Sieber, Hdb. Multimediarecht, Teil 16.2, Rdnr. 79 ff.; *Dammann*, in: Simitis, BDSG, 2006, 6. Aufl., § 3, Rdnr. 63; *Iraschko-Luscher/Kiekenbeck*, RDV 2010, 261, 265; *Eckhardt*, ITRB 2005, 46, 47; *Steidle/Pordesch*, DuD 2008, 324, 327; vgl. auch BVerfG, 1 BvR 1299/05 vom 24.01.2012, insbesondere Absatz 161; BVerfGE 125, 260, 341 ff.; Teilweise wird auch eine Ansicht vertreten, die eine differenzierte Einzelfallbetrachtung bei statischen IP-Adressen vorsieht, so z. B. *Härting*, CR 2008, 743, 745; *Voigt*, MMR 2009, 377, 380.

217 Vgl. *Gola/Schomerus*, BDSG, 11. Aufl., 2012, § 3 Rdnr. 3; Das Bundesverfassungsgericht zieht ebenfalls die Parallele zu Telefonnummern, vgl. BVerfG, 1 BvR 1299/05 vom 24.01.2012, insbesondere Absatz 161; BVerfGE 125, 260, 341 ff.

218 Vgl. BVerfGE 120, 378, 397 ff.

219 So auch *Perry*, Gefahrenabwehr und Internet, 2003, S. 139.

konkreten Person zuzuordnen[220]. Zur Herstellung des Personenbezugs könnten dabei unter Umständen auch mehrere Zwischenschritte notwendig sein[221]. Mit Inkrafttreten der Regelungen zur Vorratsdatenspeicherung bestand gemäß § 113a TKG eine Pflicht zur Speicherung der Verkehrsdaten durch die Diensteanbieter. In dem Urteil vom 2. März 2010[222] erklärte das Bundesverfassungsgericht die §§ 113a, 113b TKG und § 100g Abs. 1 Satz 1 StPO, soweit nach dieser Norm Verkehrsdaten gemäß § 113a TKG erhoben werden dürfen, wegen Verstoßes gegen das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG für nichtig[223]. Damit müssen die Access-Provider innerhalb des vorgeschriebenen Speicherzeitraums von sechs Monaten die IP-Adressen als Verkehrsdatum nicht mehr speichern. Die Umsetzung einer Vorratsdatenspeicherung ist aber auch nach Ansicht des Bundesverfassungsgerichts nicht schlechthin unvereinbar mit dem Grundgesetz[224]. Daher ist damit zu rechnen, dass die Vorratsdatenspeicherung in einer abgewandelten Form wieder eingeführt wird[225]. Die Access-Provider werden dann voraussichtlich wieder zur Speicherung der IP-Adressen verpflichtet sein[226]. Da zumindest dieser Provider dann einen Personenbezug herstellen kann, handelt es sich bei den dynamischen IP-Adressen nach dieser Ansicht allgemein um personenbezogene Daten. Insbesondere unter den Datenschutzbeauftragten ist dieser weite Begriff der Personenbezogenheit auffallend verbreitet, da er einen umfassenden Datenschutz gewährleistet[227].

220 *Schaar*, Datenschutz im Internet, 2002, Rdnr. 175; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl., 2010, § 3, Rdnr. 13; *Pahlen-Brandt*, K&R 2008, 288; *Wagner*, Das Websurfen und der Datenschutz, 2006, S. 163 ff.

221 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl., 2010, § 3, Rdnr. 13.

222 BVerfG, 1 BvR 256/08 vom 02.03.2010.

223 Vgl. dazu z. B. *Gausling*, Verdachtsunabhängige Speicherung von Verkehrsdaten auf Vorrat, 2010, S. 215 ff.; *Zimmer*, Zugriff auf Internetzugangsdaten, 2012, S. 138 ff.; *Eckhardt*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl., 2011, § 113a TKG, Rdnr. 21 ff.; *Eckhardt/Schütze*, CR 2010, 225, 226 ff.

224 Vgl. *Gausling*, Verdachtsunabhängige Speicherung von Verkehrsdaten auf Vorrat, 2010, S. 215 ff.

225 Siehe dazu beispielsweise den Vorschlag von *Schramm/Wegener*, MMR 2011, 9 ff.; vgl. auch *Britz*, JA 2011, 81 ff.; *Möstl*, ZRP 2011, 225 ff.

226 § 111 TKG verpflichtet geschäftsmäßige Anbieter von Telekommunikationsdiensten bereits zur Speicherung verschiedene personenbezogener Daten, wie beispielsweise die Rufnummer und den Namen des Anschlussinhabers.

227 U.a. vertreten vom Bundesbeauftragten für Datenschutz *Schaar*, Datenschutz im Internet, 2002, Rdnr. 175; Datenschutzbeauftragter des Landes Schleswig-Holstein *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl., 2010, § 3, Rdnr. 13; Berliner Datenschutzbeauftragter *Dix*, Tätigkeitsbericht 2004, S. 152; Europäischer Datenschutzbeauftragter *Hustinex*, Stellungnahme zum IMCO-Protokoll, *http://tinyurl.com/b89vcb*; Datenschutzbeauftragte der Universität Berlin *Pahlen-Brandt*, K&R 2008, 288.

Auch das Bundesverfassungsgericht scheint dieser Theorie im Ergebnis zu folgen[228].

Nach der Theorie der relativen Personenbezogenheit ist der Personenbezug bei der jeweils verarbeitenden Stelle zu prüfen[229]. Danach könne folglich für die eine Stelle, zum Beispiel für den Access-Provider, die IP-Adresse ein personenbezogenes Datum sein, da der Access-Provider den Personenbezug herstellen könne, während für eine andere Stelle der Personenbezug nicht möglich sei und somit kein personenbezogenes Datum vorliege. Allerdings soll nach dieser Ansicht für den Personenbezug ausreichen, wenn der Dateninhaber selbst mit vertretbarem Aufwand die tatsächliche Möglichkeit der Zuordnung hat[230].

Die Theorie der relativen Personenbezogenheit wird den heutigen Anforderungen an ein modernes Datenschutzsystem nicht gerecht. Bereits der 26. Erwägungsgrund der EU-Datenschutzrichtlinie[231] forderte, dass bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden sollen, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten. Somit sollte es für den geforderten Personenbezug ausreichend sein, wenn die Identifikation erst durch die Zusammenführung der Daten verschiedener Stellen möglich wird. Der in diesem Zusammenhang vorgebrachte Einwand, dass die Zusammenführung der Daten unterschiedlicher Stellen in vielen Fällen rechtlich unzulässig sein dürfte[232], vermag nicht zu überzeugen. Der Umgang mit Daten in der informationstechnologisch beherrschten Realität verdeutlicht regelmäßig der Gesellschaft, dass rechtliche Zulässigkeitsgrenzen nicht nur verschwimmen, sondern oftmals förmlich unbeachtet bleiben[233]. Auch der Bundesgerichtshof sieht in einer aktuellen Entscheidung den Personenbezug von dynamischen IP-Adressen als gegeben an[234], ähnlich das Bundesverfassungsgericht[235].

Auf europäischer Ebene äußerte sich der Europäische Gerichtshof in einer Entscheidung zur Zulässigkeit von Filtersystemen am Rande zur Qualifikation von IP-Adressen als personenbezogene Daten[236]. Zukünftig ist ferner

228 Vgl. BVerfG, 1 BvR 1299/05 vom 24.01.2012, Absätze 161 ff.; BVerfGE 125, 260, 341 ff.

229 *Dammann*, in: Simitis, BDSG, 2006, 6. Aufl., § 3, Rdnr. 33, 35; *Gola/Schomerus*, BDSG, 11. Aufl., 2012, § 3, Rdnr. 10; *Roßnagel/Scholz*, MMR 2000, 721, 723; *Arning/Forgó/Krügel*, DuD 2006, 704; *LG Frankenthal*, MMR 2008, 687; *Hornung*, DuD 2004, 429.

230 *Voigt*, MMR 2009, 377, 379 m. w. N.

231 RL 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

232 *Meyerdierks*, MMR 2009, 8, 12.

233 Im Ergebnis ebenso *Wagner*, Das Websurfen und der Datenschutz, 2006, S. 164.

234 BGH, Urteil vom 13.01.2011, III ZR 146/10; vgl. dazu auch *Karg*, der die vorhergehenden Entscheidungen kurz aufzeigt, *Karg*, MMR-Aktuell 2011, 315811.

235 BVerfG, 1 BvR 1299/05 vom 24.01.2012, Absätze 161 ff.; BVerfGE 125, 260, 341 ff.

236 EuGH, Urteil vom 24.11.2011, C-70/10.

mit einer umfassenden Reform des EU-Datenschutzrechts zu rechnen, um Nutzern mehr Kontrolle über ihre personenbezogenen Daten zu geben[237].

1. Datenspuren im Internet

Jeder Nutzer des Internet hinterlässt, beabsichtigt oder unbeabsichtigt, Datenspuren[238]. Für den Nutzer in der Regel leicht zu erkennen ist die Entstehung von Inhaltsdaten, die er im Internet hinterlässt. Diese können eingeteilt werden in Daten, die einer unbestimmten Adressatenzahl zugänglich sind, und in Daten, die für einen bestimmten Adressatenkreis konzipiert sind. Für die Allgemeinheit zugänglich sind beispielsweise die Inhalte von Webseiten im Internet, für die keine Zugangsbeschränkungen bestehen. Der Anbieter der Webseiten hat diese bewusst in das Internet gestellt, damit die Daten weltweit uneingeschränkt eingesehen werden können. Schreibt ein Nutzer hingegen eine E-Mail, so möchte er sich grundsätzlich nur an einen bestimmten oder mehrere bestimmte Adressaten wenden. Soweit ein Diensteanbieter nicht möchte, dass etwa bestimmte Webseiten öffentlich zugänglich sind, kann er den Zugang zu diesen Webseiten beschränken, indem beispielsweise ein Passwort eingegeben werden muss.

Neben diesen vom Nutzer selbst verfassten Inhaltsdaten entstehen im Rahmen der Internetnutzung eine Vielzahl anderer Daten, wie beispielsweise Bestands-, Abrechnungs-, Nutzungs- oder Verkehrsdaten. Bei einer einfachen WWW-Anfrage kann bei unterschiedlichen Providern eine enorme Menge an Daten entstehen[239], über die der laienhafte Nutzer nicht viel weiß. Der Betreiber einer Webseite erfährt vom Nutzer entweder automatisch oder auf Anfrage beispielsweise das Betriebssystem des vom Nutzer verwendeten Rechners, den genutzten Browser, die E-Mail-Adresse, soweit sie im Browser gespeichert ist, sowie die zuletzt aufgerufenen Webseiten[240]. Jeder Nutzer ist sich wahrscheinlich schon bewusst, dass neben den von ihm eingegebenen Daten noch weitere entstehen, jedoch wird kaum ein Nutzer das Ausmaß abschätzen können.

2. Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Internet

Im Internet ist eine fast unendliche Anzahl personenbezogener Daten vorhanden. Diese Daten werden von verschiedenen Stellen erhoben, verarbeitet und genutzt. Erheben ist das Beschaffen von Daten über den Betroffenen

237 Vgl. Pressemitteilung der EU-Kommission vom 25.01.2012 (IP/12/46).

238 Vgl. dazu *Hornung*, MMR 2004, 3, 5 ff.; *Köhntopp/Köhntopp*, CR 2000, 248 ff.; *Spiegel*, DuD 2003, 265 ff.

239 Die Datenspuren, die beim WWW-Abruf entstehen, werden dargestellt bei *Köhntopp/Köhntopp*, CR 2000, 248, 250 ff.

240 *Spiegel*, DuD 2003, 265 ff.

(§ 3 Abs. 3 BDSG). Obwohl in § 3 Abs. 3 BDSG nicht direkt von personenbezogenen Daten die Rede ist, sondern lediglich auf Daten abgestellt wird, ergibt sich aus der Verwendung des Begriffs des Betroffenen, dass nicht jede Art von Daten gemeint ist, sondern nur personenbezogene Daten erfasst werden sollen[241].

Die Verarbeitung von Daten umfasst das Speichern, Verändern, Übermitteln, Sperren und Löschen von personenbezogenen Daten (§ 3 Abs. 4 BDSG). Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt (§ 3 Abs. 5 BDSG). Sowohl Privatpersonen und Unternehmen als auch die öffentliche Gewalt erheben, verarbeiten und nutzen Daten. Daher gilt das BDSG gemäß § 1 Abs. 2 BDSG für den Umgang mit personenbezogenen Daten durch öffentliche Stellen und durch nicht-öffentliche Stellen[242].

Für das Datenschutzrecht gilt der in § 3a BDSG konkretisierte Grundsatz der Datenvermeidung und Datensparsamkeit. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten soll soweit wie möglich vermieden werden, damit Gefahren für das Recht auf informationelle Selbstbestimmung des Betroffenen von vornherein minimiert werden können[243]. Falls doch personenbezogene Daten erhoben werden, soll realisierbarst von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch gemacht werden.

Der Grundsatz des Verbots mit Erlaubnisvorbehalt beherrscht das gesamte Datenschutzrecht[244]. Danach ist zunächst jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten verboten. Eine Zulässigkeit kann sich nur ergeben, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat[245].

241 *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2008, S. 110.

242 § 1 Abs. 2 BDSG unterteilt die öffentlichen Stellen in die des Bundes und in die der Länder. Das BDSG gilt für die öffentlichen Stellen der Länder nur, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt. Das BDSG kommt gemäß § 1 Abs. 2 Nr. 3 BDSG bei nicht-öffentlichen Stellen nur dann zur Anwendung, wenn sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten. Dazu *Dammann*, in: Simitis, BDSG, 6. Aufl., 2006, § 1 Rdnr. 136 ff.

243 *Gola/Klug*, Grundzüge des Datenschutzrechts, 2003, S. 46 ff.

244 Der Grundsatz des Verbots mit Erlaubnisvorbehalt ist beispielsweise in § 4 BDSG normiert.

245 Zur Einwilligung des Betroffenen siehe *Härting*, CR 2011, 169 ff.; *Gabel*, ZUM 2002, 607, 610 ff.; *Schaar*, MMR 2001, 644 ff.; *Zscherpe*, MMR 2004, 723 ff.

2.1 Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch nicht-öffentliche Stellen

Bevor die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch öffentliche Stelle und insbesondere die Polizei dargestellt wird, sollen kurz die dahingehenden Möglichkeiten nicht-öffentlicher Stellen erörtert werden. Zu den nicht-öffentlichen Stellen gehören natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts (§ 2 Abs. 4 BDSG).

Die nicht-öffentlichen Stellen verfolgen mit der Erhebung von Daten die unterschiedlichsten Zwecke. Ein Privatmann wird in der Regel personenbezogene Daten ohne kommerzielle Absichten erheben, sondern beispielsweise eine Adresse oder Telefonnummer zur Kontaktaufnahme suchen. Für solche rein persönlichen oder familiären Tätigkeiten sind die datenschutzrechtlichen Bestimmungen grundsätzlich nicht anwendbar[246].

Unternehmen und insbesondere Onlinedienste verfolgen mit der Erhebung von Daten in vielen Fällen andere Ziele. Personenbezogene Daten sind für Unternehmen immer dann von besonderem Interesse, wenn sie einen wirtschaftlichen Wert haben[247]. Ein wirtschaftlicher Wert liegt beispielsweise für Daten über einen Kunden vor, die Aussage über die Bonität treffen. Die Daten eines Nutzers werden zudem oftmals genutzt, um gezielt Werbung zu platzieren[248].

Mithilfe von Fragebögen, Gewinnspielen oder ähnlichen Lockmitteln versuchen Unternehmen, die Daten von potenziellen Kunden zu erlangen, um systematisch und effektiv zu werben. Da die Daten im Internet global und zumeist dauerhaft gespeichert sind, können sie von jedem Internetanschluss der Welt eingesehen werden[249].

Bei jedem Abruf eines Dienstes entstehen Daten, die von dem Anbieter des Dienstes sowie von allen an der Übertragung der Daten beteiligten Unternehmen genutzt werden können. Soweit keine statische IP-Adresse vorliegt, erhält ein Rechner bei jeder Verwendung des Internet eine IP-Adresse, die von den verschiedenen Diensteanbietern gespeichert werden kann[250]. Mit der IP-Adresse und den weiteren Daten kann ein bestimmter Nutzer beziehungsweise eine bestimmte Nutzergruppe ermittelt werden. Dadurch können individuelle Benutzergewohnheiten und Interessen-

246 Vgl. § 1 Abs. 2 Nr. 3 BDSG.

247 Zum Wert von personenbezogenen Daten siehe *Weichert*, NJW 2001, 1463 ff.

248 *Determann*, Kommunikationsfreiheit im Internet, 1999, S. 58 ff.

249 Auch gelöschte Daten sind größtenteils noch im Internet aufzurufen, da sie sich im Netz gespiegelt haben. Dazu *Hilgendorf/Hong*, K&R 2003, 168, 171.

250 Zwar werden den Nutzern des Internet oft von den Zugangsanbietern dynamische IP-Adressen zugeteilt, jedoch haben zumindest die Zugangsanbieter die Möglichkeit, die wechselnden IP-Adressen bestimmten Rechnern zuzuordnen.

schwerpunkte erkannt werden, womit die Möglichkeit besteht, ein Nutzerprofil einer Person oder zumindest einer Personengruppe zu erstellen[251]. Da das Internet in immer mehr Lebensbereiche vordringt, werden die Nutzerprofile fortwährend genauer und umfassender[252].

Die Anbieter von Diensten im Internet sind stets auf der Suche nach neuen Methoden, um die Nutzer ausspähen zu können[253]. Altbekannt sind in diesem Zusammenhang Cookies[254]. Bei den Cookies handelt es sich um Informationen, zumeist eindeutige Identifikationsnummern, die durch den Aufruf der Website erzeugt und dem Browser übermittelt werden. Der Browser legt diese Informationen dann in einer Datei oder in einem speziellen Verzeichnis für Cookies ab. Bei jeder der folgenden Verbindungen zu diesem Server übermittelt der Browser die gespeicherten Informationen (Cookies), wie beispielsweise bevorzugte Waren eines Nutzers im Online-Shop oder Passwörter an den Server[255]. Da die Möglichkeiten der Nutzer, sich vor Cookies zu schützen, relativ einfach geworden sind, werden immer häufiger sog. „Web-Bugs“[256] eingesetzt. Bei Web-Bugs handelt es sich nicht wie bei Cookies um Textdateien, sondern um extrem kleine, zumeist 1×1 Pixel große Grafiken, die für den Nutzer nicht erkennbar sind, da sie transparent oder an den Hintergrund angepasst sind. Ein Anbieter kann sie an jeder beliebigen Stelle einer Website einrichten[257].

251 Weiterführendes zu Nutzerprofilen bzw. Customer Profiles bieten *Hornung*, MMR 2004, 3, 5 ff.; *Ladeur*, MMR 2000, 715, 718 ff.; *Rasmussen*, CR 2002, 36 ff.; *Schaar*, CR 1996, 170 ff.; *Taeger*, K&R 2003, 220 ff.

252 Die verschiedenen Informationen werden oft in Datenlagern (sog. „Data-Warehouses“), die die Daten ordnen und vernetzen, gesammelt. Dadurch können die Nutzerdaten systematisch verknüpft werden und somit noch detailliertere Nutzerprofile erstellt werden. Außerdem werden Kundenprofile an Dritte verkauft, die diese mit eigenen Daten zusammen verarbeiten können (sog. „Data Mining“). Siehe dazu bereits *Boehme-Neßler*, CyberLaw, 2001, S. 302 ff.

253 Siehe dazu *Koch*, ITRB 2011, 158 ff.

254 Vertiefend *Härting*, CR 2008, 743 ff.; *Bizer*, DuD 1998, 277 ff.; *Eichler*, K&R 1999, 76; *Ihde*, CR 2000, 413 ff.; *Köhntopp/Köhntopp*, CR 2000, 248, 252; *Schaar*, Datenschutz im Internet, 2002, S. 177 ff.; *Spiegel*, DuD 2003, 265, 266; zur Frage, ob es sich bei Cookies um personenbezogene Daten handelt, siehe *Ott*, K&R 2009, 308; *Iraschko-Luscher/Kiekenbeck*, RDV 2010, 261, 265.

255 Die temporären Cookies übermitteln diese Informationen nicht, da sie sich unmittelbar nach dem Beenden des Browsers löschen. In den meisten Fällen werden aber persistente Cookies gesetzt, die zumindest für einen gewissen Zeitraum gespeichert werden.

256 Web-Bugs werden harmloser auch als Netzbojen, Clear-Gifs oder 1-Pixel-Bilder bezeichnet. Weiterführendes zu Web-Bugs bieten *Köhntopp/Köhntopp*, CR 2000, 248, 253; *Bizer*, in: Roßnagel, Hdb. der Multimedia-Dienste, 3. Teil, § 4, Rdnr. 175 ff.; *Spiegel*, DuD 2003, 265, 266; *Woitke*, MMR 2003, 310 ff.

257 Häufig sind sie in Werbebannern verborgen. Es muss sich aber nicht bei jeder unsichtbaren Grafik zwingend um einen Web-Bug handeln, da sie auch zum Ausrichten von Grafiken auf Websites genutzt werden. In einem solchen Fall werden allerdings die Grafiken nicht von einem dritten Server geladen, sondern sind auf der aufgerufenen Website enthalten, was dann im HTML-Quellcode erkennbar ist. Siehe hierzu *Woitke*, MMR 2003, 310 ff.

Neben den hier vorgestellten Möglichkeiten gibt es noch einige weitere Methoden zur Datenerhebung, wie beispielsweise die Auswertung der HTTP-Header-Informationen, aktive Programme oder die FTP-Abrufe, auf die hier nicht weiter eingegangen werden soll[258]. Es bestehen somit viele Mittel für Unternehmen, Daten ihrer Kunden oder sonstiger Personen zu erheben und zu nutzen. Aus diesem Grund sind sog. Privacy Policies[259] in der E-Commerce-Praxis oder bei sonstigen Dienstleistungen im Internet ein wichtiges Instrument zur Sicherstellung eines vertrauensvollen Umgangs mit Daten[260]. In diesen Datenschutzrichtlinien erhalten die Kunden Informationen über die Erhebung und Verwendung ihrer Daten und über ihre Rechte, diesem entgegenzuwirken. In der Realität beklagen jedoch viele Anbieter den Umfang der zu erfüllenden Regelungen, und die Nutzer verzagen häufig an den endlosen, vorformulierten Klauseln.

2.2 Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch die Polizei

Die soeben dargestellten Möglichkeiten der Datenerhebung und -verarbeitung im Internet stehen selbstverständlich nicht nur den nicht-öffentlichen Stellen zur Verfügung, sondern auch den öffentlichen Stellen und der Polizei. Die Polizei kann beispielsweise, wie jeder andere Nutzer auch, die öffentlich zugänglichen Inhalte im Internet aufrufen. Neben diesen Mitteln kann die Polizei noch weitere Methoden einsetzen, um umfassend und effizient Daten zu erfassen[261]. Durch die technischen Entwicklungen und das veränderte Kommunikationsverhalten hat sich das Potential für Überwachung, Gefahrenvorsorge und Strafverfolgung erweitert[262]. Im Folgenden wird ohne eine Wertung der rechtlichen Zulässigkeit dargestellt, welche Möglichkeiten die Polizei zur Datenerhebung und Datenverarbeitung hat.

2.2.1 Erhebung von personenbezogenen Daten

Gesetzlich wird das Erheben als das Beschaffen von Daten über den Betroffenen definiert[263]. Dies setzt zunächst nach allgemeiner Auffassung ein aktives Tun durch die erhebende Stelle voraus[264]. Damit liegt beispielsweise

258 Siehe dazu *Köhntopp/Köhntopp*, CR 2000, 248, 252 ff.; *Bizer*, in: Roßnagel, Hdb. der Multimedia-Dienste, 3. Teil, § 4, Rdnr. 177 ff.; *Spiegel*, DuD 2003, 265, 266 ff.

259 Der Begriff der „Privacy Policy" beschreibt eigentlich die (Selbst-)Verpflichtung, sich bezüglich der Privatsphäre Dritter auf eine bestimmte Art und Weise zu verhalten. Vgl. dazu *Tröndle*, „Privacy Policies" und das Internet, CR 1999, 717 ff.

260 Zu Privacy Policy und Datenschutzklauseln vgl. *Bizer*, DuD 2002, 386.

261 Vgl. dazu beispielsweise *Singelnstein*, NStZ 2012, 593 ff.

262 Vgl. *Albrecht/Grafe/Kilchling*, Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO, 2008, S. 7 ff.

263 Vgl. § 3 Abs. 3 BDSG.

264 *Dammann*, in: Simitis, BDSG, 2006, 6. Aufl., § 3, Rdnr. 102 ff.; *Schaar*, Datenschutz im Internet, 2002, Rdnr. 190.

keine Erhebung von Daten vor, wenn die Polizei Daten ohne eigene Mithilfe, etwa durch zufällige Wahrnehmung oder durch unaufgeforderte Übersendung erhält[265]. Keine Datenerhebung liegt folglich vor, wenn ein Bürger der Polizei Informationen über eine Straftat übermittelt. Hingegen erhebt ein Polizist Daten, wenn er durch die Fußgängerzone geht und Passanten gezielt nach Auffälligkeiten mustert, die ein Tätigwerden notwendig machen könnten[266].

Für den Bereich des Internet bedeutet dies, dass eine öffentliche Stelle personenbezogene Daten dann erhebt, wenn sie diese über das Internet bewusst abruft. Keine Voraussetzung der Datenerhebung ist es, dass die erhobenen Daten mit dem Ziel der Verarbeitung (z. B. Speicherung) beschafft werden, wobei in der Praxis häufig gleichzeitig mit der Erhebung auch die Speicherung der Daten erfolgt[267]. Die Daten im Internet sind regelmäßig auf verschiedenen Datenspeichermedien, wie beispielsweise Festplatten, gespeichert. Hierbei ist es irrelevant, wo sich das Speichermedium befindet, wenn es mit dem Internet verbunden ist. Es kann sich also in einem Wohn- oder Geschäftsraum oder unter freiem Himmel im In- oder Ausland befinden[268].

Die Polizei kann, wie jeder andere Benutzer des Internet auch, über das Internet mit Dritten kommunizieren. Die Behörde kann dabei als aktiver Kommunikationspartner auftreten und direkt mit anderen Unterhaltungen führen. Zudem besteht die Möglichkeit, dass die Behörde passiv bleibt und Daten erhebt, die sie aus virtuellen Gesprächen zwischen zwei oder mehr Nutzern erfährt. Im Unterschied zur Überwachung kann die öffentliche Stelle in diesen Fällen frei zugängliche Kommunikationsdienste nutzen, die allen Nutzern offenstehen. Bei den Chats kann beispielsweise die öffentliche Gewalt eine Unterhaltung zwischen anderen belauschen, indem sie einen Chatraum betritt und sich passiv im Hintergrund hält. Diese Möglichkeit haben grundsätzlich auch alle anderen Internet-Nutzer. Gleichfalls kann eine staatliche Stelle die offen zugänglichen Inhalte des Internet, wie beispielsweise auf Webseiten, einsehen.

Wenn die Behörde im Gegensatz dazu einen Teilnehmer überwacht, legt sie besonderen Wert darauf, dass sie unentdeckt bleibt. Bei der gezielten Überwachung eines Teilnehmers kann die Polizei Daten erheben, die während der Nutzung des Internet entstehen beziehungsweise bei der Nutzung übertragen werden. Besonders interessant für die Polizei sind dabei die

265 *Gola/Schomerus*, BDSG, 11. Aufl., 2012, § 3, Rdnr. 24; *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2008, S. 110; *Tinnefeld*, NJW 1993, 1117.

266 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 2005, 4. Aufl., S. 499 ff. mit weiteren Beispielen.

267 *Bergmann/Möhrle/Herb*, Datenschutzrecht, Bd. 1, Teil 3, § 3 BDSG, Rdnr. 64.

268 Für die rechtliche Betrachtung kann der Zugriffsort aber relevant sein, da unterschiedliche Grundrechte betroffen sein können. Vgl. *Perrey*, Gefahrenabwehr und Internet, 2003, S. 74.

Inhaltsdaten, die über das Internet unter Anwendung von Kommunikationsdiensten verschickt und empfangen werden. Unter diese Inhaltsdaten fallen beispielsweise kinderpornografische Bilder oder Pläne zu terroristischen Anschlägen, die zwischen dem Betroffenen und mindestens einem Dritten versandt werden. Bei diesen Überwachungsmaßnahmen handelt es sich um eine Telekommunikationsüberwachung, die sich auf Internet-basierte Kommunikationsdienste bezieht. Beispiele für diese Kommunikationsdienste sind E-Mail-Dienste, Instant-Messaging-Dienste (z. B. ICQ) oder Internet-Telefonie[269].

Sobald die Kommunikation über diese Dienste allerdings verschlüsselt wird, kann die staatliche Stelle im Regelfall nicht auf dem Kommunikationsweg, auf dem die Inhalte noch verschlüsselt sind, die Daten erheben. In diesem Fall besteht die Möglichkeit einer sogenannten Quellen-Telekommunikationsüberwachung. Dafür wird der Rechner eines Betroffenen mit einer Spionagesoftware infiltriert, die vor der Verschlüsselung der Telekommunikation die Daten an die ermittelnde Stelle übermittelt[270]. Abzugrenzen davon sind die sogenannten Online-Durchsuchungen, bei denen nicht die laufende Telekommunikation überwacht wird, sondern die Daten ausgespäht werden, die sich auf dem Rechner befinden[271]. Damit handelt es sich um eine computerbezogene Durchsuchung als verdeckte Maßnahme[272].

Neben der Online-Durchsuchung und der Quellen-Telekommunikationsüberwachung gibt es als Zwischenstufe die Protokollierung der Aktivitäten am Rechner des Betroffenen, die keine Kommunikation sind[273]. Hierbei kann es sich beispielsweise um die Nutzung von Büro- oder Buchhaltungsprogrammen, die Bearbeitung von Grafiken und Fotos oder sonstige Nutzungen, die nur auf dem Rechner durchgeführt werden, handeln. Die genannten Daten können beispielsweise durch Screenshots an die Polizei übertragen werden. Diese Maßnahmen sind im Ergebnis als Anwendungsfall der Online-Durchsuchung zu qualifizieren, da sie heimlich auf dem Rechner

269 Vgl. zur E-Mail-Überwachung *Hsieh*, E-Mail-Überwachung zur Gefahrenabwehr, 2011.

270 Vgl. auch die Entscheidung des Bundesverfassungsgerichts zu Online-Durchsuchungen und Internetaufklärungen, BVerfGE 120, 274, Absätze 188 ff.

271 Siehe vertiefend zur sog. Online-Durchsuchung *Gudermann*, Online-Durchsuchung im Lichte des Verfassungsrechts, 2010; *Soiné*, NVwZ 2012, 1585 ff.; *Stadler*, MMR 2012, 18 ff.; *Herrmann/Soiné*, NJW 2011, 2922 ff.; *Roggan*, Online-Durchsuchung, 2008; *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 99; *Leisner*, NJW 2008, 2902; *Volkmann*, DVBl 2008, 590 ff.; *Britz*, DÖV 2008, 411; *Kutscha*, NJW 2008, 1042; *Böckenförde*, JZ 2008, 925; *Bartsch*, CR 2008, 613; *Hornung*, CR 2008, 299; *Stögmüller*, CR 2008, 435; *Heckmann*, in: Kluth u. a., FS Rolf Stober, 2008, S. 615; *Bär*, MMR 2008, 325.

272 *Kochheim*, Verdeckte Ermittlungen im Internet, Stand: März 2012, S. 35, abzurufen unter *http://cyberfahnder.de*.

273 Vgl. insgesamt dazu *Kochheim*, Verdeckte Ermittlungen im Internet, Stand: März 2012, S. 36, *http://cyberfahnder.de*.

des Betroffenen außerhalb einer Kommunikationsbeziehung durchgeführt werden[274].

Außer der Online-Durchsuchung kann die Polizei auch sogenannte Spyware gezielt einsetzen, um zum Beispiel ein Keylogger-Programm auf dem Rechner des Betroffenen zu installieren. Durch dieses Programm werden die Eingaben auf der Tastatur des „infizierten" Rechners an die Polizei übertragen, wodurch diese zum Beispiel die Texte einer auf dem Rechner verfassten E-Mail lesen kann.

Für die gezielte Erhebung der personenbezogenen Daten eines Betroffenen gibt es unterschiedliche Möglichkeiten, um diese entweder direkt beim Betroffenen oder bei Dritten, beispielsweise Providern, zu erheben. Die einzelnen möglichen Maßnahmen differieren daher stark in ihrer technischen Realisierbarkeit und der rechtlichen Zulässigkeit, wobei zusätzlich nach dem Zugriff auf Bestandsdaten, Verkehrsdaten, Inhaltsdaten oder sonstigen Daten unterschieden werden muss[275]. Beispielsweise kann die Polizei Dateien bei einem Provider, der für Dritte Server für Webseiten zur Verfügung stellt, beschlagnahmen. Auch der laufende Datenverkehr auf einem Server kann überwacht werden.

Um eine Vielzahl von Benutzern des Internet zu überwachen, kann eine öffentliche Stelle den Datenverkehr an einem bestimmten Netzknotenpunkt beobachten. Ein sog. Paketschnüffler (packet-sniffer) oder Filter durchsucht an diesem Knotenpunkt die einzelnen Datenpakete nach interessanten Informationen, wie beispielsweise dem Gebrauch eines bestimmten Wortes, der Rückschlüsse auf kriminelle Aktivitäten des Urhebers ziehen lässt[276]. Wenn ein Treffer vorliegt, werden die relevanten Informationen automatisch gespeichert.

2.2.2 Verarbeitung und Nutzung von personenbezogenen Daten

Die zuvor erhobenen Daten werden im Rahmen der Datenverarbeitung von der öffentlichen Stelle verwertet. Das Verarbeiten umfasst das Speichern, Verändern, Übermitteln, Sperren und Löschen von Daten[277].

Ein wesentliches Element für die Datenverarbeitung einer Behörde ist die Speicherung der erhobenen Daten. Damit können Datensammlungen angelegt werden, die repressiv oder präventiv eingesetzt werden können. Damit wird den Behörden eine Vielzahl an Möglichkeiten zur elektronischen

274 Vgl. zur Abgrenzung der einzelnen Maßnahmen LG Landshut, Beschluss vom 20.01.2011, 4 Qs 346/10.

275 Siehe zu den möglichen Ermittlungsmaßnahmen der Polizei im Internet ausführlich *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 637 ff.

276 Vgl. zu Paketschnüfflern *Kyas/Campo*, Internet professionell, 2. Aufl., 2001, S. 263 ff. sowie zu praktischen Umsetzungsmöglichkeiten und Erfolgsaussichten von sog. „elektronischen Staubsaugern" *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 279 ff.

277 Vgl. § 3 Abs. 4 BDSG. Als Nutzen bestimmt § 3 Abs. 5 BDSG grundsätzlich jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Datenverarbeitung geboten, um innerhalb kürzester Zeit wesentliche Informationen zu erhalten.

Das Internet kann außerdem als Fahndungsmittel der Strafverfolgungsbehörden genutzt werden, indem nach bestimmten Personen gesucht wird[278]. Hierzu werden die wesentlichen und bekannten Daten einer Person auf der Website einer Behörde dargestellt. Die Bevölkerung ist sodann aufgerufen, Informationen über den Verbleib der Person der Behörde zu melden.

Weiterhin können öffentliche Stellen die erhobenen Daten verarbeiten, indem sie diese an andere öffentliche Stellen übermitteln.

278 Zur Öffentlichkeitsfahndung im Internet siehe *Bär*, CR 1997, 422 ff.; *Pätzel*, NJW 1997, 3131 ff.; *Soiné*, NStZ 1997, 166 ff.; *ders.*, NStZ 1997, 321 ff.; *Wiegrefe*, CILIP 55 (1996), 67 ff.

D.
Mögliche Grundrechtsverletzungen durch verdachtsunabhängige Ermittlungen

Das Internet als rechtlich geschützter Bereich bietet den Bürgern natürlich auch den notwendigen Schutz ihrer Grundrechte. Im Internet können, wie auch im „analogen" Leben, staatliche Stellen durch ihre Maßnahmen eine Vielzahl der Grundrechte verletzen. Die Kommunikation der Beteiligten wird im Internet beispielsweise durch das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG geschützt. Den staatlichen Umgang mit personenbezogenen Daten grenzt das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts ein, um den besagten „gläsernen Menschen" zu verhindern. Auch im Internet muss ein Nutzer selbstredend nicht auf seine geschützten Rechte der Meinungs- und Informationsfreiheit (Art. 5 Abs. 1 Satz 1 GG) verzichten.

Durch die verdachtsunabhängigen Ermittlungen der Polizei im Internet können verschiedene Grundrechte berührt werden. Der rechtsdogmatische Ansatzpunkt für staatliche Ermittlungen im Internet ist immer die Frage, ob eine Maßnahme grundrechtsrelevant ist[279]. Im Folgenden wird daher untersucht, in welche Grundrechte staatliche Stellen durch die speziellen Maßnahmen im Rahmen ihrer verdachtsunabhängigen Ermittlungsmaßnahmen eingreifen.

I. Das Telekommunikationsgeheimnis (Art. 10 Abs. 1 GG)

Durch Art. 10 Abs. 1 GG wird das Brief-, Post- und Fernmeldegeheimnis geschützt. Die Vertraulichkeit individueller Kommunikation, die wegen räumlicher Distanz zwischen den Kommunikationspartnern auf eine Übermittlung durch bestimmte Medien angewiesen ist und daher einem erhöhten Risiko des Zugriffs Dritter auf die Kommunikationsinhalte unterliegt, soll durch Art. 10 Abs. 1 GG gewahrt werden[280].

Die körperliche Übermittlung von Briefen wird durch das Briefgeheimnis geschützt[281]. Damit scheidet eine Verletzung des Briefgeheimnisses durch die verdachtsunabhängigen Ermittlungen der Polizei im Internet aus, da es sich weder um Briefe noch um eine körperliche Übermittlung handelt.

279 *Brenneisen/Staack*, Kriminalistik 2012, 627.
280 *Sodan*, in: Sodan, Grundgesetz, 2009, Art. 10, Rdnr. 1.
281 Vgl. BVerfGE 67, 157, 171.

Das Postgeheimnis dient dem Schutz der Erbringung von Postdienstleistungen[282], also der körperlichen Übermittlung von Informationen und Kleingütern durch ein auf massenhaften Verkehr ausgelegtes Transportnetz[283]. Unabhängig von der Frage, ob die Bedeutung des Postgeheimnisses durch die Privatisierung der Deutschen Bundespost und den Wegfall des staatlichen Postmonopols obsolet geworden ist[284], kann der Schutzbereich hier nicht eröffnet sein, da es abermals für die zu prüfenden Konstellationen an einer körperlichen Übermittlung mangelt.

Die unkörperliche Übermittlung von Informationen wird durch das Fernmelde- bzw. Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG geschützt. Der Schutzbereich umfasst dabei die Übermittlung von Informationen durch unkörperliche, also elektrische, elektromagnetische, optische, funktechnische, analoge oder digitale Signale an individuelle Empfänger vor staatlicher Kenntniserlangung, und zwar unabhängig davon, ob Betreiber der Staat oder ein Privater ist[285]. Durch die „Verbürgung der Unverletzlichkeit des Fernmeldegeheimnisses soll vermieden werden, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form oder Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsinhalte gewinnen“[286].

Da durch das Fernmeldegeheimnis schon seit geraumer Zeit nicht mehr nur die Kommunikation über das Telefon geschützt ist, sondern sämtliche Formen der modernen Telekommunikation vom Schutzbereich umfasst werden können[287], wird im Einklang mit der Rechtsprechung des Bundes-

282 Vgl. zur Definition von Postdienstleistungen § 4 PostG.

283 Vgl. BT-Drs 12/7269, S. 4; *Jarass*, in: Jarass/Pieroth, Grundgesetz, 12. Aufl., 2012, Art. 10, Rdnr. 4.

284 Vgl. zum Streitstand *Pagenkopf*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 10, Rdnr. 13; *Gusy*, in: von Mangoldt/Klein/Starck, Grundgesetz, 6. Aufl., 2010, Art. 10, Rdnr. 35 ff. Eine in der Literatur vertretene Meinung geht davon aus, dass der grundrechtliche Schutz des Postgeheimnisses durch die Privatisierung der Deutschen Bundespost obsolet geworden ist (z. B. *Hermes*, in: Dreier, Grundgesetz, Bd. 1, 2. Aufl., 2004, Art. 10, Rdnr. 46). Als überzeugender ist die Ansicht einzuschätzen, dass trotz Postreform das Postgeheimnis dem Schutz vor staatlichen Eingriffen von außen in die postalische Beförderung dient und damit auch durch die Privatisierung der Deutschen Bundespost nicht bedeutungslos geworden ist (vgl. BVerwGE 113, 208, 211; *Bizer*, AK-GG, 3. Aufl., 2001, Art. 10, Rdnr. 56; *Hömig*, in: Hömig, Grundgesetz, 9. Aufl., 2010, Art. 10, Rdnr. 4; *Sodan*, in: Sodan, Grundgesetz, 2009, Art. 10, Rdnr. 4). Vgl. zum partiellen Funktionswandel des Art. 10 GG vom Abwehrrecht zur Schutzpflicht *Hadamek*, Art. 10 GG und die Privatisierung der Deutschen Bundespost, 2002.

285 Vgl. BVerfGE 106, 28, 36 ff.; 115, 166, 182.

286 BVerfGE 107, 299, 313.

287 Vgl. BVerfGE 100, 313, 358 ff.; *Gusy*, in: von Mangoldt/Klein/Starck, Grundgesetz, 6. Aufl., 2010, Art. 10, Rdnr. 39 ff.; *Löwer*, in: von Münch/Kunig, Grundgesetz, Bd. 1, 6. Aufl., 2012, Art. 10, Rdnr. 18 ff.; *Hufen*, Staatsrecht II, 2. Aufl., 2009, S. 295.

verfassungsgerichts[288] statt des im Gesetzeswortlaut genannten Ausdrucks „Fernmeldegeheimnis“ der Begriff „Telekommunikationsgeheimnis“ verwandt, der den heutigen Anforderungen gerechter wird. Durch die in rasendem Tempo voranschreitenden Technikentwicklungen und die Schaffung immenser Speicher- und Übertragungskapazitäten ist der Schutzbereich des Telekommunikationsgeheimnisses nicht immer leicht zu bestimmen. Aus diesem Grund handelt es sich beim Telekommunikationsgeheimnis um ein entwicklungsoffenes Grundrecht, welches sich den neuen technischen Entwicklungen anpasst[289]. Neben der Telekommunikation mittels Telefon, Telefax oder Mobilfunk ist allgemein anerkannt, dass auch die Kommunikationsdienste von Computernetzwerken, insbesondere das Internet, vom Schutzbereich des Telekommunikationsgeheimnisses umfasst werden[290]. Für die Telekommunikation über das Internet ist es für die Eröffnung des Schutzbereichs unerheblich, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt[291]. Geschützt wird durch Art. 10 Abs. 1 GG folglich die Telekommunikationsverkehrsbeziehung.

Neben den Inhalten der Kommunikation erfasst Art. 10 Abs. 1 GG auch die „Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs, zu denen insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist“[292].

Der Schutz endet auch nicht bereits nach dem ersten Zugriff, mit dem die staatliche Stelle von Telekommunikationsvorgängen und -inhalten Kenntnis nimmt. Vielmehr erstreckt sich die Schutzwirkung des Telekommunikationsgeheimnisses auf die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, sowie auf den anschließenden Gebrauch der erlangten Erkenntnisse[293]. Einen Eingriff in das Telekommunikationsgeheimnis stellt jede Kenntnisnahme, Aufzeichnung und Verwertung von geschützten Kommunikationsdaten sowie jede Auswertung ihres Inhalts oder sonstige Verwendung durch die öffentliche Gewalt dar[294].

288 BVerfGE 120, 274 bzw. BVerfG, 1 BvR 370/07 vom 27.02.2008, Absatz 1 ff., abrufbar unter *http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html*.

289 Vgl. BVerfGE 115, 166, 182; 106, 28, 36 ff.

290 BVerfGE 120, 274, 307 (Absatz 183); 115, 166, 182 ff.; *Hömig*, in: Hömig, Grundgesetz, 9. Aufl., 2010, Art. 10, Rdnr. 5 ff.; *Pieroth/Schlink*, Grundrechte, 26. Aufl., 2010, Rdnr. 837; vgl. zum Ganzen: *Sievers*, Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes, 2003, S. 103 ff.

291 BVerfGE 120, 274, 307; 115, 166, 182 ff.; 106, 28, 37 ff.

292 BVerfG, 1 BvR 1299/05 vom 24.01.2012, Absatz 112 m. w. N.

293 BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz 190; BVerfGE 100, 313, 359.

294 BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz 190; BVerfGE 110, 33, 52 ff.

Durch die Polizeistreifen im Internet werden insbesondere offen zugängliche Seiten des World Wide Web aufgerufen. Zudem werden Chats, Webforen und Newsgroups besucht bzw. in diesen wird persönlich durch Polizeibeamte kommuniziert.

Dieses heimliche Aufklären des Internet ist vergleichbar mit der dem Urteil des Bundesverfassungsgerichts zur Internet-Aufklärung und Online-Durchsuchung vorliegenden Sachlage[295]. In der damaligen Fassung des § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 des Verfassungsschutzgesetzes Nordrhein-Westfalen (NWVerfSchG) wurde die Verfassungsschutzbehörde zum „heimlichen Beobachten und sonstigen Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen", ermächtigt[296].

1. Das Urteil des Bundesverfassungsgerichts zur Internet-Aufklärung

Das Bundesverfassungsgericht hat in seinem Urteil vom 27.02.2008[297] eine Verletzung des durch Art. 10 Abs. 1 GG gewährleisteten Telekommunikationsgeheimnisses angenommen, da Maßnahmen gemäß § 5 Abs. 2 Nr. 11

295 BVerfGE 120, 274. Bei der Formulierung einer neuen Ausprägung des allgemeinen Persönlichkeitsrechtes als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme scheint es, als seien die Ausführungen des Bundesverfassungsgerichts zur Ermächtigung zum „heimlichen Beobachten und sonstigen Aufklären des Internet" in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 des Verfassungsschutzgesetzes Nordrhein-Westfalen kaum beachtet worden. So gehen beispielsweise auch Sachs/Krings treffend von einer größeren praktischen Bedeutung der heimlichen Aufklärungsmaßnahmen im Internet als der Online-Durchsuchungen aus, *Sachs/Krings*, JuS 2008, 481. Siehe vertiefend zur sog. Online-Durchsuchung *Gudermann*, Online-Durchsuchung im Lichte des Verfassungsrechts, 2010; *Soiné*, NVwZ 2012, 1585 ff.; *Stadler*, MMR 2012, 18 ff.; *Herrmann/Soiné*, NJW 2011, 2922 ff.; *Roggan*, Online-Durchsuchung, 2008; *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 99; *Leisner*, NJW 2008, 2902; *Volkmann*, DVBl 2008, 590 ff.; *Britz*, DÖV 2008, 411; *Kutscha*, NJW 2008, 1042; *Böckenförde*, JZ 2008, 925; *Bartsch*, CR 2008, 613; *Hornung*, CR 2008, 299; *Stögmüller*, CR 2008, 435; *Heckmann*, in: Kluth u. a., FS Rolf Stober, 2008, S. 615; *Bär*, MMR 2008, 325.

296 Die genaue Regelung des § 5 Abs. 2 Nr. 11 NWVerfSchG lautete: *„Die Verfassungsschutzbehörde darf nach Maßgabe des § 7 zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Mittel anwenden: (…)11. heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. Soweit solche Maßnahmen einen Eingriff in das Brief-, Post- und Fernmeldegeheimnis darstellen bzw. in Art und Schwere diesem gleichkommen, ist dieser nur unter den Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz zulässig;".*

297 BVerfGE 120, 274.

Satz 1 Alt. 1 NWVerfSchG in bestimmten Fällen einen verfassungsrechtlich ungerechtfertigten Eingriff in dieses Grundrecht darstellen könnten[298].

Zunächst ist darzustellen, zu welchen Maßnahmen die Verfassungsschutzbehörde überhaupt durch § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 NWVerfSchG ermächtigt werden sollte. Nach dem Wortlaut dieser Norm sollte das „heimliche Beobachten und sonstige Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen" erlaubt sein. Auf den ersten Blick fällt bereits auf, dass die „Heimlichkeit" der Maßnahmen im Vordergrund stehen sollte. Die Verfassungsschutzbehörde sollte folglich ohne Offenbarung ihrer Identität das Internet überwachen. Umfasst sein sollten von der Ermächtigungsgrundlage daher neben dem Aufruf von Webseiten im World Wide Web auch die Teilnahme an Chats unter Verschleierung der wahren oder Vortäuschung einer falschen Identität[299]. Außerdem beinhaltete das heimliche Aufklären des Internet nach Ansicht des Bundesverfassungsgerichts die Überwachung zugangsgesicherter Kommunikationsinhalte, also beispielsweise der Zugang zu einem E-Mail-Postfach oder zu einem geschlossenen Chat[300].

Vom Schutzbereich des Telekommunikationsgeheimnisses umfasst ist laut Bundesverfassungsgericht die „mit einem an das Internet angeschlossenen informationstechnischen System geführte laufende Fernkommunikation"[301]. Damit führt das Bundesverfassungsgericht seine Rechtsprechung fort, nach der staatliche Maßnahmen, durch welche die Umstände und Inhalte der laufenden Telekommunikation erhoben oder ausgewertet werden, an Art. 10 Abs. 1 GG zu messen sind, während sich dieser Grundrechtsschutz nicht mehr auf die nach Abschluss des Telekommunikationsvorganges bei einem Teilnehmer gespeicherten Umstände und Inhalte der Telekommunikation erstreckt[302]. Das Telekommunikationsgeheimnis schütze dabei allerdings lediglich das Vertrauen des Einzelnen darin, dass eine Fernkommunikation, an der er beteiligt sei, nicht von Dritten zur Kenntnis genommen werde. Dagegen sei das Vertrauen der Kommunikationspartner zueinander nicht Gegenstand des Grundrechtsschutzes[303]. Stehe im Vordergrund einer staatlichen Ermittlungsmaßnahme nicht der

298 Die Eingriffe in Art. 10 Abs. 1 GG waren verfassungsrechtlich nicht gerechtfertigt, da die Ermächtigungsnorm nicht dem Gebot der Normenklarheit und Normenbestimmtheit entsprach. Zudem stand die Ermächtigungsnorm nicht im Einklang mit dem Gebot der Verhältnismäßigkeit im engeren Sinn. Schließlich genügte § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 NWVerfSchG auch nicht dem Zitiergebot des Art. 19 Abs. 1 Satz 2 GG.

299 *Sachs/Krings*, JuS 2008, 481.

300 BVerfGE 120, 274, Absatz 292.

301 BVerfGE 120, 274, Absatz 290.

302 Vgl. bereits BVerfGE 115, 166, 183 ff., m. Anm. Jahn, JuS 2006, 491; dem Urteil des Bundesverfassungsgerichts zur Internet-Aufklärung und Online-Durchsuchung in diesem Punkt zustimmend *Eifert*, NVwZ 2008, 521.

303 So bereits BVerfGE 106, 28, 37.

unautorisierte Zugriff auf die Telekommunikation, sondern die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner, so liege darin kein Eingriff in Art. 10 Abs. 1 GG[304].

Als Konsequenz daraus sieht das Bundesverfassungsgericht dann keinen Eingriff in das Telekommunikationsgeheimnis vorliegen, wenn eine staatliche Stelle selbst mit einem Grundrechtsträger kommuniziert[305]. Voraussetzung für einen Eingriff ist somit auch bei Aufklärungsmaßnahmen im Internet die Überwachung einer Telekommunikationsbeziehung durch die Behörde von außen. Damit scheidet ein Eingriff in das Telekommunikationsgeheimnis nach Auffassung des Bundesverfassungsgerichts aus, wenn die Behörde allgemein zugängliche Daten erhebt, also zum Beispiel eine Webseite aufruft, die jedem Nutzer ungesichert zugänglich ist, oder offene Diskussionsforen besucht[306].

In seiner Entscheidung erweitert das Bundesverfassungsgericht den Schutz durch das Telekommunikationsgeheimnis auf bestimmte Fälle, in denen die staatliche Stelle selbst geschützte Inhalte im Internet aufruft[307]. Soweit eine staatliche Stelle Kenntnis von Inhalten einer über die Kommunikationsdienste des Internet geführten Fernkommunikation auf dem technisch dafür vorgesehenen Weg erhält, differenziert das Bundesverfassungsgericht bezüglich eines Eingriffs in Artikel 10 Abs. 1 GG danach, ob die staatliche Stelle hierzu durch einen Kommunikationsbeteiligten autorisiert war oder nicht[308]. Wenn nur einer von mehreren Kommunikationsbeteiligten den Zugriff freiwillig ermöglicht habe, liege kein Eingriff in das Telekommunikationsgeheimnis vor, da gerade das personengebundene Vertrauen der Kommunikationsbeteiligten zueinander nicht geschützt sei. Als Beispiel für einen Eingriff in Art. 10 Abs. 1 GG nennt das Bundesverfassungsgericht die Überwachung zugangsgesicherter Kommunikationsinhalte durch die Behörde, wobei die Behörde Zugangsschlüssel nutzte, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben habe[309]. Dies kann beispielsweise dadurch erfolgen, dass die Behörde mittels Keylogging[310] ein Passwort erhebt, um den Zugang zu einem geschlossenen Chat oder zu einem E-Mail-Postfach zu erreichen. Kein Eingriff in das Telekommunikationsgeheimnis liegt dementsprechend vor, wenn zum Beispiel ein Teilnehmer eines geschlossenen Chats der Behörde den passwort-

304 BVerfGE 120, 274, Absätze 290 ff.
305 BVerfGE 120, 274, Absatz 290.
306 BVerfGE 120, 274, Absatz 293.
307 Vgl. insgesamt dazu *Böckenförde*, JZ 2008, 925, 936 ff.
308 BVerfGE 120, 274, Absatz 291.
309 BVerfGE 120, 274, Absatz 292; dies Ergebnis entspricht auch der älteren Mailboxentscheidung des Bundesgerichtshofes (BGH NJW 1997, 1934), vgl. *Bär*, MMR 2008, 325, 327.
310 Beim Keylogger handelt es sich um Hard- oder Software, die die Tastatureingaben eines Benutzers am Rechner protokolliert, um beispielsweise Passwörter auszulesen.

geschützten Zugang freiwillig zur Verfügung stellt und die Behörde daraufhin den Zugang nutzt. Das Bundesverfassungsgericht stellt damit für einen Schutz durch das Telekommunikationsgeheimnis maßgeblich auf die Autorisierung ab[311].

2. Übertragung dieser Rechtsprechung auf verdachtsunabhängige Ermittlungen

Das Urteil des Bundesverfassungsgerichts zur Internet-Aufklärung betrifft in wesentlichen Teilen die für verdachtsunabhängige Ermittlungen der Polizei im Internet zu begutachtende Rechtslage. Um sich erschöpfend mit den in der Entscheidung des Bundesverfassungsgerichts aufgestellten Grundsätzen auseinanderzusetzen, muss zunächst der Schutzbereich des Art. 10 Abs. 1 GG bezogen auf die Kommunikation im Internet klar definiert werden.

2.1 Schutzbereich des Art. 10 Abs. 1 GG bezogen auf Kommunikation im Internet

Das Ziel des Telekommunikationsgeheimnisses ist es, die Vertraulichkeit individueller Kommunikation zu schützen. Daher sind Kommunikationsvorgänge, die sich an die Allgemeinheit oder einen unbestimmten Personenkreis richten, grundsätzlich nicht vom Schutzbereich umfasst[312]. Übertragen auf die Dienste des Internet bedeutet dies, dass zwischen Massen- und Individualkommunikation differenziert werden muss. Die Nutzung eines E-Mail-Dienstes wird man beispielsweise in den meisten Fällen der Individualkommunikation zurechnen können. Allerdings verschwimmen die Grenzen zur Massenkommunikation zum Beispiel bei der Verteilung von Informationen an einen beliebig großen Adressatenkreis über E-Mail-Verteil-Server[313].

Bei einer öffentlich zugänglichen Webseite im WWW, die an die Allgemeinheit gerichtet ist, wird man hingegen auf den ersten Blick eine Internet-Anwendung zur Massenkommunikation annehmen. Bei dieser Annahme wird aber oftmals leichtfertig übersehen, dass auch das WWW viele Schnittstellen zur Individualkommunikation bietet, etwa durch auf der Webseite integrierte Formulare, mit denen Informationen an den Betreiber der Webseite gesendet werden können. Die in großen Teilen der Literatur vertretene Ansicht, dass an die Allgemeinheit gerichtete Inhalte des Internet nicht dem Schutzbereich des Telekommunikationsgeheimnisses

311 *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 106 ff.

312 *Jarass*, in: Jarass/Pieroth, Grundgesetz, 12. Aufl., 2012, Art. 10, Rdnr. 6; *Hermes*, in: Dreier I, 2. Aufl., 2004, Art. 10, Rdnr. 38; *Pagenkopf*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 10, Rdnr. 14a.

313 So auch *Sievers*, Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes, 2003, S. 129 ff.

unterliegen[314], wird nicht der durch die technischen und gesellschaftlichen Entwicklungen zunehmenden Vermischung von Individual- und Massenkommunikation im Internet gerecht. Zudem erscheint es so, als würde diese Ansicht die technische Funktionsweise des Internet übersehen. Bei dem Aufruf einer Webseite im WWW wird auch dann, wenn die Webseite öffentlich zugänglich ist und sich an die Allgemeinheit richtet, eine individuelle Verbindung zwischen dem Absender und dem Empfänger der Daten aufgebaut[315]. Welcher genaue Inhalt zwischen dem Absender und dem Empfänger übermittelt wurde, kann nur dadurch ermittelt werden, indem die konkrete Telekommunikationsverbindung überwacht wird. Damit liegt auch in dieser Kommunikationsform letztendlich ein Akt individueller Kommunikation vor, so dass grundsätzlich das Internet als gesamtes Medium in den Schutzbereich des Telekommunikationsgeheimnisses fällt[316].

Diese gleichsam unendliche Ausdehnung des Schutzbereichs des Telekommunikationsgeheimnisses für Kommunikation im Internet erfährt allerdings Einschränkungen, da Art. 10 Abs. 1 GG die Vertraulichkeit individueller Kommunikation vor staatlicher Überwachung von außen schützt. Soweit eine Behörde selbst berechtigter Kommunikationsteilnehmer ist, wird dies nicht vom Schutzbereich umfasst[317]. Gegenstand der staatlichen Maßnahme ist dann nämlich nicht das Abgreifen von Telekommunikationsinhalten während der Übermittlung, sondern die Behörde lässt sich die Inhalte selbst übermitteln[318]. Danach sind beispielsweise die Aufrufe von öffentlich zugänglichen Webseiten auf dem technisch dafür vorgesehenen Weg durch Polizeibeamte nicht durch das Telekommunikationsgeheimnis geschützt[319]. Auch bei Chats ist Art. 10 Abs. 1 GG nicht betroffen, wenn ein Polizeibeamter mit einem anderen Chat-Teilnehmer kommuniziert, da durch das Telekommunikationsgeheimnis nicht das Vertrauen der Telekommunikationsteilnehmer zueinander geschützt wird. Auch wenn beispielsweise ein Polizeibeamter an einem Webforum teilnimmt, ohne aktiv zu kommunizieren, also lediglich die Inhalte der anderen Teilnehmer mitliest, ist der Schutzbereich nicht betroffen. In solch einem Fall sind sich die Kommunikationsbeteiligten dessen bewusst, dass keine vertrauliche Kommuni-

314 *Pagenkopf*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 10, Rdnr. 14a; *Jarass*, in: Jarass/Pieroth, Grundgesetz, 12. Aufl., 2012, Art. 10, Rdnr. 6 m. w. N.

315 Vgl. *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 104 ff.

316 So auch *Gausling*, Verdachtsunabhängige Speicherung von Verkehrsdaten auf Vorrat, 2010, S. 164; *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 104 ff.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 118; *Sievers*, Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes, 2003, S. 130; a. A. *Wagner*, Das Websurfen und der Datenschutz, 2006, S. 155.

317 So auch BVerfGE 120, 274, Absatz 290.

318 Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 512.

319 Vgl. auch *Perrey*, Gefahrenabwehr und Internet, 2002, S. 121 ff.

kation geführt wird, sondern zumindest eine unbeteiligte Person die Inhalte der Kommunikation zur Kenntnis nehmen kann.

Das Bundesverfassungsgericht hat sogar für die Situation, dass ein Gesprächsteilnehmer einen Dritten ein Telefongespräch über die Lautsprecherfunktion ohne Wissen des anderen Gesprächsteilnehmers mithören lässt, den Schutzbereich des Art. 10 Abs. 1 GG verneint[320]. Dies gilt folglich erst recht für den Fall, dass alle Kommunikationsteilnehmer, wie beispielsweise bei einem Chat, sich über die unverdeckte Kommunikation bewusst sind.

2.2 Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG bezogen auf Kommunikation im Internet

Ein Eingriff in den Schutzbereich kann ausnahmsweise vorliegen, wenn die vom Bundesverfassungsgericht aufgestellte Fallgruppe der unautorisierten Teilnahme an der Internetkommunikation einschlägig ist[321]. Diese liegt dann vor, wenn der Staat zugangsgesicherte Kommunikationsinhalte überwacht, indem er Zugangsschlüssel nutzt, die er ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat[322]. Damit setzt das Bundesverfassungsgericht perspektivisch bei der ermittelnden staatlichen Stelle an und nicht bei den Eigenschaften des jeweils beobachteten Kommunikationsvorgangs[323]. Ein Eingriff in Art. 10 Abs. 1 GG liegt daher vor, wenn die Behörde ein Passwort durch Keylogging erhebt und damit Zugang zu geschützten Kommunikationsinhalten auf dem dafür technisch vorgesehenen Weg erlangt[324]. Soweit die staatliche Stelle die Daten nicht auf dem dafür technisch vorgesehenen Weg erhebt, wie etwa bei der „Quellen-Telekommunikationsüberwachung“ von laufenden Telekommunikationsvorgängen, liegt gleichfalls ein Eingriff vor[325].

Zu untersuchen ist, ob im Rahmen der verdachtsunabhängigen Ermittlungen der Polizei im Internet die Fallgruppe der unautorisierten Teilnahme an der Internetkommunikation einschlägig sein kann. Die Polizisten nehmen aktiv an Kommunikationsdiensten teil, ohne ihre Behördenzugehörigkeit offenzulegen. Diese Maßnahme könnte auf den ersten Blick einen Eingriff in das Telekommunikationsgeheimnis darstellen. Allerdings ist für diesen Fall wieder die Schutzrichtung des Art. 10 Abs. 1 GG zu beachten. Durch das Telekommunikationsgeheimnis wird eine Telekommunikationsbeziehung durch die staatliche Überwachung von außen geschützt, nicht aber

320 BVerfGE 106, 28, 37 ff.

321 Vgl. BVerfGE 120, 274, Absätze 291 ff.

322 Vgl. dazu auch *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 106 ff.

323 *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 106.

324 BVerfGE 120, 274, Absatz 292.

325 Vgl. BVerfGE 120, 274, Absätze 183 ff.

die Kommunikation zwischen einem Grundrechtsträger und der staatlichen Stelle[326]. Eine staatliche Identitätstäuschung führt daher nicht zu einem Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle verdeckt mit anderen Beteiligten kommuniziert[327]. Dass die Behörde sich beispielsweise in Webforen aktiv beteiligt, obwohl sie verdeckt unter Verschleierung ihrer Behördeneigenschaft agiert, wird nicht durch das Telekommunikationsgeheimnis geschützt. Ein Eingriff in Art. 10 Abs. 1 GG läge erst dann vor, wenn sie gegen oder ohne den Willen eines Zugangsberechtigten mit seinem Zugangsschlüssel einen Internetdienst nutzt, um von den Inhalten der über den Kommunikationsdienst des Internet geführten Telekommunikation Kenntnis zu erlangen. Für die verdachtsunabhängigen Ermittlungen der Polizei im Internet ist die Fallgruppe der unautorisierten Teilnahme an der Internetkommunikation nicht einschlägig, da die Polizeibeamten nach dem derzeitigen Kenntnisstand eine solche Vorgehensweise nicht durchführen[328].

Da ein Eingriff in den Schutzbereich des Telekommunikationsgeheimnisses nur dann vorliegen kann, wenn unautorisiert eine Telekommunikationsbeziehung überwacht wird, scheidet ein Eingriff im Rahmen der verdachtsunabhängigen Ermittlungen der Polizei im Internet aus. Bedenklich ist in diesem Zusammenhang allerdings, dass das Bundesverfassungsgericht in seinem Urteil zur Internet-Aufklärung dann keinen Eingriff in Art. 10 Abs. 1 GG sieht, wenn die staatliche Stelle von nur einem von mehreren Kommunikationsbeteiligten dazu berechtigt wurde. Im Gegensatz zur Rechtsprechung, die das Mithören von Telefongesprächen durch Privatpersonen betraf[329], handelt hier die staatliche Stelle in gewisser Weise als Mithörer. Damit könnte bereits die Grenze zum „mittelbaren" staatlichen Eingriff überschritten werden, wenn der Private von der staatlichen Stelle zum Telefonat und Mithörenlassen veranlasst worden ist[330].

Auf den Bereich der Kommunikation im Internet übertragen könnte daher ein „mittelbarer" staatlicher Eingriff vorliegen, wenn die Behörde einen zugangsgesicherten, geschlossenen Chat über das Passwort und die damit einhergehende Internet-Identität eines Privaten betritt und die dortige Kommunikation überwacht. Eine Einschränkung macht das Bundesverfassungs-

326 Vgl. BVerfGE 120, 274, Absatz 290.

327 Vgl. *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 107.

328 Vgl. die Antwort der Bundesregierung vom 14.07.2011 auf eine Kleine Anfrage, BT-Drs 17/6587, S. 3 ff., sowie die Informationen zur Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) unter *www.bka.de/*.

329 BVerfGE 106, 28; vgl. insgesamt zur Entwicklung der Rechtsprechung zur Hörfallenproblematik die umfassende Darstellung von *Guder*, Die repressive Hörfalle im Lichte der Europäischen Menschenrechtskonvention, 2007, S. 22 ff.

330 Vgl. *Sachs/Krings*, JuS 2008, 481, 482.

gericht aber insoweit, dass nur dann kein Eingriff in das Telekommunikationsgeheimnis vorliegt, wenn der Private seinen Zugang freiwillig zur Verfügung gestellt hat[331]. In welchen Fällen man in der Praxis noch eine Freiwilligkeit annehmen kann, dürfte jedoch vielfach schwierig abzuschätzen sein. Gegen den Privaten selbst, der seinen Zugang zur Verfügung stellen soll, wird wahrscheinlich häufig ermittelt oder die Behörde kann in sonstiger Weise Druck auf den Privaten ausüben. In diesen Fällen wird sicherlich keine Freiwilligkeit im engeren Sinne mehr vorliegen.

3. Ergebnis

Während die das Telekommunikationsgeheimnis verletzenden gezielten Telekommunikationsüberwachungen von Personen durch die Polizei inzwischen zum „Massengeschäft" avanciert sind[332], wird Art. 10 Abs. 1 GG durch die verdachtsunabhängigen Ermittlungen der Polizei im Internet nicht verletzt. Die Behörde verhält sich im Rahmen dieser Ermittlungen ähnlich einer Privatperson und überwacht die Kommunikation nicht von außen, sondern agiert in den meisten Fällen als Kommunikationsteilnehmer. Zudem wird durch das Telekommunikationsgeheimnis die Vertraulichkeit der Nutzung des zur Nachrichtenübermittlung eingesetzten Mediums geschützt, nicht aber das Vertrauen der Kommunikationsbeteiligten zueinander. Die Fallgruppe der unautorisierten Teilnahme an der Kommunikation im Internet, die einen Eingriff in Art. 10 Abs. 1 GG darstellt, wird durch die Polizeistreifen im Internet nach dem derzeitigen Informationsstand ebenfalls nicht verwirklicht[333].

II. Die Unverletzlichkeit der Wohnung (Art. 13 GG)

Art. 13 Abs. 1 GG garantiert die Unverletzlichkeit der Wohnung. Das Grundrecht dient damit dem Einzelnen im Hinblick auf seine Menschenwürde und im Interesse der freien Entfaltung der Persönlichkeit dem Schutz der räumlichen Privatsphäre und dem elementaren menschlichen Bedürfnis,

331 BVerfGE 120, 274, Absatz 293.

332 So von Praktikern eingeräumt, siehe *Kutscha*, LKV 2008, 481, 485; *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 110a, 100b StPO und anderer verdeckter Ermittlungsverfahren, 2003, S. 34. Wie *Petri*, in: Lisken/Denninger, HbPolR, 5. Aufl., 2012, Kap. G, Rdnr. 306, mitteilt, hat sich die Anzahl der Überwachungsanordnungen im Zeitraum 1995 bis 2005 mehr als verzehnfacht. Vgl. vertiefend zur Überwachung der Telekommunikation auch *Krüpe-Gescher*, Die Überwachung der Telekommunikation nach den §§ 100a, 100b StPO in der Rechtspraxis, 2005; *Dorsch*, Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, 2005.

333 Vgl. die Antwort der Bundesregierung vom 14.07.2011 auf eine Kleine Anfrage, BT-Drs 17/6587, S. 3 ff., sowie die Informationen zur Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) unter *www.bka.de/*.

einen von der Öffentlichkeit abgeschirmten, individuell geprägten Lebensraum zu haben, in welchem der Einzelne das Recht hat, „in Ruhe gelassen zu werden“[334].

Als Wohnung sind zunächst alle Räume einzustufen, die der allgemeinen Zugänglichkeit durch eine räumliche Abschottung entzogen und zur Stätte privaten Lebens und Wirkens gemacht sind[335]. Ob dabei auch Betriebs- und Geschäftsräume in den Schutzbereich des Art. 13 Abs. 1 GG fallen, und wenn ja, welche genauen Betriebs- und Geschäftsräume, ist umstritten[336]. Insoweit stellt sich die Frage, ob das Internet selbst als Wohnung im Sinne des Art. 13 Abs. 1 GG qualifiziert werden kann[337]. Das Internet wird häufig als „virtueller Raum“ bezeichnet, weshalb ein Eingriff in Art. 13 Abs. 1 GG dann vorliegen könnte, wenn Daten, die auf eine eigene Persönlichkeitssphäre schließen lassen, aus dem Internet erhoben werden. Solch eine weite Ausdehnung des Wohnungsbegriffs ist jedoch nicht gerechtfertigt, da zwar im übertragenen Sinne das Internet ein „virtueller Raum“ sein mag, aber mangels physischer Beschaffenheit kein mit einer Wohnung im Sinne des Art. 13 Abs. 1 GG vergleichbarer Raum vorliegt. Das Internet besteht vereinfacht dargestellt aus Datenleitungen und sonstigen technischen Geräten, wie beispielsweise Datenspeichermedien. Das Internet kann damit nicht im physischen Sinne betreten oder bewohnt werden. Somit kann das Internet selbst nicht in den Schutzbereich des Art. 13 Abs. 1 GG fallen. Die Datenspeichermedien und Datenleitungen befinden sich allerdings vielfach in privaten Wohnungen oder Betriebs- oder Geschäftsräumen, welche wiederum durch dieses Grundrecht geschützt werden.

Als Eingriff in Art. 13 Abs. 1 GG ist zunächst das Eindringen in den Wohnungsbereich oder das Verweilen darin gegen den Willen des Grundrechtsträgers zu sehen[338]. Aber auch Maßnahmen, durch die sich staatliche Stellen mit besonderen Hilfsmitteln einen Einblick in Vorgänge innerhalb der Wohnung verschaffen, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind, sind als Eingriffe in Art. 13 Abs. 1 GG

334 BVerfGE 32, 54, 75; 89, 1, 12; 51, 97, 107; 103, 142, 150 ff.; 115, 166, 196.

335 BGHSt 44, 138, 140; *Jarass*, in: Jarass/Pieroth, Grundgesetz, 12. Aufl., 2012, Art. 13, Rdnr. 4; *Papier*, in: Maunz/Dürig, Grundgesetz, Bd. 2, Art. 13, Rdnr. 10.

336 Das BVerfG lässt mit der h. M. auch Betriebs- und Geschäftsräume in den Schutzbereich des Art. 13 Abs. 1 GG fallen, BVerfGE 32, 54, 69 ff.; 44, 353, 371; 76, 83, 88; 96, 44, 51; 120, 274, Absatz 192; *Hofe*, ZRP 1995, 169, 170 ff.; *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, Grundgesetz, 12. Aufl., 2011, Art. 13, Rdnr. 7; vorsichtiger BVerwGE 78, 251, 255. A. A. *Lübbe-Wolf*, DVBl 1993, 762, 764; *Meyer*, Versuch über Demokratie in Deutschland, 2003, 6 ff.; wohl auch *Hermes*, JZ 2005, 461, 463 ff.; *Hermes*, in: Dreier I, Grundgesetz, 2. Aufl., 2004, Art. 13, Rdnr. 25 ff.

337 Dazu ausführlich *Perrey*, Gefahrenabwehr und Internet, 2002, S. 126 ff.

338 BVerfGE 76, 83, 90; 89, 1, 12.

anzusehen[339]. Für den heimlichen technischen Zugriff auf ein informationstechnisches System (also z. B. auf einen an das Internet angeschlossenen PC) hat das Bundesverfassungsgericht in seinem Urteil zur Internet-Aufklärung und Online-Durchsuchung eine differenzierte Sichtweise vertreten[340]. Danach bleibt es dabei, dass die von außen erfolgende elektronische Aufzeichnung der Abstrahlungen der benutzten Tastaturen als Eindringen in die besonders geschützte räumliche Umgebung unter Art. 13 Abs. 1 GG fällt[341]. Ebenso zählen die Fälle zum Anwendungsbereich des Art. 13 Abs. 1 GG, in denen beispielsweise Polizeibeamte in eine Wohnung eindringen und physisch ein Programm zum Ausspähen der Daten, einen sogenannten „Trojaner", auf dem PC installieren. Auch wenn ein PC, der sich in einer Wohnung befindet, infiltriert wird, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Geräte wie ein Mikrofon oder eine Kamera dazu genutzt werden, ist dies an Art. 13 Abs. 1 GG zu messen[342].

Nach Ansicht des Bundesverfassungsgerichts vermittelt Art. 13 Abs. 1 GG dem Einzelnen allerdings keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltrierung seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet[343].

Das Bundesverfassungsgericht führt dazu aus:

„Denn der Eingriff kann unabhängig vom Standort erfolgen, so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren. Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt. Der Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein. Dies gilt insbesondere für mobile informations-

339 BVerfGE 120, 274, Absatz 192. Damit sind beispielsweise Observationen durch in die Wohnung verbrachte Aufzeichnungsanlagen (sog. kleiner Lauschangriff) oder durch akustische bzw. visuelle Überwachung von außen (sog. großer Lauschangriff) an Art. 13 GG zu messen. Vertiefend dazu *Kress*, Der „Große Lauschangriff" als Mittel internationaler Verbrechensbekämpfung, 2009; *Meyer-Wieck*, Der Große Lauschangriff, 2005; Mozek, Der „große Lauschangriff", 2001; *Müller*, Der sogenannte „Große Lauschangriff", 2000; *Roggan*, Große Lauschangriffe, in: Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., 2006, S. 106 ff.

340 BVerfGE 120, 274, Absätze 192 ff.

341 Vgl. BVerfGE 120, 274, Absatz 192; *Hirsch*, NJOZ 2008, 1907, 1912.

342 BVerfGE 120, 274, Absatz 193.

343 BVerfGE 120, 274, Absatz 194; ebenso *Beulke/Meininghaus*, StV 2007, 63, 64; *Gercke*, CR 2007, 245, 250; *Schlegel*, GA 2007, 648, 654 ff.; a. A. *Rux*, JZ 2007, 285, 292 ff.; *Sachs/Krings*, JuS 2008, 481, 483; *Schaar/Landwehr*, K&R 2007, 202, 204.

technische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone.

Art. 13 I GG schützt zudem nicht gegen die durch die Infiltrierung des Systems ermöglichte Erhebung von Daten, die sich im Arbeitsspeicher oder auf den Speichermedien eines informationstechnischen Systems befinden, das in einer Wohnung steht (vgl. zum gleichläufigen Verhältnis von Wohnungsdurchsuchung und Beschlagnahme BVerfGE 113, 29 [45] = NJW 2005, 1917).“[344]

Damit sieht das Bundesverfassungsgericht für die Fälle, in denen die staatliche Stelle ohne das physische Betreten der Wohnung mittels Internet einen Trojaner auf dem PC zur Überwachung bzw. Durchsuchung installiert hat, bezüglich Art. 13 Abs. 1 GG eine Schutzlücke. Die Begründung des Bundesverfassungsgerichts kann aber nicht vollends überzeugen, da insbesondere unklar bleibt, weshalb das Bundesverfassungsgericht diese Maßnahmen nicht zumindest auch an Art. 13 Abs. 1 GG messen will, wenn sich der PC in einer Wohnung befindet[345].

Für die verdachtsunabhängigen Ermittlungen der Polizei im Internet bedeutet dies, dass kein Eingriff in Art. 13 Abs. 1 GG vorliegen kann. Selbst wenn die Polizeibehörden im Rahmen der Polizeistreifen im Internet Online-Durchsuchungen durchführen würden, wofür es allerdings nach derzeitigem Kenntnisstand in keiner Weise Anzeichen gibt[346], läge nach Ansicht des Bundesverfassungsgerichts kein Eingriff in Art. 13 Abs. 1 GG vor. Soweit bereits die Online-Durchsuchungen keinen Eingriff in Art. 13 Abs. 1 GG darstellen, muss dies erst recht für die weitaus milderen Maßnahmen der verdachtsunabhängigen Ermittlungen, wie z. B. das Aufrufen von allgemein zugänglichen Webseiten im Internet sowie die Kommunikation über das Internet durch Polizeibeamte gelten[347]. Auch die verdachtsunabhängigen Ermittlungen können unabhängig vom Standort erfolgen, und die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre wird damit – bei Übertragung der in der Entscheidung des Bundesverfas-

344 BVerfGE 120, 274, Absatz 194 ff.

345 Dazu vertiefend *Sachs/Krings*, JuS 2008, 481, 483. Weitergehend wird sogar angenommen, bei Zweifeln über den Standort eines informationstechnischen Systems zum Zeitpunkt der Online-Durchsuchung gleichfalls Art. 13 Abs. 1 GG heranzuziehen, vgl. *Hornung*, DuD 2007, 575, 578.

346 Vgl. die Antwort der Bundesregierung vom 14.07.2011 auf eine Kleine Anfrage, BT-Drs 17/6587, S. 3 ff., sowie die Informationen zur Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) unter *www.bka.de/*.

347 Ein Eingriff in die Unverletzlichkeit der Wohnung müsste dann an den für den Einsatz technischer Mittel zur Gefahrenabwehr geltenden strengen Anforderungen des Art. 13 Abs. 4 GG gemessen werden. Die Voraussetzungen dafür sind in mehrfacher Hinsicht enger als diejenigen für Eingriffe und Beschränkungen im Sinne des Art. 13 Abs. 7 GG, dem Art. 13 Abs. 4 GG als Spezialregelung vorgeht (vgl. BT-Drs 13/8650, S. 5).

sungsgerichts zur Internet-Aufklärung und Online-Durchsuchungen aufgestellten Grundsätze – nicht berührt. Zwar befinden sich die Datenspeichermedien oftmals in den Geschäftsräumen von Providern, die zumindest nach der h. M. dem grundrechtlichen Schutz unterliegen, jedoch ist gerade der Zugriff auf die Datenspeichermedien gewollt. Diese Daten werden bewusst der Öffentlichkeit zur Verfügung gestellt. Damit liegt eine Einwilligung des Providers vor.

Insgesamt scheidet daher eine Verletzung des Art. 13 Abs. 1 GG aus.

III. Die Meinungs- und Informationsfreiheit (Art. 5 Abs. 1 Satz 1 GG)

Durch die Meinungsfreiheit (Art. 5 Abs. 1 Satz 1 Alt. 1 GG) wird jedermann das Recht zugestanden, die eigene Meinung in Wort, Schrift und Bild unter Wahl des Ortes und der Zeit frei zu äußern und zu verbreiten[348]. Die Wahl des Mediums zur Meinungskundgabe ist hierbei unbeachtlich, weshalb auch die Neuen Medien wie das Internet erfasst sind[349]. Die elektronische Übermittlung von Textinformationen über das Internet ist beispielsweise als Ausdrucksmittel der Schrift zu qualifizieren[350].

Zu den Eingriffen in die Meinungsfreiheit gehören Verbote, Meinungen zu äußern oder zu verbreiten, sowie faktische oder bloß mittelbare Beeinträchtigungen[351]. Damit sind staatliche Maßnahmen, die nicht final die Meinungsfreiheit einschränken sollen, faktisch aber die gleiche Wirkung haben, ebenfalls als Eingriffe zu werten[352].

Durch die verdachtsunabhängigen Ermittlungen der Polizei im Internet werden die Nutzer zwar in gewisser Weise überwacht, jedoch wird dadurch die Meinungsfreiheit nicht weiter eingeschränkt.

Eine teilweise vertretene Ansicht sieht in einer „von hinreichenden Anzeichen konkreter Rechtsgutgefährdungen unabhängige staatliche Inhaltsprüfung von Kommunikation“ eine verbotene Zensur im Sinne des

348 BVerfGE 93, 266, 289.

349 *Billmeier*, Die Düsseldorfer Sperrungsverfügung, 2006, S. 144; *Determann*, Kommunikationsfreiheit im Internet, 1999, S. 393; *Schulze-Fielitz*, in: Dreier, Grundgesetz, Bd. 1, 2. Aufl., 2004, Art. 5 Abs. 1 und 2, Rdnr. 67; *Kraft/Meister*, MMR 2003, 366, 369; vgl. insgesamt zum verfassungsrechtlichen Schutz der digitalen Massenkommunikation *Koreng*, Zensur im Internet, 2010.

350 Vgl. bereits *Bullinger/Mestmäcker*, Multimediadienste, 1996, S. 65 ff.; Mecklenburg, ZUM 1997, 525 ff. Hierbei sind aber auch Ausdrucksmittel, die nicht unter die Begriffe „Wort, Schrift und Bild“ zu subsumieren sind, grundrechtlich geschützt, siehe *Degenhart*, in: BK, Grundgesetz, Bd. 2, Art. 5 Abs. 1 und 2, Rdnr. 148.

351 *Sodan*, in: Sodan, Grundgesetz, 2009, Art. 5, Rdnr. 11.

352 Vgl. *Schmidt-Jortzig*, Meinungs- und Informationsfreiheit, in: HStR VII, 3. Aufl., 2009, § 147, Rdnr. 30; *Schulze-Fielitz*, in: Dreier, Grundgesetz, Bd. 1, 2. Aufl., 2004, Art. 5 Abs. 1 und 2, Rdnr. 128 ff.

Art. 5 Abs. 1 Satz 3 GG[353]. Danach sei eine lähmende Kommunikationsbehinderung auch dann zu befürchten, wenn zwar auf ein formelles Genehmigungsverfahren vor Verbreitung eines Kommunikationsinhalts verzichtet werde, jedoch staatliche Stellen zur systematischen Überwachung der Kommunikation eingesetzt und ihnen Aufgaben anlassunabhängiger Gefahrenerforschung im Kommunikationsbereich übertragen würden[354]. Diese Ansicht verkennt allerdings, dass das Zensurverbot des Art. 5 Abs. 1 Satz 3 GG die Vorzensur, also einschränkende Maßnahmen vor der Herstellung oder Verbreitung eines Geisteswerkes, wie beispielsweise eine vorhergehende Prüfung eines Inhalts durch eine Behörde, verbieten will[355]. Außerdem handelt es sich bei Art. 5 Abs. 1 Satz 3 GG nicht um ein eigenständiges Grundrecht mit eigenem Schutzbereich, sondern um eine „Schranken-Schranke" für die Meinungs- und Medienfreiheit[356]. Da die Polizeistreifen im Internet die Meinungsfreiheit gerade nicht einschränken, kann also kein Verstoß gegen das Zensurverbot vorliegen[357].

Ein Eingriff in die Meinungsfreiheit läge aber durch an den Äußernden oder einen Provider gerichtete Sperrungs- oder Löschungsanordnungen vor[358]. Solche Anordnungen werden allerdings nicht im Rahmen der verdachtsunabhängigen Ermittlungen getroffen, sondern beruhen gegebenenfalls auf den gesammelten Erkenntnissen dieser Ermittlungsmaßnahmen[359].

Durch die Informationsfreiheit gemäß Art. 5 Abs. 1 Satz 1 Alt. 2 GG wird das Recht geschützt, sich selbst aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Ob dabei die Informationen aus dem In- oder Ausland kommen, ist unerheblich[360]. Eine Quelle ist dann allgemein zugänglich, wenn sie technisch geeignet und bestimmt ist, der Allgemeinheit, d. h.

353 So *Hoffmann-Riem*, in: AK-GG, 3. Aufl., 2001, Art. 5 Abs. 1, 2, Rdnr. 92 ff.; *Rohde*, Die Nachzensur in Art. 5 Abs. 1 Satz 3 GG, 1997, Satz 174.

354 Vgl. BVerfGE 33, 89 ff.: Minderheitenvotum; *Hoffmann-Riem*, in: AK-GG, 3. Aufl., 2001, Art. 5 Abs. 1, 2, Rdnr. 92.

355 Vgl. statt vieler *Schemmer*, in: Epping/Hillgruber, Grundgesetz, 2009, Art. 5, Rdnr. 114; *Bethge*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 5, Rdnr. 131.

356 Vgl. *Herzog*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 5 Abs. 1, 2, Rdnr. 99; *Schemmer*, in: Epping/Hillgruber, Grundgesetz, 2009, Art. 5, Rdnr. 114.

357 Vgl. *Germann*, Strafverfolgung im Internet, 2000, S. 513.

358 Durch eine staatliche Sperrungs- oder Löschungsanordnung können auch noch weitere Grundrechte, wie beispielsweise Art. 14 Abs. 1 GG oder die Pressefreiheit, verletzt werden. Vertiefend dazu *Sieber/Nolde*, Sperrverfügungen im Internet, 2008; *Frey/Rudolph/Oster*, MMR-Beilage 2012, S. 1 ff.; *Billmeier*, Die Düsseldorfer Sperrungsverfügung, 2006, S. 143 ff.; *Ennuschat/Klestil*, ZfWG 2009, 389 ff.; *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, 2001; *Fiedler*, Meinungsfreiheit in einer vernetzten Welt, 2002, S. 62 ff.; *Stadler*, MMR 2002, 343 ff.

359 Vgl. insgesamt dazu auch das „Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen", welches jedoch mit Wirkung zum 29.12.2011 aufgehoben wurde.

360 BVerfGE 27, 71, 84; *Engel*, AfP 1996, 220, 224.

einem individuell nicht bestimmbaren Personenkreis, Informationen zu beschaffen[361]. Daher sind auch die Dienste des Internet, die für die Allgemeinheit bestimmt sind, zu den durch die Informationsfreiheit geschützten Quellen zu zählen[362]. So fällt beispielsweise eine allgemein zugängliche Webseite wie www.spiegel.de oder www.focus.de in den Schutzbereich dieses Grundrechts. Auch Newsgroups, Chats oder sonstige Informationsdienste können grundsätzlich von jedem aufgerufen werden und sind daher allgemein zugängliche Informationsquellen. Hingegen sind Dienste zur Individualkommunikation, wie in den meisten Fällen E-Mail-Dienste oder Telefonate über das Internet, nicht durch die Informationsfreiheit geschützt. Diese Dienste sind nicht für die Allgemeinheit bestimmt und Teil des Persönlichkeitsrechts der Nutzer, weshalb kein Recht besteht, sich diese Informationen zu beschaffen[363].

Die Unterrichtung aus allgemein zugänglichen Informationsquellen muss ungehindert erfolgen können. Das Informationsrecht ist dann ungehindert, wenn es frei von rechtlicher oder tatsächlicher Abschirmung, Behinderung, Lenkung oder auch nur Verzögerung wahrgenommen werden kann[364]. Bei der Überwachung des Internet handeln die Polizisten im Grunde wie „normale“ Nutzer. Dadurch werden keine Nutzer behindert, bestimmte Webseiten aufzurufen oder sonstige Dienste des Internet zu nutzen. Durch den Einsatz von automatisierten Suchprogrammen ist ebenfalls nicht davon auszugehen, dass es auf Grund der laufenden Suchprogramme bei der Nutzung der verschiedenen Dienste zu Verzögerungen oder gar Behinderungen kommt.

Die Abwehrfunktion der Informationsfreiheit ist aber weiter zu fassen. Eine Behinderung des Informationsrechts liegt auch in der Beobachtung und Registrierung des Informationsverhaltens einzelner Menschen[365]. So wird beispielsweise der Schutzbereich der Informationsfreiheit bei Anwesenheit eines Polizisten bei einer öffentlichen Informationsveranstaltung oder bei der Speicherung des Nutzungsverhaltens bei elektronischen Medien berührt[366]. Dieser von einer Beobachtung, Speicherung oder Regist-

361 Vgl. BVerfGE 27, 71, 81 ff.; 90, 27, 32; *Kannengießer*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, Grundgesetz, 12. Aufl., 2011, Art. 5, Rdnr. 9.

362 *Degenhart*, in: BK, Grundgesetz, Bd. 2, Art. 5 Abs. 1 und 2, Rdnr. 289 ff.; *Herzog*, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, 2000, S. 189.

363 *Perrey*, Gefahrenabwehr und Internet, 2002, S. 130.

364 Vgl. BVerfGE 27, 88, 98 ff.

365 *Herzog*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 5 Abs. 1, 2, Rdnr. 99; *Starck*, in: Mangoldt/Klein/Starck, 6. Aufl., 2010, Art. 5 Abs. 1, 2, Rdnr. 56. *Wendt* warnt dabei passend mit lediglich einem Wort: „Einschüchterungseffekt!“, in: von Münch/Kunig, Grundgesetz, Bd. 1, 6. Aufl., 2012, Art. 5, Rdnr. 27.

366 *Degenhart*, in: BK, Grundgesetz, Bd. 2, Art. 5 Abs. 1 und 2, Rdnr. 309. Für die Vorratsdatenspeicherung hat das Bundesverfassungsgericht Art. 5 GG aber nicht weiter problematisiert, vgl. BVerfG, 1 BvR 256/08 vom 02.03.2010. Für den staatlichen Einsatz von Cookies oder

rierung ausgehende Einschüchterungseffekt kann die Informationsfreiheit beeinträchtigen[367].

Bei den verdachtsunabhängigen Ermittlungen überwachen die Polizisten zwar auch bestimmte Personen, jedoch wird nur punktuell eine Person beispielsweise in einem Chat beobachtet. Es findet kein unberechtigter Zugriff auf den Rechner der „Zielperson" statt und es werden auch nicht die Zugriffe auf andere Webseiten, die von diesem Rechner ausgehen, überwacht. Anders als bei der Teilnahme eines (uniformierten) Polizisten an einer Informationsveranstaltung findet die Internetüberwachung außerdem heimlich statt, so dass die Betroffenen von der virtuellen Anwesenheit der Polizisten nichts wahrnehmen. Auch von einem Einschüchterungseffekt bei der Ausübung der Informationsfreiheit ist durch die Polizeistreifen im Internet nicht auszugehen, da keine umfassende Überwachung durch die Polizeistreifen erfolgt, sondern lediglich stichprobenartig in geringem Maße beobachtet wird. Zudem ist, bedingt durch die technische und insbesondere personelle Ausstattung der Behörden, die Überwachung des Internet mit seinem geradezu unendlichen Ausmaß allenfalls als ein Tröpfchen auf den heißen Stein anzusehen. Eine auch nur faktische Behinderung bei der Informationsbeschaffung liegt damit nicht vor.

IV. Die Versammlungsfreiheit (Art. 8 Abs. 1 GG)

Das durch Art. 8 Abs. 1 GG garantierte Grundrecht der Versammlungsfreiheit ergänzt das Grundrecht der Meinungsfreiheit, indem es die kollektive Meinungsbildung und Meinungskundgabe gewährleistet. Bedingt durch die technischen und gesellschaftlichen Entwicklungen verlagert sich das heutige Kommunikationsverhalten immer mehr von der realen in die virtuelle Welt. Statt auf der Straße werden mittlerweile Meinungen oftmals eher im Internet verbreitet. Da diese Meinungsbildungen im Internet regelmäßig nicht nur aus der Feder eines Einzelnen stammen bzw. eine gemeinsam gebildete Meinung zusammen nach außen kommuniziert wird, könnte damit auch ein Wandel im Verständnis der Versammlungsfreiheit einhergehen[368]. Es stellt sich daher die Frage, ob eine „virtuelle Versammlung" durch die Versammlungsfreiheit besonders geschützt wird.

Eine „virtuelle Versammlung" kann beispielsweise in einem Chat bestehen, in dem sich die Teilnehmer zur Kundgabe einer bestimmten politischen Meinung zusammenfinden. Nach der Rechtsprechung des Bundesverfassungsgerichts setzt der Schutz durch Art. 8 Abs. 1 GG allerdings eine

Web Bugs vertritt *Wagner* die Ansicht, dass es sich aufgrund der damit einhergehenden Datenverarbeitungen um einen Eingriff in das Recht auf Informationsfreiheit aus Art. 5 Abs. 1 GG handele, *Wagner*, Das Websurfen und der Datenschutz, 2006, S. 157.

367 Vgl. *Schulze-Fielitz*, in: Dreier, Grundgesetz, Bd. 1, 2. Aufl., 2004, Art. 5, Rdnr. 130.

368 Vgl. *Kraft/Meister*, MMR 2003, 366, 367 ff.

örtliche Zusammenkunft mehrerer Personen voraus[369]. Die damit geforderte physische Präsenz liegt zweifelsohne in der virtuellen Welt nicht vor. Eine „virtuelle Versammlung" fällt damit grundsätzlich nicht in den Schutzbereich des Art. 8 Abs. 1 GG[370].

Allerdings könnte der Schutzbereich der Versammlungsfreiheit auch auf „virtuelle Versammlungen" auszudehnen sein, da zum Zeitpunkt des Grundgesetzerlasses diese zunehmende Verschiebung der Kommunikation und Meinungskundgabe von der realen in die virtuelle Welt nicht absehbar war. Der Wandel der Normsituation kann damit Anlass für eine Änderung beziehungsweise Erweiterung der Auslegung eines Gesetzes sein[371]. Wenn sich also die tatsächlichen Verhältnisse oder Gepflogenheiten, die der historische Gesetzgeber vor Augen hatte und auf die hin er seine Regelung entworfen hat, in solcher Weise geändert haben, dass die verabschiedete Norm auf die geänderten Verhältnisse nicht mehr „passt", kann eine Neuinterpretation der Norm angebracht sein[372]. Hierbei ist jedoch zu beachten, dass ein Gesetz regelmäßig für eine Vielzahl von auch zukünftigen Fällen konzipiert wurde und dadurch den unterworfenen Bürgern eine gewisse Konstanz garantiert werden soll. In diesem Spannungsverhältnis ist erst dann eine Neuinterpretation des Gesetzes durch eine veränderte Auslegung oder richterliche Rechtsfortbildung angebracht, wenn die Unzulänglichkeit des bisherigen Gesetzesverständnisses „evident" geworden ist[373].

Für die Versammlungsfreiheit im Sinne des Art. 8 Abs. 1 GG ist zu beachten, dass das Grundrecht in der Praxis auch weiterhin unverändert seinen ursprünglichen Anwendungsbereich hat, es also ohne die Ausdehnung auf „virtuelle Versammlungen" nichts von seiner Relevanz einbüßt[374]. Da eine neue Auslegung im Rahmen des Wortsinnes und des Kontextes des Gesetzes liegen muss und sich in der Regel nicht über den Zweck des Gesetzes hinwegsetzen darf[375], würde eine Ausdehnung auf die virtuelle Welt den Ver-

369 BVerfGE 104, 92, 104; 111, 147, 154.

370 Im Ergebnis ebenso *Baudewin*, Der Schutz der öffentlichen Ordnung im Versammlungsrecht, 2007, S. 145 ff.; *Klutzny*, RDV 2006, 50, 51 ff.; *Seidel*, DÖV 2002, 283, 285. Depenheuer vergleicht dabei die Diskussionsforen im Internet mit einer Telefonkonferenz, welche auch nicht von Art. 8 Abs. 1 GG geschützt wird. Zwar ist dieser Vergleich nicht besonders passend gewählt, da sich die visualisierte, grundsätzlich jedem zugängliche Kommunikation im Internet tiefgreifend von der von bestimmten Personen ausgeübten Kommunikation durch das gesprochene Wort bei einer Telefonkonferenz unterscheidet, jedoch ist Depenheuer im Ergebnis unumwunden zuzustimmen. Siehe *Depenheuer*, in: Maunz/Dürig, Grundgesetz, Bd. 2, Art. 8, Rdnr. 45.

371 Vertiefend zur Wirksamkeit und Legitimität der Rechtsfortbildung siehe *Zippelius*, Juristische Methodenlehre, 10. Aufl., 2006, S. 78 ff.

372 Vgl. *Kraft/Meister*, MMR 2003, 366, 367 ff.

373 Vgl. *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, 3. Aufl., 1995, S. 171.

374 *Kraft/Meister*, MMR 2003, 366, 368.

375 *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, 3. Aufl., 1995, S. 171.

sammlungsbegriff überdehnen. Als ein wesentliches Charakteristikum des Versammlungsbegriffs wird die örtliche Zusammenkunft gefordert. Diese äußere Verbundenheit liegt bei einer „virtuellen Versammlung" gerade nicht vor, da jeder Teilnehmer über seinen Rechner, räumlich getrennt von den anderen Teilnehmern, kommuniziert[376]. Zudem ist dem einzelnen Teilnehmer einer „virtuellen Versammlung" oftmals noch nicht einmal ersichtlich, ob und mit wie vielen anderen Nutzern er eine Meinung kundgibt. Da sich die Kommunikation in Diskussionsforen oftmals über längere Zeiträume – sogar Jahre – hinziehen kann und dabei nicht unbedingt jederzeit überhaupt ein Teilnehmer dieser „virtuellen Versammlung" online ist, mangelt es vielfach an diesem zeitlichen Element. Daher besteht kein Anlass für einen Wandel im Verständnis des grundgesetzlichen Versammlungsbegriffs.

Soweit eine Vielzahl von Internet-Nutzern in einem Massenzugriff eine Webseite „besetzt", liegt ebenso bereits mangels körperlicher Präsenz keine Versammlung im rechtlichen Sinne vor, da lediglich elektronische Signale von verschiedenen Orten durch räumlich getrennte Menschen an einen Server gesandt werden[377].

Eine mögliche Verletzung der Versammlungsfreiheit könnte aber darin liegen, dass häufig die Orte, Daten etc. für Versammlungen über das Internet verbreitet werden[378] und dies durch die Polizei überwacht wird. Es ist allgemein anerkannt, dass die Freiheitsverbürgung des Art. 8 Abs. 1 GG ihre Wirkung nicht erst mit dem Beginn einer Versammlung entfaltet, sondern die Versammlungsfreiheit ebenso die vorbereitenden Maßnahmen und die ungehinderte Anreise zum Versammlungsort garantiert[379]. Damit können

376 Ähnlich *Kraft/Meister*, MMR 2003, 366, 368.

377 *Depenheuer*, in: Maunz/Dürig, Grundgesetz, Bd. 2, Art. 8, Rdnr. 45. Ein derartiger Massenzugriff, auch „virtueller Sit-in" genannt, kann durchaus auch zu einer Art Meinungskundgabe genutzt werden. Am 20.06.2001 fand während der Hauptversammlung der Lufthansa AG die Aktion „Lufthansa goes offline" statt. Dabei sollten durch massive Zugriffe auf die Lufthansa-Webseite die Server zum Absturz gebracht werden. Durch diese Aktion sollte auf den Umstand, dass sich die Lufthansa AG an Abschiebungen beteiligt, hingewiesen werden bzw. das Image des Unternehmens geschädigt werden. Da das Unternehmen vor Beginn der Aktion seine Server-Kapazitäten erhöht hatte, konnte ein Totalabsturz verhindert werden. Zu den Rechtsproblemen „virtueller Sit-ins" siehe *Kraft/Meister*, MMR 2003, 366, 368.

378 Siehe zu den rechtlichen Aspekten der Koordination von Versammlungen über Soziale Netzwerke *Söllner/Wecker*, ZRP 2011, 179 ff.

379 BVerfGE 69, 315, 349; 84, 203, 209; *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 292; *Kniesel/Poscher*, in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl., 2012, Kap. K, Rdnr. 57; *Depenheuer*, in: Maunz/Dürig, Grundgesetz, Bd. 2, Art. 8, Rdnr. 75 und 125; *Geis*, Die Polizei, 1993, 293 ff.; *ders.*, in: Berliner Kommentar zum Grundgesetz, Stand Juli 2012, Art. 8, Rdnr. 34; *Brenneisen*, DuD 2000, 651 m. w. N.

informationelle Eingriffe im Vorfeld von Versammlungen den verfassungsrechtlichen Schutzbereich des Art. 8 Abs. 1 GG betreffen[380].

Nach der Rechtsprechung des Bundesverfassungsgerichts kann eine exzessive Observation und Registrierung der (potentiellen) Versammlungsteilnehmer einen Grundrechtseingriff darstellen[381]. Das Bundesverfassungsgericht stellt in seinem Urteil zur automatisierten Erfassung von Kraftfahrzeugkennzeichen klar, dass die gezielte Notierung der Versammlungsteilnehmer eine verhaltenssteuernde Wirkung entfalten und die ausgeübten Kommunikationsfreiheiten als eingriffsgleiche Maßnahme betreffen kann[382].

Bei den Polizeistreifen im Internet wird man nicht von einer exzessiven Observation ausgehen können. Diese exzessive Observation würde auch nicht mehr als verdachtsunabhängige Ermittlung einzustufen sein, sondern auf die Abwehr konkreter Gefahren zielen. Soweit überhaupt eine mit einer Observation vergleichbare virtuelle Überwachung bestimmter Personen stattfinden sollte, dürfte diese nicht als exzessiv zu bewerten sein. Zudem kommt in diesem Fall hinzu, dass diese Überwachung von der Zielperson nicht registriert wird und damit keine Einwirkung auf die Entscheidung stattfindet, ob diese Person an einer Versammlung teilnehmen will oder dieses unterlässt. Nach dem derzeitigen Informationsstand[383] scheidet daher ein Eingriff in die Versammlungsfreiheit durch die Maßnahmen der Polizei im Rahmen der verdachtsunabhängigen Ermittlungen im Internet aus.

V. Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG)

Das Recht auf die freie Entfaltung der Persönlichkeit des Art. 2 Abs. 1 GG gewährleistet neben der allgemeinen Handlungsfreiheit, die als aktives Element der Persönlichkeitsentfaltung jegliche Erscheinungsform menschlichen Verhaltens erfasst, auch das allgemeine Persönlichkeitsrecht. Das allgemeine Persönlichkeitsrecht schützt dabei als „unbenanntes“ Freiheitsrecht die „engere persönliche Lebenssphäre und die Erhaltung ihrer Grund-

380 Vgl. dazu vertiefend *Brenneisen*, DuD 2000, 651 ff.

381 BVerfGE 69, 315, 349. Bereits in seinem Volkszählungsurteil hat das Bundesverfassungsgericht diesen möglichen Eingriff angedeutet, BVerfGE 65, 1, 43. So auch *Benda*, in: BK, Grundgesetz, Bd. 3, Art. 8, Rdnr. 96; *Depenheuer*, in: Maunz/Dürig, Grundgesetz, Bd. 2, Art. 8, Rdnr. 125.

382 BVerfGE 120, 378, 406; vgl. auch *Kunig*, in: von Münch/Kunig, Grundgesetz, Bd. 1, 6. Aufl., 2012, Art. 8, Rdnr. 19 m. w. N.

383 Vgl. die Antwort der Bundesregierung vom 14.07.2011 auf eine Kleine Anfrage, BT-Drs 17/6587, S. 3 ff., sowie die Informationen zur Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) unter *www.bka.de/*.

bedingungen“ und ist damit vornehmlich statisch auf die „Respektierung des geschützten Bereichs“ gerichtet[384].

Bereits in der Elfes-Entscheidung aus dem Jahre 1957 hat das Bundesverfassungsgericht auf die besondere Schutzbedürftigkeit der menschlichen Persönlichkeit in ihrer geistig-seelischen Dimension hingewiesen, die dem einzelnen Bürger eine „Sphäre privater Lebensgestaltung“ und einen letzten, unantastbaren Bereich menschlicher Freiheit zugesteht[385]. Als dogmatischer Ausgangspunkt für das allgemeine Persönlichkeitsrecht wird heute allgemein Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG angesehen[386]. Die Verbindung von Art. 2 Abs. 1 GG und Art. 1 Abs. 1 GG hat allerdings nicht zur Folge, dass hier zwei Grundrechte kumulativ zur Anwendung kämen[387]. Als subjektives Recht ist das allgemeine Persönlichkeitsrecht auf Art. 2 Abs. 1 GG zurückzuführen, während Art. 1 Abs. 1 GG auf die Rolle als Auslegungsmaßstab für die Ermittlung des Inhalts und der Reichweite des Schutzumfangs begrenzt ist[388].

Das allgemeine Persönlichkeitsrecht soll dabei „namentlich auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen für den Schutz der menschlichen Persönlichkeit“ gewährt werden[389], womit auch neuartige Gefährdungen der Persönlichkeitsentfaltung, die meist in Begleitung des wissenschaftlich-technischen Fortschritts auftre-

384 Vgl. BVerfGE 54, 148, 153. Entwickelt wurde das allgemeine Persönlichkeitsrecht in Rechtslehre und Rechtsprechung im Anschluss an wegbereitende Entscheidungen des Bundesgerichtshofs zu einem ergänzenden Persönlichkeitsschutz unter Verankerung in Art. 2 Abs. 1 GG. Vgl. zur Entwicklung des Persönlichkeitsschutzes in Literatur sowie Rechtsprechung des Bundesgerichtshofs und des Bundesverfassungsgerichts *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?, 1987, S. 39 ff.; *Brandner*, JZ 1983, 689 ff.; *Seifert*, NJW 1999, 1889 ff.; *Jarass*, NJW 1989, 857 ff.

385 BVerfGE 6, 32, 41. Das Bundesverfassungsgericht führte in dieser Entscheidung fast schon pathetisch auf S. 41 aus (wörtlich zitiert): *„Hieraus ergibt sich, daß dem einzelnen Bürger eine Sphäre privater Lebensgestaltung verfassungskräftig vorbehalten ist, also ein letzter unantastbarer Bereich menschlicher Freiheit besteht, der der Einwirkung der gesamten öffentlichen Gewalt entzogen ist. Ein Gesetz, das in ihn eingreifen würde, könnte nie Bestandteil der „verfassungsmäßigen Ordnung“ sein; es müßte durch das Bundesverfassungsgericht für nichtig erklärt werden.“*

386 Beispielsweise BVerfGE 27, 1, 6; 54, 148, 153; mit einer Vielzahl an weiteren Nachweisen *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 128. Gegen eine Inbezugnahme des Art. 1 Abs. 1 GG *Lorenz*, JZ 2005, 1121, 1125; *ders.*, in: BK, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 33 ff.; *Luch*, Das Medienpersönlichkeitsrecht, 2008, S. 85 ff.; *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 25 ff.

387 *Murswiek*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 2, Rdnr. 63.

388 Vgl. *Murswiek*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 2, Rdnr. 63; *Starck*, in: v. Mangoldt/Klein/Starck, Grundgesetz, 6. Aufl., 2010, Art. 2 Abs. 1, Rdnr. 15; *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 128 m. w. N.

389 BVerfGE 54, 148, 153.

ten, umfasst werden sollen[390]. Eine abschließende Festlegung des Schutzbereichs ist damit nicht möglich[391], weshalb es sich um ein entwicklungsoffenes Freiheitsrecht handelt.

Das Bundesverfassungsgericht hat im Laufe seiner Rechtsprechung das allgemeine Persönlichkeitsrecht in verschiedenen Fallgruppen konkretisiert, die als Antworten auf moderne Beeinträchtigungen, die nicht bereits von den bestehenden Freiheitsrechten erfasst werden, zu sehen sind[392]. Zu diesen Ausprägungen des allgemeinen Persönlichkeitsrechts gehören beispielsweise das Recht auf informationelle Selbstbestimmung, der Schutz der Privatsphäre, das Recht am eigenen Wort oder das neu durch das Bundesverfassungsgericht entwickelte Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[393].

1. Verhältnis des allgemeinen Persönlichkeitsrechts zu anderen Grundrechten

Das allgemeine Persönlichkeitsrecht mit all seinen Ausprägungen und Unterfällen kann in seinem Regelungsbereich neben einer Vielzahl von anderen Grundrechten anwendbar sein. Während für die allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG weitestgehend Einigkeit besteht, dass dieses Grundrecht als Auffanggrundrecht hinter die speziellen Freiheitsrechte zurücktritt[394], ist bei dem allgemeinen Persönlichkeitsrecht genauer zu differenzieren. Da das allgemeine Persönlichkeitsrecht als „unbenanntes" Freiheitsrecht einen besonders schutzwürdigen Lebensbereich gegen Eingriffe absichern soll, ist es im Verhältnis zur allgemeinen Handlungsfreiheit das speziellere Grundrecht und verdrängt dieses[395]. Neben den speziellen Freiheitsrechten steht das allgemeine Persönlichkeitsrecht grundsätzlich selbständig[396]. Dies gilt allerdings nur, soweit der Persönlichkeitsschutz als zusätzlicher Gesichtspunkt eigenständig neben den Freiheitsbereich des konkurrierenden Grundrechts tritt. Wenn dagegen das andere Grundrecht in einem Teilbereich Gehalte des Persönlichkeitsrechts sichert, wie beispielsweise Art. 10 GG oder Art. 13 GG, geht dieses Grundrecht regelmäßig

390 BVerfGE 101, 361, 380; BVerfGE 120, 274, Absatz 169.

391 *Siekmann/Duttge*, Grundrechte, 3. Aufl., 2000, Rdnr. 846.

392 *v. Mutius*, Anonymität als Element des allgemeinen Persönlichkeitsrechts, in: Bäumler/von Mutius, Anonymität im Internet, 2003, S. 12, 14. Siehe zu den gebildeten Fallgruppen auch *Wanckel*, Persönlichkeitsschutz in der Informationsgesellschaft, 1999, S. 116 ff.

393 Auf die genannten Ausprägungen soll weiter unten vertieft eingegangen werden.

394 Vgl. nur *Heß*, Grundrechtskonkurrenzen, 1999, S. 216, m. w. N.

395 Vgl. *Dreier*, in: ders., Grundgesetz, Bd. 1, 2. Aufl., 2004, Art. 2 Abs. 1, Rdnr. 94; *Murswiek*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 2, Rdnr. 64.

396 *Murswiek*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 2, Rdnr. 138; *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 25; *Kunig*, in: von Münch/Kunig, Grundgesetz, Bd. 1, 6. Aufl., 2012, Art. 2, Rdnr. 91.

vor[397]. Allerdings wird das allgemeine Persönlichkeitsrecht dort nicht verdrängt, „wo sich der Schutzbereich dieses Grundrechts mit demjenigen eines speziellen Freiheitsrechts nur partiell überschneidet oder in den Fällen, in denen ein eigenständiger Freiheitsbereich mit festen Konturen erwachsen ist“[398]. In welchen Fällen nur eine partielle Überschneidung der Schutzbereiche vorliegt oder sich ein eigenständiger, fest umrissener Freiheitsbereich etabliert hat, ist regelmäßig nur schwierig einzuschätzen. Insbesondere bei einem entwicklungsoffenen Freiheitsrecht wie dem allgemeinen Persönlichkeitsrecht drohen dadurch die Konturen noch stärker zu verwischen und es besteht die Gefahr, dass sich dieser ungeschriebene grundrechtliche Schutz intransparent und willkürlich ausdehnt.

Für das Telekommunikationsgeheimnis bzw. Fernmeldegeheimnis hat das Bundesverfassungsgericht gegenüber dem Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts ein Ergänzungsverhältnis angenommen[399].

Das Bundesverfassungsgericht führt dazu aus:

„Fernmeldegeheimnis und Recht auf informationelle Selbstbestimmung stehen, soweit es den Schutz der Telekommunikationsverbindungsdaten betrifft, in einem Ergänzungsverhältnis. In seinem Anwendungsbereich enthält Art. 10 GG bezogen auf den Fernmeldeverkehr eine spezielle Garantie, die die allgemeine Gewährleistung des Rechts auf informationelle Selbstbestimmung verdrängt (vgl. BVerfGE 67, 157, 171; 100, 313, 358; 107, 299, 312; 110, 33, 53; Urteil des Ersten Senats des Bundesverfassungsgerichts vom 27. Juli 2005 – 1 BvR 668/04 –, NJW 2005, S. 2603, 2604). Soweit der Eingriff in das Fernmeldegeheimnis die Erlangung personenbezogener Daten betrifft, sind dabei die Maßgaben, die das Bundesverfassungsgericht im Volkszählungsurteil aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG entwickelt hat (vgl. BVerfGE 65, 1, 44 ff.), grundsätzlich auch auf die speziellere Garantie in Art. 10 Abs. 1 GG zu übertragen (vgl. BVerfGE 100, 313, 359; 110, 33, 53).

Greift Art. 10 GG nicht ein, werden die in der Herrschaftssphäre des Betroffenen gespeicherten personenbezogenen Verbindungsdaten durch das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützt. Damit wird der besonderen Schutzwürdigkeit der Telekommunikationsumstände Rechnung getragen und die Vertraulichkeit räumlich distanzierter Kommunikation auch nach Beendigung des Übertragungsvorgangs gewahrt.“[400]

397 Vgl. *Jarass*, in: Jarass/Pieroth, Grundgesetz, 12. Aufl., 2012, Art. 2, Rdnr. 38; *Epping*, Grundrechte, 4. Aufl., 2010, Rdnr. 648 ff. m. w. N.

398 BVerfGE 115, 166, 187.

399 BVerfGE 115, 166, 188 ff.

400 BVerfGE 115, 166, 188 ff.

Damit ist das allgemeine Persönlichkeitsrecht mit seinen Ausprägungen grundsätzlich neben den Freiheitsrechten wie Art. 10 GG und Art. 13 GG anwendbar, soweit diese keinen oder keinen hinreichenden Schutz gewähren[401]. Art. 10 GG und Art. 13 GG können zwar vor Datenerhebungen schützen, die dem Telekommunikationsgeheimnis widerstreben bzw. in Wohn- oder Geschäftsräumen stattfinden. Jedoch bieten die beiden Grundrechte, wie bereits oben gezeigt wurde, keinen ausreichenden Schutz im Zusammenhang mit den verdachtsunabhängigen Ermittlungen der Polizei im Internet. Daher ist das allgemeine Persönlichkeitsrecht, insbesondere mit seinen Ausprägungen, dem Recht auf informationelle Selbstbestimmung, dem Recht am eigenen Wort, dem Schutz der Privatsphäre und dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, hier anwendbar, um bei den neuartigen Gefährdungen einen lückenlosen Grundrechtsschutz zu gewährleisten.

2. Das Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung gewährleistet dem Einzelnen als Ausprägung[402] des allgemeinen Persönlichkeitsrechts die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen[403]. Es steht in engem Zusammenhang mit dem in Deutschland seit dem Jahre 1970 kodifizierten Datenschutzrecht[404] und soll den Einzelnen vor den neuartigen Gefahren der Informationsgesellschaft schützen. Insbesondere im Internet ist zumeist mit geringem Aufwand eine Unmenge an Daten – teils öffentlich und teils in geschützten Bereichen – zu erheben.

Für die rechtliche Beurteilung, ob das Recht auf informationelle Selbstbestimmung durch die verdachtsunabhängigen Ermittlungen der Polizei im Internet verletzt wird, ist von zentraler Bedeutung, wie der Schutzbereich

401 Vgl. BVerfGE 120, 274, 303. Siehe zur Abgrenzung des Rechts auf informationelle Selbstbestimmung zu anderen Grundrechten auch *Schoch*, Jura 2008, 352, 355.

402 Statt „Ausprägung" werden in der Literatur häufig andere Begriffe, wie beispielsweise „Fallgruppe", „Komponente" oder „Teilbereich" genannt. Trotz dieser unterschiedlichen Terminologie ist aber die Zugehörigkeit des Rechts auf informationelle Selbstbestimmung zum allgemeinen Persönlichkeitsrecht übereinstimmend anerkannt, vgl. weiterführend *Wanckel*, Persönlichkeitsschutz in der Informationsgesellschaft, 1999, S. 129.

403 BVerfGE 113, 29, 46; 115, 166, 188; 118, 168, 184. Der Ausdruck „informationelles Selbstbestimmungsrecht" wird in der Literatur nicht von allen als besonders glückliche Umschreibung angesehen, siehe z. B. *Starck*, in: v. Mangoldt/Klein/Starck, Grundgesetz, Bd. 1, 6. Aufl., 2010, Art. 2 Abs. 1, Rdnr. 114 m. w. N.

404 Zunächst wurde als erstes Datenschutzgesetz der Welt das Hessische DSG am 30.09.1970 (GBl. 1970, S. 625) verkündet. Das erste nationale Datenschutzgesetz trat in Schweden 1973 in Kraft. Nach heftigen parlamentarischen Kontroversen folgte schließlich am 01.01.1978 das BDSG (BGBl. I 1977, S. 201). Vgl. vertiefend *Abel*, Geschichte des Datenschutzrechts, in: Roßnagel, Hdb. Datenschutzrecht, 2003, S. 194 ff.

und vor allem ein Eingriff in diesen Schutzbereich definiert werden. Hierfür soll vorab die Entwicklung des Rechts auf informationelle Selbstbestimmung dargestellt werden, um die Bedeutung dieses Rechts sowohl im historischen als auch im verfassungsrechtlichen Kontext zu erfassen[405].

2.1 Entwicklung des Rechts auf informationelle Selbstbestimmung

Das Bundesverfassungsgericht hat das Recht auf informationelle Selbstbestimmung erstmalig im Volkszählungsurteil vom 15.12.1983[406] aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG entwickelt[407]. Dem Urteil lagen mehrere Verfassungsbeschwerden gegen das Volkszählungsgesetz (VZG)[408] zu Grunde. Nach dem VZG waren beispielsweise der Name und die Anschrift, der Geburtstag, die Quelle des überwiegenden Lebensunterhalts, die rechtliche Zugehörigkeit zu einer Religionsgesellschaft, die Berufsausbildung, die Stellung im Beruf und im Anstaltsbereich die Eigenschaft als Insasse oder die Zugehörigkeit zum Personal zu erheben[409]. In § 5 VZG wurde bestimmt, wer auskunftspflichtig war. Zur Weiterleitung der erhobenen Daten enthielt § 9 VZG verschiedene Übermittlungsregelungen.

Bei der einstimmigen Verabschiedung des VZG von Bundestag und Bundesrat 1982 ahnte wahrscheinlich keiner der Volksvertreter, welche Brisanz dieses Gesetz entwickeln würde und dass damit die Geburtsstunde des Rechts auf informationelle Selbstbestimmung mit seinen nachhaltigen Auswirkungen bis heute und auch für die Zukunft verbunden sein würde[410]. Die

405 Vgl. zur politischen Entwicklung und Diskussion des Rechts auf informationelle Selbstbestimmung *Wiedemann*, Regieren mit Datenschutz und Überwachung, 2011.

406 BVerfGE 65, 1.

407 Siehe vertiefend zur Entwicklung des Volkszählungsurteils *Albers*, Informationelle Selbstbestimmung, 2005, S. 152 ff.; *Baumann*, DVBl 1984, 612 ff.; *Benda*, DuD 1984, 86 ff.; *Denninger*, KJ 1985, 215 ff.; *Son*, Heimliche polizeiliche Eingriffe in das informationelle Selbstbestimmungsrecht, 2006, S. 32 ff.

408 Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung vom 25.03.1982, BGBl I, S. 369.

409 Vgl. § 2 des VZG.

410 Ob sich auch alle Richter des Bundesverfassungsgerichts der besonderen Bedeutung dieses neuen Rechts bewusst waren, ist nicht ganz sicher. So bestand anscheinend keine Gewissheit darüber, ob die informationelle Selbstbestimmung ein Grundrecht ist oder nicht. In dem NJW-Abdruck (NJW 1984, 425) wird die Formulierung „Grundrecht auf informationelle Selbstbestimmung" gewählt, während in der amtlichen Sammlung (BVerfGE 65, 1, 58) lediglich von einem „Recht auf informationelle Selbstbestimmung" gesprochen wird. Daher sind die teilweise gewonnenen Eindrücke, dass das Urteil „mit heißer Nadel gestrickt ist", nicht völlig von der Hand zu weisen, vgl. dazu *Rogall*, Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht, 1992, S. 42 ff.; *Schneider*, DÖV 1984, 161. In der Presse wurde vielfach von der Erfindung eines neuen Grundrechtes gesprochen, so beispielsweise Fromme in der Frankfurter Allgemeinen Zeitung vom 17.12.1983, S. 12. Mittlerweile dürfte in Literatur und Praxis allerdings die Frage, ob mit dem Recht auf informationelle Selbstbestimmung ein

durch das VZG geplanten Datenerhebungen des Staates kanalisierten die Befürchtungen vieler Bürger vor der modernen Datenverarbeitung und führten zu massenhaftem Widerstand gegen das Gesetz. Bürger aus den unterschiedlichsten politischen Lagern und sozialen Schichten legten Rechtsmittel ein oder verweigerten die geforderten Auskünfte[411]. Das Bundesverfassungsgericht erkannte die Zeichen der Zeit und setzte sich in seinem richtungsweisenden Urteil grundlegend mit den verfassungsrechtlichen Anforderungen an die Verarbeitung personenbezogener Daten auseinander. Bezogen auf das VZG erkannte es die Übermittlungsregelungen im VZG überwiegend für unvereinbar mit Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG. Die Ermächtigungsnormen zur Datenerhebung hingegen waren nach Ansicht des Bundesverfassungsgerichts, sofern ergänzende verfahrensrechtliche Vorkehrungen für Durchführung und Organisation der Datenerhebung getroffen würden, verfassungsgemäß.

Als Leitsätze hielt das Bundesverfassungsgericht unter anderem fest:

„1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.“[412]

---

neues Grundrecht entwickelt, eine neue Grundrechtsbedeutung entdeckt oder eine alte Grundrechtsbedeutung neu interpretiert wurde, überwiegend in den Hintergrund getreten sein, siehe dazu bereits *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?, 1987, 52. Das Bundesverfassungsgericht spricht in neueren Entscheidungen bezüglich des Rechts auf informationelle Selbstbestimmung von einem Grundrecht, vgl. BVerfGE 113, 29, 46; 115, 166, 188.

411 Die Situation ist wahrscheinlich vergleichbar mit dem Protest gegen die sog. Vorratsdatenspeicherung, die nach Verabschiedung des Gesetzes in einer Verfassungsbeschwerde mit über 34.000 Beschwerdeführern gipfelte, siehe dazu auch *http://www.heise.de/newsticker/meldung/34-443-Klageschriften-gegen-die-Vorratsdatenspeicherung-185285.html* sowie *http://www.vorratsdatenspeicherung.de/content/view/46/42/lang,de/*.

412 BVerfGE 65, 1.

Das Bundesverfassungsgericht stellt zunächst in dem Urteil fest, dass die bis zu dem Zeitpunkt durch die Rechtsprechung erfolgten Konkretisierungen den Inhalt des allgemeinen Persönlichkeitsrechts nicht abschließend umschreiben[413]. Als Anknüpfungspunkt für die Konstitution des Rechts auf informationelle Selbstbestimmung sieht das Gericht die moderne Datenverarbeitung. Mit Hilfe der automatischen Datenverarbeitung seien Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar. Eine besondere Gefahr wird dabei in dem Zusammenfügen der gesammelten Daten zu einem weitgehend vollständigen Persönlichkeitsbild gesehen, dessen Richtigkeit und Verwendung der Betroffene nicht zureichend kontrollieren könne[414]. Genau vor diesen Gefahren der Einsicht- und auch Einflussnahme solle aber der Einzelne geschützt werden.

Das Bundesverfassungsgericht wählte hingegen im vorausgegangenen Mikrozensus-Beschluss noch einen weniger weitreichenden Ansatz. In dem Beschluss führte das Gericht aus, dass es mit der Menschenwürde unvereinbar sei, wenn der Staat das Recht für sich in Anspruch nehmen könne, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich sei[415]. Im Vordergrund stand also der Schutz des Menschen vor Herabwürdigung zum bloßen Objekt. Im Folgenden deutete das Gericht im Mikrozensus-Beschluss eines der wesentlichen Elemente zur Herleitung des Rechts auf informationelle Selbstbestimmung an. Das Bundesverfassungsgericht sah in der staatlichen Einsichtnahme in den engen Bereich privater Lebensgestaltung ein Hemmnis für die freie Entfaltung der Persönlichkeit durch den „psychischen Druck öffentlicher Anteilnahme“[416]. Diesen Gedanken verfolgte das Bundesverfassungsgericht auch in nachfolgenden Entscheidungen[417] weiter und präzisierte und erweiterte ihn schließlich, ausgehend von der individuellen Selbstbestimmung, zum Recht auf informationelle Selbstbestimmung.

Als wesentliches Element der individuellen Selbstbestimmung sieht es das Bundesverfassungsgericht an, dass der Einzelne frei entscheiden kann,

413 BVerfGE 65, 1, 41.

414 BVerfGE 65, 1, 42; zu dieser Problematik bereits *Benda*, Privatsphäre und „Persönlichkeitsprofil“, in: Leibholz/Faller/Mikat/Reis, Menschenwürde und freiheitliche Rechtsordnung: Festschrift für Willi Geiger, 1974, S. 23 ff.

415 BVerfGE 27, 1, 6; vgl. auch zum Mikrozensus-Beschluss die Ausführungen von *Albers*, Informationelle Selbstbestimmung, 2005, S. 195 ff.

416 BVerfGE 27, 1, 6 ff.

417 BVerfGE 27, 344, 350 ff.; 32, 373, 379; 35, 202, 220; 44, 353, 372 ff.; 54, 148, 155 ff.

welche Handlungen er vornimmt oder unterlässt[418]. Wer dabei nicht mit hinreichender Sicherheit überschauen könne, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt seien, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermöge, könne in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden[419].

Zum Recht auf informationelle Selbstbestimmung führt das Bundesverfassungsgericht weiter aus:

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“[420]

Da der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann, stellte das Bundesverfassungsgericht im Weiteren klar heraus, dass es unter den Bedingungen der auto-

418 BVerfGE 65, 1, 42 ff.

419 Bereits im Jahre 1890 haben *Samuel D. Warren* und *Louis D. Brandeis* in ihrem berühmt gewordenen Artikel „The Right to Privacy“ gegenüber der Presse für jeden ein „Right to be let alone“ gefordert, damit jeder nach eigenem Dafürhalten entscheiden und handeln kann, *Warren/Brandeis*, Havard Law Review, 1890, S. 193 ff. Siehe dazu auch *Horn*, Schutz der Privatsphäre, in: HStR VII, 3. Aufl., 2009, § 149, Rdnr. 14 ff.

420 BVerfGE 65, 1, 43.

matischen Datenverarbeitung kein belangloses Datum mehr gebe[421]. Ein für sich genommen belangloses Datum kann nämlich im Zusammenhang mit anderen Daten, beispielsweise durch die modernen Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologie, einen neuen Stellenwert erlangen.

Das Verfügungsrecht des Einzelnen über die Verwendung seiner personenbezogenen Daten besteht aber nicht unbeschränkt, sondern er muss grundsätzlich Einschränkungen seines Rechts auf informationelle Selbstbestimmung hinnehmen, wenn dies zum Schutz überwiegender Allgemeininteressen erforderlich ist. Diese Einschränkungen bedürfen allerdings einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht. Weiterhin hat der Gesetzgeber den Grundsatz der Verhältnismäßigkeit zu beachten und den Verwendungszweck der Daten bereichsspezifisch und präzise in der Ermächtigungsgrundlage zu bestimmen[422].

Nach dem Volkszählungsurteil hat sich das Bundesverfassungsgericht in zahlreichen weiteren Entscheidungen mit dem Recht auf informationelle Selbstbestimmung befasst und es dabei weiterentwickelt und konkretisiert[423]. Gerade in der neueren Literatur gibt es allerdings eine Vielzahl an Ansätzen[424], die insbesondere auf Grund der Digitalisierung der Welt durch das Internet das Recht auf informationelle Selbstbestimmung und das damit zusammenhängende Datenschutzrecht vor umfassenden Reformen sehen[425].

2.2 Schutzbereich

Durch das Recht auf informationelle Selbstbestimmung wird, wie oben bereits festgestellt wurde, dem Einzelnen die Befugnis gewährt, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen[426]. Geschützt werden dabei die persönlichen bzw. personenbezogenen Daten. Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person[427]. Damit fallen alle Informationen, die sich auf eine

421 BVerfGE 65, 1, 45.

422 Vgl. zum Ganzen BVerfGE 65, 1, 44 ff.

423 Weiterführend dazu *Frenz*, DVBl 2009, 333 ff.; *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2008, S. 77 ff.; *Albers*, Informationelle Selbstbestimmung, 2005, S. 241 ff.; *Placzek*, Allgemeines Persönlichkeitsrecht und privatrechtlicher Informations- und Datenschutz, 2006, S. 64 ff.

424 Auf diese Ansätze wird im Folgenden näher eingegangen.

425 Vgl. nur *Bull*, NVwZ 2011, 257 ff.; *Ladeur*, DÖV 2009, 45 ff.; bereits schon früher *Lorenz*, JZ 1996, 716 ff.

426 BVerfGE 113, 29, 46; 115, 166, 188; 118, 168, 184; 120, 274, 312.

427 So bezog sich das Bundesverfassungsgericht bereits im Volkszählungsurteil auf die Definition in § 2 Abs. 1 BDSG a. F., BVerfGE 65, 1, 42. Siehe dazu auch *Schaar*, Datenschutz im Internet, S. 46 ff.

bestimmte einzelne natürliche Person beziehen oder geeignet sind, einen Bezug zu ihr herzustellen, unter den weiten Begriff der personenbezogenen Daten[428].

2.2.1 Allgemeine Bestimmung des Schutzbereichs

Für den Schutzbereich des Rechts auf informationelle Selbstbestimmung darf nicht nur an dem einzelnen Datum festgehalten werden. Nicht die inhaltliche Nähe zur wie auch immer definierten Intim-, Geheim- oder Privatsphäre des jeweiligen Datums bestimmt, ob der Schutzbereich eröffnet wird oder nicht[429]. Damit ist auch die Ansicht abzulehnen, die in Anlehnung an die „Sphärentheorie" von einem bereichsspezifisch abgestuften Persönlichkeitsschutz ausgeht[430]. Da es im Rahmen der elektronischen Datenverarbeitung kein schlechthin, also ungeachtet des Verwendungskontextes, belangloses personenbezogenes Datum gibt, beschränkt sich der Schutzumfang des Rechts auf informationelle Selbstbestimmung nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden[431]. Dadurch wird deutlich, dass die informationelle Selbstbestimmung nicht daten-, sondern verwendungsorientiert ist, was eine Kategorisierung oder Privilegierung bestimmter Arten von Daten ausschließt[432].

Selbst wenn ein Datum nur geringen Informationsgehalt hat, kann der Umgang mit dem Datum, je nach Ziel und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, durchaus auf die Privatheit und Verhaltensfreiheit eines Betroffenen grundrechtsrelevante Auswirkungen haben[433]. Es kommt also allein auf die abstrakte Eignung eines Datums an. Damit flankiert und erweitert das Recht auf informationelle Selbstbestimmung den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem der Schutz bereits auf der Stufe einer Persönlichkeitsgefährdung beginnt[434]. Zutreffend geht das Bundesverfassungsgericht folglich davon aus, dass

428 Vgl. *Gola/Schomerus*, BDSG, 11. Aufl., 2012, § 3, Rdnr. 3.

429 So auch *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 174; *Schwenke*, Individualisierung und Datenschutz, 2006, S. 70.

430 So setzt sich *Böckenförde*, Die Ermittlung im Netz, 2003, S. 182 ff., noch für einen abgestuften Persönlichkeitsschutz im Sinne des „Sphärenmodells" zur Bestimmung des sachlichen Schutzbereichs des Rechts auf informationelle Selbstbestimmung ein. Ob das Bundesverfassungsgericht im Volkszählungsurteil die „Sphärentheorie" aufgegeben, relativiert oder beibehalten hat, ist umstritten. Zum Streitstand siehe *Albers*, Informationelle Selbstbestimmung, 2005, S. 162, Fn. 52.

431 BVerfGE 120, 378, 398 ff.

432 Simitis, NJW 1984, 394, 402 ff.

433 BVerfGE 118, 168, 185.

434 So auch *Scholz/Pitschas*, Informationelle Selbstbestimmung, 1984, S. 23 ff., S. 71; *Bull*, NJW 2006, 1617, 1623; *Gruner*, Biometrie und informationelle Selbstbestimmung, 2005, S. 140.

bereits im Vorfeld einer konkreten Bedrohung eines Rechtsguts eine solche Gefährdungslage entstehen kann[435].

Insbesondere dann, wenn der Betroffene weder überschauen noch verhindern kann, in welcher Art und Weise die personenbezogenen Daten genutzt werden, kann diese Persönlichkeitsgefährdung vorliegen. Dabei liegt die Gefährdung der Persönlichkeit nicht allein in dem Wissen um Daten eines Menschen und in Informationen über ihn, sondern insbesondere in den neuen technischen Möglichkeiten ihrer Speicherung, Zusammenführung, Verknüpfung und vielfältigen Verwendung, im damit immer größeren Potential an persönlichen Daten, mit denen die Lebensweise und Lebensgestaltung eines Menschen bis hin zum Inneren entschlüsselt und entblößt werden kann[436]. Außerdem dient das Recht auf informationelle Selbstbestimmung „auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß“[437]. Um diesen Einschüchterungseffekt zu verhindern, wird damit der Schutz insoweit vorverlagert, als bereits der Einzelne vor staatlichem Verhalten geschützt werden soll, welches ihn in seiner Freiheitsausübung wesentlich hemmt[438].

Der Schutz durch das Recht auf informationelle Selbstbestimmung ist auch nicht auf die automatisierte Datenverarbeitung begrenzt, sondern erfasst generell die staatliche Erhebung und Verarbeitung personenbezogener, sogar auch manuell registrierter Daten[439].

Teilweise wird in der Literatur der Schutzbereich des Rechts auf informationelle Selbstbestimmung als konturlos und nicht abgrenzbar dargestellt[440]. Statt der dogmatischen Struktur als klassisches Eingriffsabwehrrecht sollte es in einzelne Komponenten, die spezifischen „sachgeprägten“ Grundrech-

435 Vgl. BVerfGE 120, 274, 312.

436 *Hohmann-Dennhardt*, Informationeller Selbstschutz als Bestandteil des Persönlichkeitsrechts, RDV 2008, 1, 7.

437 BVerfGE 113, 29, 46.

438 Vgl. BVerfGE 113, 29, 46; 115, 320, 342; grdl. bereits BVerfGE 65, 1, 42 ff.; kritisch dazu z. B. *Schoch*, Jura 2008, 352, 357, der die Vorverlagerung des Rechtsschutzes bei einer bestimmten „Informationsvorsorge“, die lediglich den Grad einer Belästigung des Einzelnen erreicht, für problematisch hält.

439 BVerfGE 78, 77, 84; *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 176; *Aulehner*, CR 1993, 446, 453; *Deutsch*, Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, 1992, S. 72 ff. In dem genannten Beschluss des Bundesverfassungsgerichts zur „öffentlichen Bekanntmachung der Entmündigung wegen Verschwendung oder wegen Trunksucht“ sieht das Gericht die öffentliche Bekanntmachung als eine Sonderform staatlicher Datenübermittlung an, die in das Recht auf informationelle Selbstbestimmung eingreift.

440 So beispielsweise *Ladeur*, DÖV 2009, 45 ff.

ten zuzuordnen wären, ausdifferenziert werden[441]. Diese Lösungsansätze versuchen zwar, damit die aktuellen Entwicklungen der Digitalisierung unserer Gesellschaft aufzugreifen und das Datenschutzrecht dem neuen Kommunikationsverhalten anzupassen, können jedoch nicht überzeugen. Gerade der weite Schutzbereich des Rechts auf informationelle Selbstbestimmung mit seiner Verwendungsorientierung sichert den Individuen ihre notwendige Selbstbestimmung. Eine Eingrenzung auf der Ebene des Schutzbereichs würde den Grundsätzen dieses Rechts insgesamt widersprechen. Für eine grundlegende Novellierung des Rechts auf informationelle Selbstbestimmung besteht, zumindest auf der Schutzbereichsebene, keine Notwendigkeit[442].

Bei der Bestimmung des allgemeinen Schutzbereichs stellt sich allerdings zusätzlich die Frage, ob der personelle Schutzbereich des Rechts auf informationelle Selbstbestimmung auch die Daten juristischer Personen und sonstiger Personenvereinigungen einschließt. Allgemein gelten Grundrechte gemäß Art. 19 Abs. 3 GG auch für inländische juristische Personen, wenn sie ihrem Wesen nach auch auf diese anwendbar sind. Früher wurden juristische Personen unter Berufung auf den Schutzgehalt des Persönlichkeitsrechts insbesondere im Hinblick auf seine Ableitung aus der Menschenwürdegarantie vom Schutzbereich des Persönlichkeitsrechts pauschal ausgeklammert[443]. Die aktuellere Rechtsprechung und Literatur hat sich größtenteils von dieser undifferenzierten Ablehnung gelöst und prüft nunmehr im Einzelfall, ob das Persönlichkeitsrecht in seiner jeweiligen Ausprägung einen wesentlichen Bezug zur menschlichen Persönlichkeit aufweist und aus diesem Grund nur für natürliche Personen relevant sein kann[444]. Durch hoheitliche informationelle Maßnahmen können nicht nur natürliche Personen betroffen sein, sondern diese Maßnahmen können auch Gefährdungen und Verletzungen der grundrechtlich geschützten Freiheit juristischer Personen herbeiführen und einschüchternd auf die Ausübung von Grundrechten wirken[445]. Damit besteht auch für juristische Personen in dieser Hinsicht ein Schutzbedürfnis, welches dem natürlicher Personen im

441 *Ladeur*, DÖV 2009, 45; auch *Bull* sähe grundsätzlich in der Lösung von dem dogmatischen Eingriffsdenken auf Basis des „informationellen Selbstbestimmungsrecht“ eine wirkliche Reform, *Bull*, NVwZ 2011, 257, 259.

442 Auch *Ladeur* selbst sieht seine Infragestellung des bisherigen Verständnisses des Rechts auf informationelle Selbstbestimmung eher als Anstoß zu alternativen Modellen, *Ladeur*, DÖV 2009, 45, 55.

443 Vgl. *Höfelmann*, Das Grundrecht auf informationelle Selbstbestimmung anhand der Ausgestaltung des Datenschutzrechts und der Grundrechtsnormen der Landesverfassungen, 1997, S. 69 ff.

444 Vgl. BVerfGE 95, 220, 242; 118, 168, 203; *Dreier*, in: Grundgesetz, Bd. 1, 2004, Art. 2 Abs. 1, Rdnr. 82; *Lorenz*, in: BK, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 383 m. w. N.

445 Vgl. BVerfGE 113, 29, 49.

Ansatz entspricht[446]. Für die Entscheidung, ob der Grundrechtsschutz eröffnet ist, kommt es allerdings maßgeblich auf die Bedeutung der betroffenen Informationen für den grundrechtlich geschützten Tätigkeitskreis der juristischen Person an[447]. Auch juristische Personen werden somit in den Schutzbereich des Rechts auf informationelle Selbstbestimmung einbezogen.

2.2.2 Konkrete Bestimmung des Schutzbereichs

Nachdem der Schutzbereich des Rechts auf informationelle Selbstbestimmung allgemein umrissen wurde, soll dieser im Folgenden konkret für mögliche Verletzungen durch die Polizeistreifen im Internet bestimmt werden. Die geradezu unendliche Menge an personenbezogenen Daten, die über das Internet abgerufen werden kann, wird nicht vollständig durch die Polizeistreifen im Internet oder durch sonstige staatliche Stellen erhoben und durch Polizeibeamte gesichtet. Eine vollumfängliche Überwachung des Internet würde insbesondere an den personellen Grenzen scheitern. Dennoch werden bei vielen unterschiedlichen Internetdiensten personenbezogene Daten einem bestimmten Personenkreis oder der Allgemeinheit zugänglich gemacht, die dann auch von den Polizeibehörden erhoben und gegebenenfalls verarbeitet werden können beziehungsweise könnten. Bereits bei der Betrachtung einer zufälligen Webseite im World Wide Web, gleichgültig, ob diese Webseite direkt oder durch einen Link auf einer anderen Webseite oder durch eine Suchmaschine aufgerufen wird, ist im Regelfall eine Vielzahl an personenbezogenen Daten zu erfassen. Bei vielen Webseiten von Unternehmen sind beispielsweise die Namen der Führungskräfte mit der genauen Berufsbezeichnung bzw. Position im Unternehmen, Foto, Telefonnummer und teilweise sogar mit einem detaillierten Lebenslauf veröffentlicht.

Schon die Tatsache, dass eine bestimmte Webseite im Internet unter einer bestimmten Domain-Adresse erreichbar ist, kann als personenbezogenes Datum qualifiziert werden. Über die Domain-Adresse können die auf der Webseite enthaltenen Informationen nach der Ermittlung weitergehender Daten, wie beispielsweise durch die Auskunft bei der DE-NIC über den Inhaber der Domain-Adresse, regelmäßig einer bestimmten Person zugeordnet werden. Diese Zuordnung gibt damit Aufschluss über das Verhalten der

446 BVerfGE 118, 168, 203 ff.; *Lorenz*, in: BK, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 383; *Wilms/Roth*, JuS 2004, 577. Im Ergebnis mit einer anderen Begründung so auch *Germann*, Strafverfolgung im Internet, 2000, S. 474: Danach bezögen sich die Daten einer juristischen Person immer auch auf die dahinterstehenden natürlichen Personen. Somit seien die Daten einer juristischen Person über das persönliche Attribut der Zugehörigkeit einer natürlichen zu der juristischen Person immer auch der einzelnen natürlichen Person zurechenbar.

447 BVerfGE 118, 168, 204; *Antoni*, in: Hömig, Grundgesetz, 9. Aufl., 2010, Art. 1, Rdnr. 14; *Sodan*, in: Sodan, Grundgesetz, 2009, Art. 2, Rdnr. 9.

Person, welche die Webseite betreibt. Insoweit ist es irrelevant, dass der Betreiber nicht immer direkt bestimmt werden kann. Gemäß § 3 Abs. 1 BDSG liegt auch dann ein personenbezogenes Datum vor, wenn die Person bestimmbar ist. Dies ist immer dann der Fall, wenn sich zur Identität des Betroffenen, in diesem Fall also zur Identität des Betreibers, ein Bezug herstellen lässt, indem entsprechendes Zusatzwissen verknüpft wird[448].

Auf privaten Webseiten, die in den Anfängen des Internet-Zeitalters eher einfachen, visuell unkoordinierten Sammlungen einiger weniger Daten glichen und sich zusehends unter Ausschöpfung der angebotenen Hard- und Software zu wahren virtuellen Kunstwerken entwickelt haben, sind oftmals sogar noch wesentlich mehr personenbezogene Daten der Betroffenen zu finden. So werden auf diesen Webseiten häufig genaue Angaben zu Adresse, E-Mail-Adresse, Personenstand, Hobbies und sonstigen privaten Daten gemacht.

Da sich mittlerweile für eine stetig wachsende Masse an Menschen ein erheblicher Teil des Daseins in einer virtuellen Welt abspielt beziehungsweise reale Freundschaften oder berufliche Kontakte hauptsächlich über das Internet gehalten werden, bieten sich dem Datensuchenden fast unendliche Möglichkeiten zur Erhebung selbst intimster Daten. Sogenannte Communities bzw. Soziale Netzwerke, wie beispielsweise StudiVZ, Facebook oder Xing, entblößen den einzelnen Menschen und machen diesen, im Regelfall auf seinen eigenen Wunsch und selbst gesteuert, zum annähernd gläsernen Menschen. Teilweise muss man beim Betrachten dieser Sozialen Netzwerke den Eindruck gewinnen, dass die Betroffenen, auch wenn man in diesem Zusammenhang diese Menschen kaum noch als Betroffene im eigentlichen Wortsinn bezeichnen möchte, ein regelrechtes Mitteilungsbedürfnis bezüglich ihrer personenbezogenen Daten haben[449].

Noch weitergehend sind in vielen Fällen die sogenannten Blogs, also Tagebücher, die im Internet geführt werden und der Allgemeinheit zugänglich sind. In diesen Blogs schildern die Autoren gewöhnlich ihre Erlebnisse, Gefühle oder Ansichten politischer oder sonstiger Natur. Dabei beschränken sich die Betreiber der Blogs, die sogenannten Blogger, zumeist auf ein bestimmtes Thema, wie beispielsweise Mode, Ereignisse in einer bestimmten Stadt oder aber auch die rechtlichen Entwicklungen[450].

448 Vgl. *Dammann*, in: Simitis, BDSG, 6. Aufl., 2006, § 3, Rdnr. 22 ff.; *Schwenke*, Individualisierung und Datenschutz, 2006, S. 97.

449 *Mark Zuckerberg*, der Begründer von Facebook, hat dies zutreffend so formuliert: „Die Menschen fühlen sich wohl dabei, Informationen über sich offener an viele Menschen weiterzugeben." Siehe dazu *Hoeren*, ZRP 2010, 251, 252.

450 So berichtet beispielsweise der Düsseldorfer Rechtsanwalt *Udo Vetter* unter *http://www.lawblog.de/* über aktuelle rechtliche Entwicklungen, persönliche Erlebnisse, Kuriositäten etc. Siehe weiterführend zu Blogs *Kaufmann*, Weblogs – Rechtliche Analyse einer neuen Kommunikationsform, 2009.

Eine weitere wesentliche Nutzung des Internet sind die Diskussions- und Kommunikationsforen, wie beispielsweise Chats oder Newsgroups. Im Unterschied zu den oben genannten Sozialen Netzwerken kommunizieren die Teilnehmer in Kommunikations- oder Diskussionsforen zumeist nicht unter ihren wirklichen Namen, sondern sie benutzen sogenannte Nicknames, also Pseudonyme. Auch in diesen Chats oder Newsgroups können personenbezogene Daten offenbart werden. In vielen Fällen baut sich über Jahre eine virtuelle Gemeinschaft auf, die sich über alle Themen unterhält, die die Teilnehmer beschäftigen. Teilweise kennen sich die Teilnehmer im realen Leben und können dadurch einen noch stärkeren Personenbezug herstellen.

Zudem sind unzählige Fälle bekannt, in denen ein vermeintlich anonymer Teilnehmer durch seine Beiträge im Chat, die Mosaikstein für Mosaikstein von einem oder mehreren anderen Teilnehmern des Chats zusammengetragen wurden, „enttarnt" und damit die natürliche Person hinter dem Pseudonym erkannt wurde. Durch ein Zusammenfügen der in den einzelnen Beiträgen enthaltenen Informationen konnte so ein konkreter Personenbezug hergestellt werden. Da aber auch regelmäßig für die Teilnahme an Chats oder Newsgroups bei den Anbietern dieser Dienste personenbezogene Daten wie Name oder E-Mail-Adresse hinterlegt werden müssen, kann anhand dieser Daten zumeist ein Personenbezug hergestellt werden. Durch die Speicherung der IP-Adresse besteht außerdem später die Möglichkeit, den für einen Beitrag genutzten Rechner zu identifizieren.

Der Schutzumfang des Rechts auf informationelle Selbstbestimmung wird nicht lediglich auf zwangsweise oder heimliche Datenerhebungen und Datenverarbeitungen beschränkt[451]. Aulehner will den Schutzbereich dahingehend einschränken und begründet dies damit, dass ein „Individuum für seine Selbstverwirklichung und Selbstdarstellung auf Fremdwahrnehmung angewiesen" sei[452]. Wenn ein Betroffener daher freiwillig in eine staatliche Datenerhebung einwillige, berühre dies das Recht auf informationelle Selbstbestimmung nicht[453]. Auch Bull vertritt die Ansicht, dass freiwillig veröffentlichte Daten nicht durch das Selbstbestimmungsprinzip geschützt seien[454]. Diese Ansichten verkennen jedoch, dass für den Schutzbereich des Rechts auf informationelle Selbstbestimmung gerade die mögliche Verwendung und nicht die Art oder der Inhalt eines Datums relevant ist[455]. Die Einwilligung in eine Datenerhebung betrifft nicht die Schutzbereichsebene,

451 So aber *Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, 1998, S. 450 ff.
452 *Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, 1998, S. 450.
453 *Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, 1998, S. 451.
454 Vgl. *Bull*, NVwZ 2011, 257, 258.
455 Vgl. bereits BVerfGE 65, 1 ff.

sondern ist für die Eingriffs- oder Rechtfertigungsebene relevant[456]. Einer Ansicht, die für Daten im Internet eine Begrenzung vornimmt, indem der Grundrechtsschutz von vornherein „auf das soziale Umfeld des Grundrechtsträgers ausgerichtet" sein soll, um „grundrechtstypische Gefährdungslagen benennen und abgrenzen zu können", oder die „besondere Sensibilität bestimmter Informationen" fordert[457], kann daher nicht gefolgt werden. Auch offen zugängliche oder mit Einwilligung des Betroffenen veröffentlichte Daten im Internet werden vom Schutzbereich umfasst.

Soweit offen zugängliche Daten nicht vom Schutzbereich umfasst würden, dürften staatliche Stellen diese unbegrenzt erheben. Dadurch bestünde die Gefahr, dass die Behörde die allgemein zugänglichen Daten gezielt zusammenträgt, speichert und gegebenenfalls unter Hinzuziehung weiterer Daten auswertet und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt. Genau vor dieser Gefahr soll aber, wie das Bundesverfassungsgericht zutreffend feststellt, das Recht auf informationelle Selbstbestimmung schützen[458]. Da für den Schutzbereich des Rechts auf informationelle Selbstbestimmung gerade die mögliche Verwendung und nicht die Art oder der Inhalt eines Datums relevant ist, sind damit weder allgemein zugängliche noch offenkundige Daten auszuschließen.

Im Ergebnis werden damit alle Daten im Internet mit direktem oder zumindest herstellbarem Personenbezug durch das Recht auf informationelle Selbstbestimmung geschützt[459]. Dabei umfasst der Schutzbereich den gesamten Datenverarbeitungsprozess, also von der Erhebung bis zur Löschung der Daten[460].

2.3 Eingriff

Da oben festgestellt wurde, dass alle personenbezogenen Daten im Internet durch das Recht auf informationelle Selbstbestimmung geschützt werden, ist im Folgenden zu prüfen, durch welche Ermittlungsmaßnahmen der Polizeibehörden im virtuellen Raum ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt bzw. vorliegen kann.

Ein Eingriff in den genannten Schutzbereich liegt zunächst vor, wenn der Staat den Einzelnen zur Offenbarung konkreter personenbezogener Daten, insbesondere durch die Ausübung von Zwang, verpflichtet[461]. Dass eine sol-

456 Vgl. BVerfGE 120, 274, Absatz 308; 120, 351, 361 ff.; *Germann*, Strafverfolgung im Internet, 2000, S. 471 ff.

457 *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 121 ff.

458 Vgl. BVerfGE 120, 274, Absatz 309.

459 So auch *Germann*, Strafverfolgung im Internet, 2000, S. 474.

460 *Schaar*, Datenschutz im Internet, 2002, S. 47.

461 Vgl. BVerfGE 65, 1, 45; 78, 77, 84.

che Informationsbeschaffung, die auf Willensbeugung beim Betroffenen gerichtet ist, einen Grundrechtseingriff darstellt, dürfte offensichtlich sein.

Allerdings greift nicht nur eine zwangsweise Datenerhebung in das Recht auf informationelle Selbstbestimmung ein[462], sondern der Schutz durch dieses Grundrecht ist erheblich weiter zu fassen. Durch die moderne Informationstechnologie und die damit einhergehenden automatisierten Verarbeitungs- und Verknüpfungsmöglichkeiten kann jedes personenbezogene Datum grundrechtlich bedeutsam werden, weshalb nicht nur eine zwangsweise Datenerhebung einen Grundrechtseingriff darstellt, sondern grundsätzlich überschreitet jeder Akt der Informationserhebung oder -verarbeitung durch eine Behörde, der nicht durch eine freiwillig erteilte Einwilligung legitimiert ist, die Eingriffsschwelle[463]. Nach dem modernen Eingriffsbegriff schützen die Grundrechte auch vor mittelbaren beziehungsweise faktischen Eingriffen durch staatliche Maßnahmen, wenn diese in der Zielsetzung und in ihren Wirkungen klassischen Eingriffen gleichkommen[464]. Damit schützt das Recht auf informationelle Selbstbestimmung in diesem weiten Sinne über den durch die Kriterien der Unmittelbarkeit und Finalität geprägten klassischen Eingriffsbegriff hinaus vor jeder Form der Erhebung, schlichter Kenntnisnahme, Speicherung, Verwendung, Weitergabe oder Veröffentlichung von persönlichen Daten[465]. Insoweit kommt es auch nicht darauf an, dass sich eine Maßnahme gezielt gegen einen Betroffenen richtet oder dieser davon weiß[466].

Als erste entscheidende Schwelle zum Eingriff in das Recht auf informationelle Selbstbestimmung, insbesondere auch für die verdachtsunabhängigen Ermittlungen der Polizei im Internet, ist die Datenerhebung zu sehen, die als Vorphase der weiteren Verarbeitung zu sehen ist[467]. Die Datenerhebung wird als aktive Beschaffung von personenbezogenen Daten über den Betroffenen definiert. Übertragen auf die Ermittlungen der Polizei im Internet würde dies bedeuten, dass nach dieser weiten Eingriffsdefinition bei jeder bewussten Beschaffung personenbezogener Daten aus dem Internet in

462 So aber *Deutsch*, Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, 1992, S. 71 ff.; *v. Hippel/Weiß*, JR 1992, 319, 323.

463 Vgl. BVerfGE 78, 77, 84 ff.; *Petri*, in: Lisken/Denninger, HbPolR, 5. Aufl., 2012, Kap. G, Rdnr. 21 m. w. N.

464 Heute ist unbestritten, dass sich der Grundrechtsschutz nicht auf „klassische" Grundrechtseingriffe (geprägt durch Finalität, Unmittelbarkeit, Rechtswirkung, Anordnung und Durchsetzung) beschränkt, sondern auch Fälle faktischer und/oder mittelbarer Beeinträchtigungen erfasst. Vgl. dazu BVerfGE 105, 279, 303; 110, 177, 191; 113, 63, 76; 116, 202, 222; *Jarass*, in: Jarass/Pieroth, Grundgesetz, 12. Aufl., 2012, Vorb. vor Art. 1, Rdnr. 28 ff.; *Sachs*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Vor Art. 1, Rdnr. 83 ff. m. w. N.

465 *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 176 m. w. N.

466 *Schoch*, Jura 2008, 352, 356.

467 Siehe allgemein dazu *Gola/Schomerus*, BDSG, 11. Aufl., 2012, § 3, Rdnr. 24; *Rogall*, Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht, 1992, S. 49 ff. sowie S. 87 ff.

das Recht auf informationelle Selbstbestimmung eingegriffen würde. Damit würde also der einfache Abruf einer Webseite durch die Polizei bereits regelmäßig einen Eingriff darstellen, da grundsätzlich alle personenbezogenen Daten im Internet vor dem Informationseingriff geschützt werden. Ein Eingriff in das Recht auf informationelle Selbstbestimmung bedarf aber, wie sich aus Art. 2 Abs. 1 GG ergibt, einer verfassungsgemäßen gesetzlichen Grundlage, die nach der Rechtsprechung des Bundesverfassungsgerichts den Geboten der Bestimmtheit und der Normenklarheit auch im Hinblick auf die spezifische grundrechtliche Gefährdungslage entspricht und den Grundsatz der Verhältnismäßigkeit wahrt[468]. Außerdem ist der Zweck der Informationserhebung präzise zu bestimmen, die Informationsverwendung ist auf das zur Erreichung des Gesetzeszwecks Erforderliche zu begrenzen und der Eingriff muss durch Organisations- und Verfahrensregelungen, wie beispielsweise Löschungs- oder Mitteilungspflichten, auf das gebotene Mindestmaß beschränkt werden[469]. Diese strengen Anforderungen an die Ermächtigungsnormen müssten also bei jedem Eingriff zur Rechtfertigung erfüllt werden. Da allerdings die staatlichen Organe bei der Erfüllung der ihnen obliegenden legislativen, exekutiven und judikativen Aufgaben in großem Maße auf personenbezogene Daten angewiesen sind, ist dieser uferlose Eingriffstatbestand einzuschränken.

2.3.1 Eingrenzung des Eingriffsbegriffs

Die modernen staatlichen Bedürfnisse der Datenerhebung und -verarbeitung im Internet erfordern eine Beschränkung des Eingriffsbegriffs. Zur Eingrenzung des uferlosen Eingriffstatbestands werden dabei unterschiedliche Lösungsansätze vertreten[470].

2.3.1.1 Eingrenzung über die Unüberschaubarkeit des Verwendungszwecks

Nach Ansicht des Bundesverfassungsgerichts im Volkszählungsurteil sollte dem Bürger zur freien Entfaltung seiner Persönlichkeit das Recht gegeben werden, den Umgang mit seinen personenbezogenen Daten überschauen zu können[471]. Daran anknüpfend konstruiert Germann zur Eingrenzung des Eingriffsbegriffs einen Lösungsansatz, der den durch den Betroffenen überschaubaren Verwendungszweck eines Datums in den Mittelpunkt der Konturierung des Eingriffsmerkmals rückt[472]. Die Eingriffsschwelle solle dort

468 Vgl. BVerfGE 65, 1, 44; BVerfGE 115, 320, 344 ff.

469 BVerfGE 113, 29, 57 ff.; *Zippelius/Würtenberger*, Deutsches Staatsrecht, 32. Aufl., 2008, § 21, Rdnr. 37.

470 Vgl. allgemein zur Eingrenzung des Eingriffsbegriffs bei der Grundrechtsprüfung die verschiedenen Ansätze in Literatur und Rechtsprechung bei *v. Arnauld*, Die Freiheitsrechte und ihre Schranken, 1999, S. 93 ff.

471 Vgl. BVerfGE 65, 1, 42 ff.

472 *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 489 ff.

angesiedelt werden, wo die Behörde bei der Erhebung und Verwendung personenbezogener Daten den Kreis der konkret überschaubaren Verwendungszwecke überschreite, also den Umgang mit personenbezogenen Daten von denjenigen Zwecken ablöse, die der Betroffene bei Entäußerung der Daten überschauen könne[473]. Eine „Entäußerung der Daten" liegt für den Bereich des Internet beispielsweise dann vor, wenn ein bestimmter Inhalt auf einer Webseite veröffentlicht wird oder in einem Chat ein Beitrag verfasst, abgesendet und für Dritte zugänglich wird. Die „überschaubaren Verwendungszwecke" definiert Germann dahingehend, dass alle Verwendungsmöglichkeiten, mit denen ein Betroffener im Moment der Entäußerung normalerweise zu rechnen habe, umfasst werden sollten. Es sei also jeweils danach zu fragen, für welchen Zweck die zuständige staatliche Stelle, wenn sie das betreffende Datum wahrnehme, dieses Datum zu verwenden Anlass habe[474].

Eine Eingriffsdefinition, die an die Überschaubarkeit des Erhebungszwecks anknüpft, kann allerdings nicht überzeugen, da sie weder eine klare Systematik zur Beschränkung des Eingriffsbegriffs bietet noch den besonderen Anforderungen des Datenschutzes im virtuellen Raum gerecht werden kann. In welchen Fällen ein Betroffener mit einer Verwendung seiner Daten, sei es als Erhebung, Speicherung oder Weitergabe, normalerweise zu rechnen hat, kann nicht allgemeingültig bestimmt werden. So soll nach Germann zum Beispiel durch Recherchen im Internet kein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegen, wenn Register oder Suchmaschinen nach Reizwörtern durchsucht werden. Sobald aber nach Begriffen ausgewertet werde, die keinen selbständigen Indizwert hätten, sondern nur in Kombination mit anderen Erkenntnissen ermittlungsrelevant würden, sei der Erhebungszweck nicht mehr überschaubar und somit ein Eingriff gegeben[475].

An diesem Beispiel wird deutlich, wie unklar und intransparent eine Anknüpfung an die Überschaubarkeit des Erhebungszwecks ist. Letztendlich wird nach dieser Ansicht regelmäßig auf die Umstände des Einzelfalls[476] abgestellt, womit eine systematische Eingriffsbestimmung, die sowohl den staatlichen Stellen als auch den Betroffenen eine eindeutige Rechtslage vorgibt, nicht umsetzbar ist. Bei welchen Ermittlungsmaßnahmen einer Behörde im Internet eine den Eingriff in das Recht auf informationelle Selbstbestimmung rechtfertigende Ermächtigungsgrundlage notwendig wäre, würde also davon abhängen, ob ein Betroffener mit einer

473 *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 489.

474 *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 490.

475 *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 511.

476 So sieht auch *Germann* selbst bei der Bestimmung, ob ein Eingriff vorliegt oder nicht, die Umstände des Einzelfalles als den letzten Ausschlag gebend an, *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 512.

Datenerhebung rechnen musste oder nicht. Eine gebotene Differenzierung, die sich an objektiven Elementen orientiert, ist daher nicht möglich, sondern es wird vielmehr auf die subjektive Sicht der Betroffenen bzw. der Beamten abgestellt. Für eine transparente und methodische Eingrenzung des Eingriffsbegriffs ist die Abhängigkeit von der Unüberschaubarkeit des Verwendungszwecks somit abzulehnen.

2.3.1.2 Eingrenzung über die Zugänglichkeit der Daten

Die Daten im Internet sind zu großen Teilen öffentlich zugänglich, jedoch ist eine nicht zu unterschätzende Datenmenge in passwortgeschützten oder nur unter bestimmten Bedingungen zugänglichen Bereichen gespeichert. Zur Eingrenzung des Eingriffstatbestands wird daher vielfach die Zugänglichkeit der Daten einbezogen. Dabei wird zumeist nicht allein dieses Kriterium als ausreichend angesehen, sondern es werden zur Differenzierung weitere Anknüpfungspunkte angewandt[477].

Zunächst ist zu untersuchen, ob die Zugänglichkeit der Daten ein geeignetes Eingrenzungskriterium zur Einschränkung des andernfalls übersteigerten Schutzes durch das Recht auf informationelle Selbstbestimmung ist. Nach der herrschenden Meinung soll die Erhebung von öffentlich zugänglichen Daten im Internet auf dem technisch dafür vorgesehenen Weg grundsätzlich kein Eingriff in das Recht auf informationelle Selbstbestimmung sein[478]. Dies soll auch ausdrücklich dann gelten, wenn „auf diese Weise im Einzelfall personenbezogene Informationen erhoben werden können“[479]. Zu den öffentlich zugänglichen Bereichen des Internet werden die Webseiten gezählt, die Inhalte „an jedermann oder zumindest einen nicht weiter abgegrenzten Personenkreis“ richten, also beispielsweise allgemein zugängliche

477 Vgl. dazu z. B. BVerfGE 120, 274, Absätze 308 ff.

478 BVerfGE 120, 274, Absatz 308; 120, 351, 361; *Bär*, Auf dem Weg zur „Internet-Polizei“?, in: Bäumler, „Polizei und Datenschutz“ – Neupositionierung im Zeichen der Inforamtionsgesellschaft, 1999, S. 167, 171; *ders.*, MMR 2008, 325, 326; *ders.*, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007, Rdnr. 453 ff.; *ders.*, MMR 1998, 463, 464; *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 544, Fn. 38; *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, BKAG, 2000, § 7, Rdnr. 6; *Bull*, Grundsatzentscheidungen zum Datenschutz bei den Sicherheitsbehörden, in: Möllers/van Ooyen, Bundesverfassungsgericht und Öffentliche Sicherheit, 2011, 65, 68; *Böckenförde*, Die Ermittlung im Netz, 2003, S. 196 ff.; *ders.*, JZ 2008, 925, 935 ff.; *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 133; *Hornung*, CR 2008, 299, 305; *Perrey*, Gefahrenabwehr und Internet, 2003, S. 150 ff.; *Graf*, DRiZ 1999, 281, 285; *Lahrmann*, RdJB 1997, 419 ff.; *Sachs/Krings*, JuS 2008, 481, 482; *Zöller*, GA 2000, 563, 569; *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 176; *Steinle*, Die Polizei 2004, 296, 300; *Jacob*, 17. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz 1997/1998, BT-Drs 14/850, S. 111; *ders.*, 18. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz 1999/2000, BT-Drs 14/5555, S. 105.

479 BVerfGE 120, 274, Absatz 308 m. w. N.

Seiten im World Wide Web, offene Chats und Webforen oder eine jedem Interessierten offenstehende Mailingliste[480].

Die Gegenmeinung unterscheidet für einen Eingriff in das Recht auf informationelle Selbstbestimmung nicht danach, ob Daten im Internet öffentlich zugänglich sind oder nicht[481]. Durch die öffentliche Zugänglichkeit dieser Daten im Internet werde mit der Beschaffung dieser Daten durch die Sicherheitsbehörden der Kreis der Institutionen erweitert, die diese Daten zu nutzen gedenken[482]. Petri hält die Feststellung, dass im Internet frei zugängliche Daten nicht schutzwürdig sind, für bedenklich und in ihren Auswirkungen für nicht überschaubar[483]. Diese Gegenmeinung scheint auf den ersten Blick in der Rechtsprechung des Bundesverfassungsgerichts Rückhalt zu finden, da das Bundesverfassungsgericht in aktuellen Entscheidungen im „realen" beziehungsweise „analogen" Bereich, also außerhalb des Internet, durchaus einen Eingriff in das Recht auf virtuelle Selbstbestimmung auch in den Fällen bejaht hat, in denen Daten aus öffentlich zugänglichen Quellen erhoben werden[484].

In seinem Beschluss zur Videoüberwachung öffentlicher Plätze führt das Bundesverfassungsgericht aus, dass ein Eingriff in das Recht auf informationelle Selbstbestimmung nicht dadurch entfalle, dass lediglich Verhaltensweisen im öffentlichen Raum erhoben würden, da das allgemeine Persönlichkeitsrecht in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen des Einzelnen, der sich in die Öffentlichkeit begebe, Rechnung trage[485]. Bereits in der mit einer Videoaufnahme verbundenen Bildübertragung und der dadurch herbeigeführten Beobachtungsmöglichkeit, sogenanntes Kamera-Monitor-Prinzip mit der Möglichkeit zu Zoom-, Standbild- und Einzelbildaufnahmen, ist eine inten-

480 BVerfGE 120, 274, Absatz 308; siehe zur Abgrenzung von öffentlich zugänglichen und nicht öffentlich zugänglichen Bereichen des Internet *Henrichs*, Kriminalistik 2011, 622 ff.

481 *Petri*, in: Lisken/Denninger, HbPolR, 4. Aufl., 2007, Kap. H, Rdnr. 19, 154; *ders.*, DuD 2010, 25, 27; *ders.*, DuD 2008, 443, 447 ff.; *Schulz/Hoffmann*, CR 2010, 131, 132 ff.

482 *Petri*, in: Lisken/Denninger, HbPolR, 4. Aufl., 2007, Kap. H, Rdnr. 19.

483 *Petri*, DuD 2010, 25, 27; *ders.*, DuD 2008, 443, 447 ff.

484 Vgl. insbesondere BVerfGE 120, 378, 398 ff.; BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23.02.2007 – 1 BvR 2368/06 –, NVwZ 2007, 688, 690; *Horn*, in: Stern/Becker, Grundgesetz, 2010, Art. 2, Rdnr. 50.

485 BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23.02.2007 – 1 BvR 2368/06 –, NVwZ 2007, 688, 690. Vgl. auch zur Videoüberwachung *Siegel*, VerwArch 2011, 159 ff.; *Röll/Brink*, LKRZ 2011, 330 ff.; *Röll/Brink*, LKRZ 2011, 373 ff.; *Brink/Völler*, LKRZ 2011, 201 ff.; *Schnabel*, NVwZ 2010, 1457 ff.; *Hornung/Desoi*, K&R 2011, 153 ff.; *Krist*, LKRZ 2011, 171 ff.; *Assall/Steinke*, FoR 2008, S. 58 ff.; *Bausch*, Videoüberwachung als Mittel der präventiven Kriminalitätsbekämpfung in Deutschland und in Frankreich, 2004, insbesondere S. 25 ff.; *Bartsch*, Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen öffentlich zugänglicher Orte in Deutschland und den USA, 2004, insbesondere S. 90 ff.; *Geiger*, Verfassungsfragen, 1994; *Büllesfeld*, Videoüberwachung, 2002; *Zöller*, NVwZ 2005, 1235 ff.

sivere Beobachtung als eine polizeiliche Beobachtung ohne den Einsatz technischer Mittel möglich und somit ein Eingriff in das Recht auf informationelle Selbstbestimmung gegeben[486]. Die der Polizei bei der Videoüberwachung zur Verfügung stehenden besonderen technischen Mittel mit ihren über die allgemeinen menschlichen Funktionen zur Beobachtung hinausgehenden Funktionen intensivieren damit die Maßnahme und führen zu einem Eingriff, während die bloße Streifenfahrt oder der Streifengang der Polizisten nach allgemeiner Ansicht nicht als Eingriffe zu klassifizieren sind[487].

Das Urteil des Bundesverfassungsgerichts zur automatisierten Erfassung von Kraftfahrzeugkennzeichen zwecks Abgleich mit dem Fahndungstatbestand argumentiert in ähnlicher Weise. Danach entfalle der grundrechtliche Schutz nicht schon deshalb, weil die betroffene Information öffentlich zugänglich sei[488], sondern das Recht auf informationelle Selbstbestimmung schütze auch dann, wenn der Einzelne sich in die Öffentlichkeit begebe, dessen Interesse, dass die damit verbundenen personenbezogenen Informationen nicht im Zuge automatisierter Informationserhebung zur Speicherung mit der Möglichkeit der Weiterverwertung erfasst würden[489]. Auch für diese Kennzeichenerfassung nutzen die Behörden besondere technische Mittel, die die Maßnahme intensivieren und im Vergleich zu den gewöhnlichen menschlichen Funktionen zur Beobachtung der Kennzeichen die Persönlichkeitsgefährdung verstärken.

In beiden Entscheidungen betont das Bundesverfassungsgericht also, dass der Schutz durch das Recht auf informationelle Selbstbestimmung nicht allein deshalb entfalle, weil die Daten öffentlich zugänglich seien. Im Umkehrschluss bedeutet dies allerdings nicht, dass alle öffentlich zugänglichen Daten umfassend und ausnahmslos durch dieses Grundrecht geschützt werden und jede Erhebung personenbezogener Daten einen Eingriff darstellt[490]. Durch das Recht auf informationelle Selbstbestimmung soll der Ein-

486 *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 186; *Bartsch*, Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen öffentlich zugänglicher Orte in Deutschland und den USA, 2004, insbesondere S. 92; *Fetzer/Zöller*, NVwZ 2007, 775, 776 ff.; *Roggan*, NVwZ 2001, 134, 136; *Zöller*, NVwZ 2005, 1235, 1238; a. A. *Dolderer*, NVwZ 2001, 130, 131; *VG Karlsruhe*, NVwZ 2002, 117.

487 *Gusy*, Polizei- und Ordnungsrecht, 7. Aufl., 2009, Rdnr. 165; *Bull*, NJW 2009, 3279, 3282; *ders.*, Informationelle Selbstbestimmung – Vision oder Illusion?, 2009, S. 90.

488 Für Kraftfahrzeugkennzeichen ist die öffentliche Zugänglichkeit zur Identifizierung sogar ausdrücklich in § 23 Abs. 1 Satz 3 StVO vorgeschrieben.

489 BVerfGE 120, 378, 399: Das Bundesverfassungsgericht verneint allerdings dann einen Eingriff in das Recht auf informationelle Selbstbestimmung, wenn nach einer unverzüglich erfolgten Abgleichung kein Treffer zu verzeichnen ist und das Kennzeichen daher sofort und spurlos gelöscht wird. Vgl. insgesamt dazu auch *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 213d.

490 Dies bestätigt sich gerade auch in BVerfGE 120, 274, Absatz 308.

zelne vor der staatlichen Informationsmacht abgeschirmt werden. Durch dieses Recht wird jedoch keine generelle prima-facie-Pflicht staatlicher Stellen begründet, sich blind zu stellen und vor den Datenmengen des Internet zu verschließen[491]. Eine Person, die sich auf öffentlichen Straßen bewegt und damit einen bestimmten Lebenssachverhalt offenbart, hat keinen Anspruch, dabei unerkannt zu bleiben[492]. Es darf dem Staat nicht verwehrt werden, innerhalb bestimmter Grenzen die allgemein verfügbaren Daten im Internet auf dem technisch dafür vorgesehenen Weg, ebenso wie jeder beliebige Dritte, zur Kenntnis zu nehmen[493]. Der Staat benötigt zur angemessenen, sparsamen und wirksamen Erfüllung seiner verfassungsgemäßen Aufgaben Daten in erheblichem Umfang[494]. Soweit ein Polizeibeamter im „analogen" Leben eine Zeitung liest oder einen Streifengang unternimmt, wird man darin keinen Eingriff sehen können. Im Rahmen der Polizeistreifen im Internet setzen die staatlichen Stellen auch nur diejenigen technischen Mittel, wie beispielsweise Computer ein, die jeder Dritte nutzt beziehungsweise nutzen kann.

Wenn ein öffentlich zugänglicher Chat oder ein Webforum überwacht wird, also ohne eine staatliche Kommunikationsbeteiligung die Dialoge oder Kommentare gelesen werden, kann darin noch kein Eingriff liegen. Im „analogen" Leben wäre eine solche Kommunikation vergleichbar mit an einem schwarzen Brett ausgehängten Papierblättern, die den Text enthielten und jedem Interessierten, also auch einem Polizeibeamten, zur Lektüre bereit stünden. Im Ergebnis liegt daher grundsätzlich kein Eingriff in das Recht auf informationelle Selbstbestimmung vor, wenn staatliche Stellen auf dem technisch dafür vorgesehenen Weg öffentlich zugängliche (personenbezogene) Daten im Internet unter Einhaltung bestimmter Grenzen, auf die später genauer eingegangen wird, erheben.

---

491 Vgl. *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 133.

492 *Bull*, NJW 2009, 3279, 3282. Bull sieht sogar durch die „Weite und Unbestimmtheit des Begriffs der informationellen Selbstbestimmung bei den Bürgern Erwartungen entstehen, die nicht erfüllt werden können – weil sie nämlich mit den gerechtfertigten Erwartungen anderer oder der Allgemeinheit kollidieren", *Bull*, NJW 2009, 3279, 3282.

493 Vgl. *Perrey*, Gefahrenabwehr und Internet, 2003, S. 147 m. w. N.; auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit *Schaar* hat in seinem 21. Tätigkeitsbericht (2005/2006) gegen verdachtsunabhängige Ermittlungen der Polizeibehörden im Internet keine grundsätzlichen Bedenken, „soweit dabei in frei zugänglichen, aber gleichwohl einschlägigen Bereichen des Internets ‚gesurft' wird", S. 67 des Tätigkeitsberichts.

494 *Starck*, in: v. Mangoldt/Klein/Starck, Grundgesetz, Bd. 1, 6. Aufl., 2010, Art. 2 Abs. 1, Rdnr. 119. *Starck* will zur Vermeidung übertriebener Datenschutzforderungen folgende Kontrollfragen stellen: „Kenne ich einen weniger belastenden, ebenso wirksamen Weg der notwendigen Tatsachenerhebung und Prognose? Gibt es gute Gründe für den Verzicht auf Staatsaufgaben, die Datenhunger erzeugen?".

Zur grundrechtsdogmatischen Begründung der Eingrenzung über die Zugänglichkeit der Daten können unterschiedliche Lösungsansätze vertreten werden[495].

2.3.1.2.1 Lösung über eine Geringfügigkeitsgrenze

Zunächst könnte man der Ansicht sein, dass die Grundrechte einer allgemeinen Geringfügigkeitsgrenze für Grundrechtsbeeinträchtigungen unterlägen und somit Belästigungen, bloße Bagatelleingriffe und geringfügige Beeinträchtigungen nicht vom Grundrechtsschutz umfasst würden[496]. Für das allgemeine Persönlichkeitsrecht, insbesondere in seiner Ausgestaltung als Recht auf informationelle Selbstbestimmung, ist der Ruf nach einer Erheblichkeitsschwelle durchaus aufgekommen[497]. Danach wäre also eine gewisse Intensität der Grundrechtsbeeinträchtigung notwendig, die bei einer Datenerhebung auf einer öffentlich zugänglichen Webseite im Internet noch nicht gegeben sein könnte.

Für das Recht auf informationelle Selbstbestimmung kann diese Ansicht nicht überzeugen, da die Intensität der Beeinträchtigung dieses Grundrechts gerade nicht relevant sein soll bei der Entscheidung, ob ein rechtfertigungsbedürftiger Eingriff vorliegt oder nicht. Nach der Rechtsprechung des Bundesverfassungsgerichts soll kein Datum belanglos sein und durch die automatisierten Verarbeitungs- und Verknüpfungsmöglichkeiten kann jedes personenbezogene Datum grundrechtlich bedeutsam werden, weshalb jeder Akt der Informationserhebung oder -verarbeitung die Eingriffsschwelle überschreitet, soweit keine Einwilligung vorliegt[498]. Grundrechtsdogmatisch würde also ein Lösungsansatz über eine Geringfügigkeitsgrenze an den Grundfesten des Rechts auf informationelle Selbstbestimmung rütteln. Zudem dürfte es faktisch kaum möglich sein, klare Konturen für eine rechtliche Bewertung zu ermitteln, in welchen Fällen nun ein rechtfertigungsbedürftiger Eingriff vorläge oder aber nur ein schutzloser Bagatelleingriff gegeben wäre. Die Konkretisierung einer solchen Schwelle würde auch deshalb schwerfallen, da es sich regelmäßig um eine einzelfallbezogene Tatsachenfrage handeln würde, die dabei von der subjektiven Konstitution des Grundrechtsträgers abhinge, ob und inwieweit eine staatliche Maßnahme die Per-

495 Siehe insgesamt dazu *Schulz/Hoffmann*, CR 2010, 131, 134 ff.

496 Vgl. *Eckhoff*, Der Grundrechtseingriff, 1992, S. 255 ff.; *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, HStR V, 2. Aufl., 2000, § 111, Rdnr. 65 m. w. N. So soll etwa bei bloßen Bagatellen, alltäglichen Lästigkeiten und subjektiven Empfindlichkeiten noch nicht von einem Eingriff zu reden sein, vgl. *Pieroth/Schlink*, Grundrechte, 26. Aufl., 2010, Rdnr. 260 ff.; a. A. *Sachs*, in: Stern, Staatsrecht III/2, 1994, S. 204 ff.

497 Vgl. *Kloepfer*, Verfassungsrecht II, 2010, § 56, Rdnr. 82.

498 Vgl. BVerfGE 65, 1, 45; 78, 77, 84 ff.

sönlichkeitsentfaltung hemmen würde[499]. Somit ist eine Geringfügigkeitsgrenze als dogmatische Begründung ungeeignet[500].

2.3.1.2.2 Lösung über eine Unterteilung in öffentliche und private Sphären
Ein anderer Lösungsansatz unterteilt den virtuellen Raum in eine öffentliche und eine private Sphäre[501]. Danach soll sich bei der Suche nach Informationen im Internet die Schwelle für einen Eingriff in das Recht auf informationelle Selbstbestimmung anhand der Unterscheidung einer geschützten Privatsphäre und einer grundsätzlich ungeschützten Öffentlichkeitssphäre bestimmen lassen[502]. An diesem Punkt ist bereits anzumerken, dass die Begriffe „Öffentlichkeitssphäre" und „Privatsphäre" missverständlich sein können. Während es im „analogen" Leben zweifelsohne eine öffentliche Sphäre beziehungsweise öffentliche Räume gibt, wie beispielsweise Straßen oder öffentliche Plätze, wird man dies für den Bereich des Internet negieren müssen, da die Webseiten, auf denen insbesondere die Polizeistreifen im Internet surfen, regelmäßig privat betrieben werden[503].

Für eine Unterscheidung der Sphären soll es vielmehr auf den „Verteilungsmodus der Zugangsberechtigung" ankommen[504]. Wenn also beispielsweise für einen passwortgeschützten Chat oder eine passwortgeschützte Newsgroup ein Nutzer nur dann eine Zugangsberechtigung erhält, soweit er persönlich bekannt ist oder einen Ausweis vorgelegt hat, soll es sich um die grundrechtlich geschützte Privatsphäre handeln[505]. Bei keinem individualisierten Verteilungsmodus der Zugangsberechtigung würde hingegen die Öffentlichkeitssphäre vorliegen, die nicht durch das Recht auf informationelle Selbstbestimmung geschützt wird. Diese Ansicht, die in Anlehnung an die „Sphärentheorie" von einem bereichsspezifisch abgestuften Persönlichkeitsschutz ausgeht, sieht Böckenförde sogar ausdrücklich durch das Bundesverfassungsgericht in seinem Urteil zur Internet-Aufklärung und Online-Durchsuchung[506] bestätigt und spricht in diesem Zusammenhang gar von einer „Rehabilitierung der Öffentlichkeitssphäre"[507].

Dem kann allerdings insoweit nicht gefolgt werden und aus dem Urteil des Bundesverfassungsgerichts sind diese weitreichenden Folgen nicht erkennbar. Das Bundesverfassungsgericht hat in seiner Entscheidung lediglich bestimmt, dass eine Kenntnisnahme öffentlich zugänglicher Informationen, also Kommunikationsinhalte, die sich an jedermann oder zumindest an

499 *Kube*, Persönlichkeitsrecht, in: HStR VII, 3. Aufl., 2009, § 148, Rdnr. 81.
500 Im Ergebnis ebenso *Schulz/Hoffmann*, CR 2010, 131, 134 ff.
501 *Böckenförde*, Die Ermittlung im Netz, 2003, S. 170 ff.; *ders.*, JZ 2008, 925, 935 ff.
502 *Böckenförde*, Die Ermittlung im Netz, 2003, S. 184 ff.; *ders.*, JZ 2008, 925, 935.
503 Vgl. *Schulz/Hoffmann*, CR 2010, 131, 134.
504 *Böckenförde*, Die Ermittlung im Netz, 2003, S. 195 ff.
505 Vgl. *Böckenförde*, JZ 2008, 925, 936.
506 BVerfGE 120, 274.
507 *Böckenförde*, JZ 2008, 925, 935.

einen nicht weiter abgegrenzten Personenkreis richten, dem Staat grundsätzlich nicht verwehrt ist[508]. In keiner Weise geht das Bundesverfassungsgericht auf einen nach Sphären abgestuften Persönlichkeitsschutz durch das Recht auf informationelle Selbstbestimmung ein, sondern differenziert vielmehr nach der Schutzwürdigkeit des Vertrauens[509]. Das Bundesverfassungsgericht widerspricht sogar einer strikten Unterteilung in Öffentlichkeits- und Privatsphäre, wenn es zutreffend feststellt, dass ein Eingriff in das Recht auf informationelle Selbstbestimmung gegeben sein kann, „wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt“[510]. Somit kann auch bei Datenerhebungen aus der Öffentlichkeitssphäre ein Eingriff vorliegen.

Problematisch sind bei einer Trennung in Öffentlichkeitssphäre und Privatsphäre auch die Fälle, in denen nicht der Betroffene selbst, sondern ein Dritter die personenbezogenen Daten in der Öffentlichkeitssphäre publiziert. An dieser Stelle verdeutlicht sich, dass eine Begrenzung des Eingriffsbegriffs, die sich ausschließlich an der Zugänglichkeit der Daten orientiert, zu keinen interessengerechten Ergebnissen führen kann. Aus grundrechtsdogmatischer Sicht kann eine Aufteilung in Sphären ebenfalls nicht zufriedenstellen, da die informationelle Selbstbestimmung nicht daten-, sondern verwendungsorientiert ist, was eine Kategorisierung oder Privilegierung bestimmter Arten von Daten ausschließt[511].

2.3.1.2.3 Lösung über (mutmaßliche) Einwilligungen

Eine insbesondere in der Literatur vertretene Ansicht sieht in der Einwilligung beziehungsweise mutmaßlichen Einwilligung der Betroffenen die Begründung dafür, dass öffentlich zugängliche Daten im Internet eingriffslos erhoben werden dürfen[512]. Teilweise wird vertreten, dass auch das Bundesverfassungsgericht sich dieser Einwilligungslösung in seiner Entscheidung zur Internet-Aufklärung und Online-Durchsuchung angeschlossen habe[513].

508 BVerfGE 120, 274, Absatz 308.

509 BVerfGE 120, 274, Absätze 310 ff.

510 BVerfGE 120, 274, Absatz 309; zustimmend *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 133; *Bär*, MMR 2008, 325, 326 ff.; *Hornung*, CR 2008, 299, 305; *Sachs/Krings*, JuS 2008, 481, 482; eher kritisch *Böckenförde*, JZ 2008, 925, 935 ff.

511 *Simitis*, NJW 1984, 394, 402 ff.

512 *Bär*, in: Wabnitz, Handbuch des Wirtschafts- und Steuerstrafrechts, 3. Aufl., 2007, 25. Kap., Rdnr. 98; *ders.*, MMR 1998, 463, 464; *Graf*, DRiZ 1999, 281, 285; *Zöller*, GA 2000, 563, 569; *Kudlich*, JA 2000, 227, 229; ähnlich *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 783.

513 So *Schulz/Hoffmann*, CR 2010, 131, 135.

Das Bundesverfassungsgericht lehnt aber lediglich im Rahmen der Prüfung des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme einen Eingriff in dieses Recht ab, da der Betroffene, wenn er Daten im Internet veröffentliche, für Datenerhebungen durch staatliche Stellen sein System technisch geöffnet habe[514]. Aus dieser technischen Öffnung eine Einwilligung auch für das Recht auf informationelle Selbstbestimmung zu konstruieren, erscheint mehr als bedenklich. Zudem öffnet beispielsweise der Autor eines Eintrags in einem Webforum, also der durch das Recht auf informationelle Selbstbestimmung geschützte Betroffene, nicht sein System im technischen Sinne, wenn er die Nachricht veröffentlichen möchte, sondern der Betreiber des Webforums macht dies, da die Nachricht auf seinem Server gespeichert ist. Die weiteren Ausführungen des Bundesverfassungsgerichts in seiner Entscheidung bieten keine Anhaltspunkte dafür, dass sich das Bundesverfassungsgericht einer Einwilligungslösung anschließen wollte[515].

Die Einwilligungslösung als dogmatischer Lösungsansatz kann zudem nicht überzeugen, da den Betroffenen eine pauschale (mutmaßliche) Einwilligung unterstellt wird. An eine eingriffsausschließende Einwilligung Betroffener sind aber angemessen hohe Anforderungen zu stellen, insbesondere hinsichtlich der Freiwilligkeit und der Einsichtsfähigkeit[516]. Allein aus dem Umstand, dass eine Information in einem öffentlich zugänglichen Bereich des Internet publiziert wird, kann nicht geschlossen werden, dass der Betroffene mit der Kenntnisnahme durch staatliche Stellen einverstanden ist[517]. Gerade in den Sozialen Netzwerken wie StudiVZ oder Facebook, die hauptsächlich privaten Zwecken der Nutzer dienen, wird man, obwohl der Personenkreis der möglichen Betrachter dieser Daten nicht immer überschaubar ist, keine antizipierte Einwilligung der Nutzer in eine staatliche Datenerhebung sehen können. Insbesondere wenn ein Soziales Netzwerk eine bestimmte Nutzergruppe anspricht, wird man eine staatliche Beobachtung, also die Kontrolle durch einen Außenstehenden, nicht wünschen[518].

Wenn also ein öffentlich zugängliches Soziales Netzwerk oder ein Webforum eine Registrierung durch den Nutzer verlangt, bedeutet dies, dass der

514 BVerfGE 120, 274, Absatz 306.

515 Siehe BVerfGE 120, 274, Absätze 307 ff.

516 *Kube*, Persönlichkeitsrecht, in: HStR VII, 3. Aufl., 2009, § 148, Rdnr. 82 m. w. N. Für eine Einwilligung in strafprozessuale Grundrechtsbeeinträchtigungen werden insbesondere an die Einwilligungserklärung hohe Anforderungen gestellt. So soll zwar eine Einwilligung auch konkludent erklärt werden können, jedoch muss das Vorliegen einer wirksamen Einwilligung mit Sicherheit festgestellt werden können, vgl. *Putzhammer*, Die Einwilligung in strafprozessuale Grundrechtsbeeinträchtigungen, 2007, S. 83 ff.

517 Ebenso *Perrey*, Gefahrenabwehr und Internet, 2003, S. 146; *Schulz/Hoffmann*, CR 2010, 131, 135 ff.

518 Vgl. insgesamt dazu *Schulz/Hoffmann*, CR 2010, 131, 135 ff.

Nutzerkreis mit Zugriffsmöglichkeiten nicht unbeschränkt sein soll. Den Betreibern dieser Dienste wird man keine pauschale Einwilligung unterstellen können, da sie, wenn sie beispielsweise als Nutzergruppe Studenten bzw. ehemalige Studenten ansprechen, einer staatlichen Kenntnisnahme nicht indifferent gegenüberstehen. Die Vertraulichkeit des geschlossenen Systems, obwohl es per se für jeden zugänglich ist, wird dabei sogar Teil des Geschäftsmodells des Betreibers sein[519].

An seine Grenzen würde die Einwilligungslösung ferner in den Fällen stoßen, in denen sich Betroffene ausdrücklich gegen eine staatliche Kenntnisnahme wehren würden. Dies könnte beispielsweise so erfolgen, indem auf einer öffentlich zugänglichen Webseite deutlich eine Nachricht erscheinen würde, gemäß der eine Kenntnisnahme durch staatliche Stellen unerwünscht wäre.

Für eine jedem Interessierten offenstehende Newsgroup könnte eine solche Beschränkung zudem ausdrücklich und klar in den Nutzungsbedingungen enthalten sein, die jeder Benutzer bei seiner Registrierung akzeptieren müsste[520]. Soweit eine staatliche Stelle diese Bedingungen missachten würde, könnte sie sich nicht mehr auf eine mutmaßliche Einwilligung der Betroffenen berufen und ein rechtfertigungsbedürftiger Eingriff läge vor.

Dem kann auch nicht entgegengehalten werden, dass ein ausdrücklicher oder geheimer Vorbehalt des Betreibers, keine staatlichen Benutzer zuzulassen, irrelevant sei[521]. In diesem Zusammenhang wird häufig die Parallele zur Rechtsprechung in den sogenannten „Testkäufer"-Fällen herangezogen[522]. In den „Testkäufer"-Fällen wurden in den Geschäftsräumen Schilder mit dem Hinweis aufgehängt, dass Testkäufern das Betreten des Geschäftes verboten sei und diese im Falle der Zuwiderhandlung wegen Hausfriedensbruchs verfolgt würden. Eine Strafbarkeit wegen Hausfriedensbruchs (§ 123 Abs. 1 StGB) der Testkäufer, die in den Geschäften die Einhaltung von Preisbindungen prüfen wollten, wurde abgelehnt, da das Eindringen nicht widerrechtlich erfolgt sei. Durch die vertragliche Befugnis der Herstellerfirmen zur Entsendung von Testkäufern sei keine Widerrechtlichkeit gegeben, da dem Hausrecht der Geschäftsinhaber eine stärkere, dieses brechende Befugnis gegenüberstünde[523].

Die „Testkäufer"-Fälle und der Zugriff auf öffentlich zugängliche Daten im Internet durch staatliche Stellen sind allerdings keineswegs vergleichbar. Während die „Testkäufer"-Fälle die Strafbarkeit einer Privatperson betref-

519 Vgl. *Schulz/Hoffmann*, CR 2010, 131, 136.

520 Vgl. *Schulz/Hoffmann*, CR 2010, 131, 136.

521 So aber *Bär*, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007, Rdnr. 455; *Bär*, in: Wabnitz, Handbuch des Wirtschafts- und Steuerstrafrechts, 3. Aufl., 2007, 25. Kap., Rdnr. 98.

522 Siehe zu den „Testkäufer"-Fällen *Schäfer*, in: MünchKommStGB, Bd. 3, 2012, § 123, Rdnr. 33 m. w. N.

523 Vgl. etwa LG Frankfurt/M., NJW 1963, 1022, 1023.

fen, muss hier die Zulässigkeit staatlichen Handelns, gemessen an den Grundrechten und insbesondere am Recht auf informationelle Selbstbestimmung, untersucht werden. Die staatliche Gewalt ist im Rahmen ihrer Maßnahmen gemäß Art. 1 Abs. 3 GG unmittelbar an die Grundrechte gebunden und kann gerade nicht sämtliche Möglichkeiten privaten Handelns rechtmäßig nutzen[524]. Für Datenerhebungen sind daher Behörden an strengere Regeln gebunden als private Informationsinteressenten[525]. Auch die „Einwilligungstatbestände" sind unterschiedlich. Während die Widerrechtlichkeit für den Hausfriedensbruch aufgrund einer vertraglichen Befugnis trotz eines bestehenden Vorbehalts verneint wird, sind für staatliche Datenerhebungen aus öffentlich zugänglichen Bereichen an die eingriffsausschließende Einwilligung Betroffener angemessen hohe Anforderungen zu stellen. Es kann damit nicht durch eine konstruierte Parallele zu den strafrechtlichen „Testkäufer"-Fällen auf eine Einwilligung insgesamt verzichtet werden oder sogar ein entgegenstehender Wille unberücksichtigt bleiben. Die Einwilligungslösung kann daher nicht zur grundrechtsdogmatischen Begründung, dass öffentlich zugängliche Daten im Internet durch staatliche Stellen eingriffslos erhoben werden dürfen, herangezogen werden.

2.3.1.2.4 Zwischenergebnis

Im Ergebnis kann keiner dieser Lösungsansätze vollumfänglich überzeugen. Um gleichzeitig den Besonderheiten des virtuellen Raumes und den speziellen Anforderungen an das Recht auf informationelle Selbstbestimmung gerecht werden zu können, bedarf es einer differenzierteren Lösung. Im Rahmen dieser Lösung muss berücksichtigt werden, dass zwar grundsätzlich eine Erhebung öffentlich zugänglicher Daten im Internet ohne Eingriff erfolgen darf, jedoch die staatlichen Stellen für diese Datenerhebungen bestimmte Grenzen einhalten müssen. Spätestens bei einem „Exzess" der (verdachtsunabhängigen) Datenerhebung, wenn also öffentlich zugängliche Daten im Internet gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefährdungslage für die Persönlichkeit des Betroffenen ergibt, wird man einen Eingriff in das Recht auf informationelle Selbstbestimmung annehmen müssen[526]. Besonderheiten ergeben sich ferner in

524 Vertiefend dazu *Herdegen*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 1 Abs. 3, Rdnr. 1 ff.; *Hillgruber*, in: Epping/Hillgruber, Grundgesetz, 2009, Art. 1, Rdnr. 60 ff.; *Böckenförde*, Die Ermittlung im Netz, 2003, S. 170 ff.

525 So stellt auch *Bull*, NJW 2009, 3279, 3282, zutreffend fest, dass Behörden strenger als private Informationsinteressenten an rechtliche Regeln zu Datenerhebungen gebunden sind und in den meisten Fällen eine Ermächtigungsgrundlage schon für die Beschaffung von Informationen benötigen.

526 So zutreffend auch BVerfGE 120, 274, Absatz 309.

den Fällen, in denen die staatliche Stelle verdeckt aktiv mit den Betroffenen, beispielsweise in Webforen, kommuniziert.

2.3.1.3 Weiter Eingriffsbegriff und Eingrenzung auf der Rechtfertigungsebene

In der Literatur werden beziehungsweise wurden unterschiedliche Lösungsansätze diskutiert, die erst auf der Ebene der verfassungsrechtlichen Rechtfertigung die Eingriffe in das Recht auf informationelle Selbstbestimmung legitimieren wollen[527]. Diese Ansichten gehen zunächst von einem weiten Eingriffsbegriff aus und beschränken faktisch erst auf der Rechtfertigungsebene den Grundrechtsschutz. Soweit auf der Rechtfertigungsebene einer der Lösungsansätze zu einem überzeugenden und interessengerechten Ergebnis käme, müsste der weite Eingriffstatbestand nicht eingeengt werden. Daher sollen zunächst die Lösungsansätze auf der Rechtfertigungsebene überprüft werden, ob sie im Ergebnis zur Limitierung des Grundrechtsschutzes geeignet sind[528].

Eine frühere Ansicht rechtfertigte nach dem Volkszählungsurteil für eine Übergangszeit die Beibehaltung der alten Rechtslage[529]. Somit sollte die alte Praxis nach dem Volkszählungsurteil bis zum Erlass verfassungsgemäßer Ermächtigungsnormen trotz der durch das Bundesverfassungsgericht verschärften Anforderungen weiterhin zulässig sein[530]. Nach über 25 Jahren seit dem Volkszählungsurteil kann sich eine staatliche Stelle auf diesen Übergangsbonus zweifelsohne nicht mehr berufen[531].

Um auf die Entwicklung des Rechts auf informationelle Selbstbestimmung mit seinen strengen Vorgaben für eine Eingriffsbefugnis zeitnah reagieren zu können, behalfen sich Rechtsprechung und herrschende Lehre

527 Zwar leitet sich das Recht auf informationelle Selbstbestimmung nach h. M. aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG her, jedoch ist das allgemeine Persönlichkeitsrecht und damit auch das Recht auf informationelle Selbstbestimmung den Schranken des Art. 2 Abs. 1 GG unterworfen und nicht, wie die Menschenwürde des Art. 1 Abs. 1 GG, schrankenlos gewährt. Dies ergibt sich insbesondere aus dem Umstand, dass Art. 1 Abs. 1 GG auf die Rolle als Auslegungsmaßstab für die Ermittlung des Inhalts und der Reichweite des Schutzumfangs begrenzt ist. Siehe dazu *Kube*, in: HbStR, Band VII, 3. Aufl., 2009, § 148, Rdnr. 83 ff.; *Murswiek*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 2, Rdnr. 103; *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 133 m. w. N.; a. A. *Tiedemann*, DÖV 2003, 74 ff.

528 Siehe insgesamt dazu mit den verschiedenen Fallgruppen *Germann*, Strafverfolgung im Internet, 2000, S. 478 ff.

529 Siehe zu diesem „Übergangsbonus“ *Simitis*, BDSG, 6. Aufl., 2006, Einleitung, Rdnr. 39 ff. m. w. N.

530 BVerwGE 84, 375; BVerwG, NJW 1990, 2765; siehe zur „Übergangsrechtsprechung“ auch *Herrmann/Lang/Schneider*, Polizeirelevante Grundrechte, 1998, S. 99 ff.

531 So bereits schon *Perschke*, Die Zulässigkeit nicht spezialgesetzlich geregelter Ermittlungsmethoden im Strafverfahren, 1997, S. 136 ff.; *Simitis/Fuckner*, NJW 1990, 2713, 2714; *Wolter*, GA 1988, 49, 83.

zunächst damit, lediglich als Aufgabenzuweisung ausgestaltete Normen zugleich als Ermächtigungsgrundlagen für weniger eingriffsintensive Ermittlungen zu interpretieren (vielfach als „Schwellentheorie“ bezeichnet)[532]. Diese für die §§ 160, 161, 163 StPO a. F. entwickelte Theorie hat allerdings ihre Relevanz durch Inkrafttreten des Strafverfahrensänderungsgesetzes 1999 verloren, da ab diesem Zeitpunkt die betreffenden Vorschriften ausdrücklich als Befugnisgeneralklauseln formuliert wurden[533]. In diesem Zusammenhang bleibt festzuhalten, dass heute eine Aufgabenzuweisungsnorm noch nicht allein einen Eingriff in das Recht auf informationelle Selbstbestimmung rechtfertigen kann, da beispielsweise die als Eingriffsverwaltung gestaltete polizeiliche Tätigkeit stets dem Gesetzesvorbehalt unterliegt[534]. Das System der klaren Trennung zwischen Aufgaben und Befugnissen fordert zum Beispiel für den Einsatz eines polizeilichen Mittels, welches in die Rechtssphäre einer Person eingreift, über die Aufgabenzuweisung hinausgehend eine gesetzliche Befugnis[535]. Eine Datenerhebung, die in das Recht auf informationelle Selbstbestimmung eingreift, darf nicht lediglich auf eine Aufgabenzuweisungsnorm gestützt werden, sondern benötigt eine den strengen Anforderungen des Bundesverfassungsgerichts genügende Ermächtigungsgrundlage[536].

Das Bundesdatenschutzgesetz trifft in § 13 Abs. 1 die allgemeine Regelung, dass das Erheben personenbezogener Daten zulässig ist, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Diese Norm wird teilweise so interpretiert, dass sie eine Auffangermächtigungsgrundlage für sämtliche Datenerhebungen darstelle und bei keiner spezielleren Ermächtigungsgrundlage auf diese Norm zurückgegriffen werden könne[537]. Diese Ansicht verkennt jedoch den Regelungsinhalt des § 13 Abs. 1 BDSG in schwerwiegender Weise[538]. Durch diese Norm soll gerade keine allgemeine Ermächtigung der öffentlichen Stellen zur Datenerhebung erfolgen, sondern die Betroffenen sollen vor der Datenerhebung,

532 Siehe zur „Schwellentheorie“ *Rieß*, in: Löwe-Rosenberg, StPO, 24. Aufl., 1989, § 160, Rdnr. 3 ff. m. w. N. In der Folgeauflage sieht Rieß die „Schwellentheorie“ auf Grund der Reaktion des Gesetzgebers bereits als weitgehend überholt an, *Rieß*, in: Löwe-Rosenberg, StPO, 25. Aufl., 2004, § 160, Rdnr. 3.

533 *Frister*, in: Lisken/Denninger, HbPolR, 5. Aufl., 2012, Kap. F, Rdnr. 114.

534 Vgl. *Kugelmann*, Polizei- und Ordnungsrecht, 2006, S. 181 ff.; *Kube*, in: HbStR, Band VII, 3. Aufl., 2009, § 148, Rdnr. 83 ff.

535 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 161 ff.; *Knemeyer*, Polizei- und Ordnungsrecht, 11. Aufl., 2007, Rdnr. 76 ff.; *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 36 ff.

536 Auch eine Verwaltungsvorschrift kann für sich keinen Eingriff in das Grundrecht der informationellen Selbstbestimmung rechtfertigen, da es einer formell-gesetzlichen Grundlage für solch ein einen Eingriff bedarf, BVerfG, Beschluss vom 11.08.2009, 2 BvR 941/08, Absatz 19.

537 *Kniesel*, Die Polizei 1983, S. 385.

538 Vgl. *Germann*, Strafverfolgung im Internet, 2000, S. 480 ff.

also dem entscheidenden Eingriff in das Recht auf informationelle Selbstbestimmung, geschützt werden, indem gemäß § 13 Abs. 1 BDSG eine Datenerhebung nur dann erfolgen darf, wenn sie zur Aufgabenerfüllung erforderlich ist[539]. Durch § 13 Abs. 1 BDSG wird keine eigenständige Verpflichtung von Betroffenen zur Preisgabe von Daten und ebenso kein Anspruch für öffentliche Stellen auf die zu erhebenden Daten begründet, sondern hierzu können nur spezialgesetzliche Befugnisnormen ermächtigen[540]. Nach der Rechtsprechung des Bundesverfassungsgerichts bedürfen die Einschränkungen des Rechts auf informationelle Selbstbestimmung einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und in der der Verwendungszweck der Daten bereichsspezifisch und präzise bestimmt ist[541]. Eine derart weit gefasste, generalklauselartig formulierte Bestimmung wie § 13 Abs. 1 BDSG würde damit keineswegs den restriktiven Vorgaben des Bundesverfassungsgerichts nach einer bereichsspezifischen und präzisen gesetzlichen Regelung entsprechen[542].

Nach einer aktuellen Ansicht in der Literatur zur staatlichen Beobachtung im Netz wird angenommen, dass in der Internet-Aufklärung in der Regel ein Grundrechtseingriff vorliege[543]. Dieser solle aber durch einen Rückgriff auf die polizeilichen Generalklauseln gerechtfertigt sein, da die Internet-Aufklärung lediglich eine geringe Eingriffsintensität aufweise[544]. Diese Ansicht begegnet starken Bedenken, da sie die strengen Vorgaben des Bundesverfassungsgerichts für die Ermächtigungsnormen staatlicher Eingriffe in das Recht auf informationelle Selbstbestimmung verkennt. Der Rückgriff auf die polizeirechtlichen Generalklauseln kann für die Internet-Aufklärung keine verfassungsgemäße gesetzliche Rechtfertigungsnorm bilden, die nach der Rechtsprechung des Bundesverfassungsgerichts den Geboten der Bestimmtheit und der Normenklarheit im Hinblick auf die spezifische grundrechtliche Gefährdungslage entspricht und den Grundsatz der Verhältnismäßigkeit wahrt[545].

Im Ergebnis kann keiner der oben genannten Lösungsansätze auf der Rechtfertigungsebene ein überzeugendes und interessengerechtes Ergebnis zur Eingrenzung des Schutzes durch das Recht auf informationelle Selbstbe-

539 Vgl. *Sokol*, in: Simitis, BDSG, 6. Aufl., 2006, § 13, Rdnr. 5 ff.

540 Vgl. *Däubler/Klebe/Wedde/Weichert*, BDSG, 3. Aufl., 2010, § 13, Rdnr. 6; *Sokol*, in: Simitis, BDSG, 6. Aufl., 2006, § 13, Rdnr. 7; zumindest Datenerhebungen mit schwerwiegenden Grundrechtseingriffen sollen nicht durch § 13 BDSG gerechtfertigt sein, vgl. *Gola/Schomerus*, BDSG, 11. Aufl., 2012, § 13, Rdnr. 2.

541 Vgl. BVerfGE 65, 1, 44 ff.

542 So auch *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 480 ff.

543 Vgl. *Schulz/Hoffmann*, CR 2010, 131, 136.

544 Vgl. *Schulz/Hoffmann*, CR 2010, 131, 136.

545 Vgl. BVerfGE 65, 1, 44; BVerfGE 115, 320, 344 ff.

stimmung bieten. An dieser Stelle wird nun die eigentliche Problematik des Rechts auf informationelle Selbstbestimmung sichtbar: Einerseits wird durch den allumfassenden Schutzbereich, geprägt durch das Dogma, dass kein Datum belanglos sei, und durch den weiten Eingriffsbegriff ein umfänglicher Schutz der personenbezogenen Daten gewährt[546], der andererseits durch die engen Vorgaben des Bundesverfassungsgerichts für eine verfassungsrechtliche Rechtfertigung der Informationseingriffe nicht in geeigneter und praxisgerechter Weise eingeschränkt werden kann. Auf der Rechtfertigungsebene wird eine bereichsspezifische, den Geboten der Normenklarheit, Bestimmtheit und Verhältnismäßigkeit genügende Befugnisnorm gefordert. Da der Staat bei der Durchführung der ihm obliegenden Aufgaben in großem Umfang auf personenbezogene Daten angewiesen ist, wie beispielsweise bei der Führung der Melderegister[547], bei der Durchführung von Strafverfahren[548] oder insbesondere bei der polizeilichen Tätigkeit zur Gefahrenabwehr und Strafverfolgung[549], müssten bereichsspezifische Detailregelungen durch den Gesetzgeber erlassen werden. Diese Fülle an Gesetzen würde jedoch durch ihre Intransparenz den Bürgern verbieten, das genaue Ausmaß der staatlichen Datenerhebung und -verarbeitung tatsächlich zu erkennen und damit letztendlich den Zweck des Gesetzesvorbehalts vereiteln[550].

Zusätzlich würden die Entfaltungsmöglichkeiten der Grundrechtsträger durch eine Verrechtlichung des Datenschutzes unnötig verengt werden, wenn selbst bei geringsten Gefährdungen des Rechts auf informationelle Selbstbestimmung, ungeachtet der Intensität und der Gewichtigkeit des Missbrauchspotentials und damit des Schutzbedarfs, präzise Ermächtigungsgrundlagen gefordert würden[551]. Damit könnte sich der Datenschutz sogar gegen die geschützten Grundrechtsträger richten, wenn der Gesetzgeber die Erhebung und Verwendung jedweder Daten nicht nur durch Gesetze regeln, sondern diese auch inhaltlich detailliert und damit regelmäßig bevormundend ausgestalten müsste[552].

546 *Bäcker* spricht in diesem Zusammenhang sogar von einem „Totalvorbehalt des Gesetzes“ und einem „unspezifischen Super-Abwehrrecht gegen jeden staatlichen Umgang mit Informationen“, *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 121.

547 Vgl. BVerfG, DVBl 1993, 601; BVerwG, NVwZ 1988, 621; *Mallmann*, NJW 1994, 1687.

548 Vgl. *Rogall*, Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht, S. 71; *Riepl*, Informationelle Selbstbestimmung im Strafverfahren, 1998, S. 34 ff., 107 ff.

549 Vgl. *Son*, Heimliche polizeiliche Eingriffe in das informationelle Selbstbestimmungsrecht, 2006, S. 83 ff.

550 Vgl. *Germann*, Strafverfolgung im Internet, 2000, S. 482.

551 Vgl. *Hoffmann-Riem*, AöR 123 (1998), 513, 528.

552 Vgl. insgesamt dazu *Hoffmann-Riem*, AöR 123 (1998), 513, 528, der in diesem Zusammenhang von einer „Verrechtlichung des Alltäglichen“ spricht.

Gleichfalls würde eine unübersichtliche und überdetaillierte Normenmasse erkennbar die Forderung nach Deregulierung und schlankem Staat konterkarieren[553]. Ein echter rechtsstaatlicher Fortschritt wäre mit dieser Verrechtlichung nicht verbunden[554], sondern eine solche Entwicklung würde sich vielmehr als „Bumerang" für den Datenschutz erweisen[555]. Statt einer „Entbürokratisierung" des Datenschutzrechts, wie beispielsweise Bull sie fordert[556], erhielten Bürger und Exekutive eine intransparente Masse an Gesetzesnormen.

Um die Flut an Ermächtigungsgrundlagen zu verhindern, könnte man die Ansicht vertreten, dass durch einige wenige bereichsübergreifende Generalklauseln eine verfassungsgemäße Rechtfertigung der Eingriffe erreicht werden könnte. Zwar scheiden Generalklauseln nicht per se als Ermächtigungsgrundlagen aus[557], jedoch sind gerade diese an den Vorgaben des Bundesverfassungsgerichts zu messen[558]. Insbesondere müssen die jeweiligen Befugnisnormen dem aus Art. 20 Abs. 3 GG abgeleiteten Bestimmtheitsgebot genügen[559]. Dementsprechend muss eine Ermächtigungsgrundlage in Tatbestand und Rechtsfolge so formuliert sein, dass die von ihr Betroffenen, also neben den Bürgern auch die normanwendenden Behörden, die Rechtslage erkennen und ihr Verhalten danach richten können[560]. Zur Gewährleistung der nötigen Rechtssicherheit muss es dem Bürger ermöglicht werden, Inhalt und Ausmaß des Eingriffs selbst erkennen zu können und sein Verhalten nach der Rechtslage auszurichten[561].

Für das Recht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht ausdrücklich klargestellt, dass eine Einschränkung dieses Grundrechts einer bereichsspezifischen gesetzlichen Befugnisnorm bedürfe, aus der sich Voraussetzungen und Umfang der Beschränkung klar und für

553 *Kloepfer*, NJW 1998, Beilage zu Heft 23, S. 21, 22.

554 So *Schenke*, DVBl 1996, 1393, 1398.

555 *Denninger*, KJ 1985, 215 ff.

556 *Bull*, NJW 2006, 1617. Ähnlich auch *Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, 1998, S. 452, der einen „Schutz gegen diese alltägliche Informationstätigkeit" weder für erforderlich noch für wünschenswert hält. Vielmehr würde dadurch sogar das Gegenteil von informationeller Selbstbestimmung, nämlich „institutionalisierte Kommunikationslosigkeit und monopolisierte Information" bewirkt werden.

557 Vgl. dazu *Krüger*, DÖV 1990, 641 ff.; *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 182 m. w. N.; a. A. *Simitis*, NJW 1984, 394, 400, nach dem „die informationelle Selbstbestimmung den Rückzug in die Generalklauseln versperrt". Relativierend *Simitis* später in BDSG, 6. Aufl., 2006, Einführung, Rdnr. 48 ff.

558 Vgl. dazu *Son*, Heimliche polizeiliche Eingriffe in das informationelle Selbstbestimmungsrecht, 2006, S. 71 ff.

559 Vgl. BVerfGE 86, 288, 311.

560 BVerfGE 87, 234, 263; 84, 133, 149; siehe zur Vereinbarkeit einer Ermächtigungsgrundlage zur Videoüberwachung mit dem Bestimmtheitsgebot *Bausch*, Videoüberwachung als Mittel der präventiven Kriminalitätsbekämpfung in Deutschland und in Frankreich, 2004, S. 45 ff.

561 So bereits schon BVerfGE 8, 274, 325.

den Bürger erkennbar ergeben[562]. Diese Forderung nach präzisen und bereichsspezifischen Datenschutzregelungen stellt sich dabei als eine spezifische verfassungsgerichtliche Antwort auf die Herausforderung durch die moderne Datenverarbeitung dar[563]. Nur durch genaue, bereichsspezifische Normen über einzelne Informationseingriffe können die gebotene Transparenz der Datenverarbeitung und die ihr dienende Normenklarheit gesichert werden[564]. Lediglich ein paar allgemein gehaltene Generalklauseln würden diesen Anforderungen und damit auch dem Schutzbedürfnis der Bürger nicht gerecht werden können. Der staatliche Umgang mit personenbezogenen Daten kann nicht auf bereichsübergreifende Generalklauseln gestützt werden, sondern benötigt eigenständige Spezialvorschriften[565]. Die Rechtfertigung von einer Vielzahl unspezifischer Eingriffe mit unterschiedlicher Intensität durch nur eine beziehungsweise einige wenige Generalklauseln kann nicht den Bestimmtheitsanforderungen genügen. Zudem kann eine Generalklausel auf Grund ihrer begrifflichen Unschärfe regelmäßig nur Maßnahmen rechtfertigen, die nicht tief in den grundrechtlich geschützten Bereich der Bürger eingreifen[566]. Damit können Eingriffe durch verdeckte Maßnahmen zur Datenerhebung der Polizei im Internet, die in ihrer Art und Schwere den sogenannten „besonderen Mitteln“ oder „besonderen Methoden“ der Datenerhebung entsprechen und damit nicht nur leicht in das Recht auf informationelle Selbstbestimmung eingreifen, grundsätzlich nicht durch eine Generalklausel legitimiert werden, sondern es bedarf einer Einzeleingriffsermächtigung[567].

Um einerseits eine überdetaillierte, intransparente Masse an Ermächtigungsgrundlagen zu verhindern und andererseits insbesondere den Bestimmtheitsanforderungen zu genügen, kann eine praxisgerechte Lösung zur Eingrenzung des Schutzes durch das Recht auf informationelle Selbstbestimmung nicht erst auf der Rechtfertigungsebene ansetzen, sondern muss vielmehr bereits den Eingriffsbegriff einschränken[568]. Im Folgenden soll daher versucht werden, eine sowohl rechtsdogmatisch begründete als auch zugleich systematische und praxistaugliche Lösung zur Eingrenzung des Eingriffsbegriffs zu entwickeln.

562 Vgl. BVerfGE 65, 1, 44.

563 *Bäumler*, JR 1984, 361, 363.

564 Vgl. *Bäumler*, JR 1984, 361, 364; *Simitis*, NJW 1984, 394, 400.

565 *Würtenberger/Schenke*, JZ 1999, 548, 549.

566 Vgl. *Hilger*, NStZ 2000, 561, 564.

567 So sieht § 27 Abs. 2 Satz 2 BremPolG sogar eine derartige ausdrückliche Regelung vor. Vgl. auch *Petri*, in: Lisken/Denninger, HbPolR, 5. Aufl., 2012, Kap. G, Rdnr. 170.

568 Im Ergebnis so auch *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 481 ff.

2.3.1.4 Eingrenzung über die Schutzwürdigkeit des kommunikativen Vertrauens

Das Bundesverfassungsgericht wählt in seiner Entscheidung zur Internet-Aufklärung und Online-Durchsuchung einen vielversprechenden Lösungsansatz zur Eingrenzung des Eingriffsbegriffs, der die Schutzwürdigkeit des Vertrauens bei Kommunikationsbeziehungen im Internet in den Mittelpunkt rückt[569]. Daher soll zunächst der Inhalt der Entscheidung des Bundesverfassungsgerichts dargestellt werden.

2.3.1.4.1 Das Urteil des Bundesverfassungsgerichts zur Internet-Aufklärung

Das Bundesverfassungsgericht stellt zu Beginn seiner Ausführungen zu einem möglichen Eingriff in das Recht auf informationelle Selbstbestimmung durch das heimliche staatliche Aufklären des Internet klar, dass eine Kenntnisnahme öffentlich zugänglicher Informationen, auch im Einzelfall personenbezogener Daten, keinen Eingriff darstelle[570].

Ein Eingriff und damit die Notwendigkeit einer Ermächtigungsgrundlage liege aber nach Ansicht des Bundesverfassungsgerichts dann vor, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen werden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergebe[571]. In einer nachfolgenden Entscheidung konkretisiert das Bundesverfassungsgericht diesen möglichen „Datenerhebungsexzess“ noch weiter. Danach sei ein Eingriff in das Recht auf informationelle Selbstbestimmung anzunehmen, wenn die aus öffentlich zugänglichen Quellen stammenden Daten durch ihre systematische Erfassung, Sammlung und Verarbeitung einen zusätzlichen Aussagewert erhielten, aus dem sich die für dieses Grundrecht spezifische Gefährdungslage für die Freiheitsrechte oder die Privatheit des Betroffenen ergebe. So könne es etwa liegen, wenn diese Daten mit anderen Daten verbunden würden, die bereits für sich genommen dem Grundrechtsschutz unterfielen, und dadurch der Aussagegehalt der verknüpften Daten insgesamt zunehme[572].

Für die heimlichen Aufklärungsmaßnahmen im Internet sind jedoch nicht nur die Aufrufe von Webseiten relevant, sondern eine besondere Gefährdungslage der Persönlichkeit der Betroffenen kann durch Kommuni-

569 BVerfGE 120, 274, Absatz 310.

570 BVerfGE 120, 274, Absatz 308.

571 BVerfGE 120, 274, Absatz 309; befürwortend *Sachs/Krings*, JuS 2008, 481, 482; *Bär*, MMR 2008, 325, 326 ff.; *Hornung*, CR 2008, 299, 305; *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 133; *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 784.

572 BVerfGE 120, 351, 361 ff.

kationsbeziehungen zwischen staatlichen Stellen und den Betroffenen entstehen.

Dies hat auch das Bundesverfassungsgericht erkannt und führt dazu aus:

„Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt nicht schon dann vor, wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt, wohl aber, wenn sie dabei ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde (…).

Danach wird die reine Internetaufklärung in aller Regel keinen Grundrechtseingriff bewirken. Die Kommunikationsdienste des Internet ermöglichen in weitem Umfang den Aufbau von Kommunikationsbeziehungen, in deren Rahmen das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner nicht schutzwürdig ist, da hierfür keinerlei Überprüfungsmechanismen bereitstehen. Dies gilt selbst dann, wenn bestimmte Personen – etwa im Rahmen eines Diskussionsforums – über einen längeren Zeitraum an der Kommunikation teilnehmen und sich auf diese Weise eine Art „elektronische Gemeinschaft" gebildet hat. Auch im Rahmen einer solchen Kommunikationsbeziehung ist jedem Teilnehmer bewusst, dass er die Identität seiner Partner nicht kennt oder deren Angaben über sich jedenfalls nicht überprüfen kann. Sein Vertrauen darauf, dass er nicht mit einer staatlichen Stelle kommuniziert, ist in der Folge nicht schutzwürdig."[573]

Damit kann nach Ansicht des Bundesverfassungsgerichts ein Eingriff in das Recht auf informationelle Selbstbestimmung bei aktiver Teilnahme einer staatlichen Stelle an der Internetkommunikation nur dann vorliegen, wenn das schutzwürdige kommunikative Vertrauen eines Betroffenen enttäuscht wurde, um Daten zu erheben, welche die staatliche Stelle ohne diesen Vertrauensbruch nicht erhalten hätte. Die Eingriffsschwelle wird damit für die aktive staatliche Kommunikation im Internet sehr hoch gelegt, da das Bundesverfassungsgericht ein schutzwürdiges Vertrauen des Betroffenen in die Identität und Wahrhaftigkeit seines Kommunikationspartners nur in Ausnahmefällen annimmt.

2.3.1.4.2 Kritik am Urteil des Bundesverfassungsgerichts zur Internet-Aufklärung

Die hoch angesetzte Eingriffsschwelle des Bundesverfassungsgerichts begegnet starken Bedenken. Während die Grundaussagen zu eingriffslosen Erhebungen aus öffentlich zugänglichen Daten mit Ausnahme des „Datenerhebungsexzesses" im Ergebnis überzeugen können, sind die Ausführungen

573 BVerfGE 120, 274, Absätze 310 ff.

zu den nach Ansicht des Bundesverfassungsgerichts in den meisten Fällen eingriffslosen Kommunikationsbeziehungen staatlicher Stellen kritisch aufzunehmen. Für die Kommunikationsbeziehungen staatlicher Stellen wählt das Bundesverfassungsgericht als entscheidendes Kriterium, ob ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt, die Ausnutzung eines schutzwürdigen Vertrauens des Betroffenen in die Identität und die Motivation seines Kommunikationspartners. Selbst in den Fällen, in denen sich über einen längeren Zeitraum eine Art „elektronische Gemeinschaft" zwischen den beteiligten Personen gebildet hat, lehnt das Bundesverfassungsgericht ein schutzwürdiges Vertrauen darauf ab, dass kein Repräsentant einer staatlichen Stelle Teil dieser Gemeinschaft ist[574].

2.3.1.4.2.1 Charakterisierung der Kommunikationsbeziehung

Um die besondere Problematik der aktiven staatlichen Internetkommunikation mit Grundrechtsträgern und die damit zusammenhängende Möglichkeit zur Identitätstäuschung rechtlich umfassend begutachten zu können, sollen zunächst die hierfür relevanten Handlungen der Polizei im Internet genau charakterisiert werden. Sowohl bei den heimlichen Aufklärungsmaßnahmen des Internet, über die das Bundesverfassungsgericht in seinem Urteil zu entscheiden hatte, als auch bei den Polizeistreifen im Internet wird durch die staatliche Stelle neben dem Abruf von Webseiten eine direkte Konversation mit einem oder mehreren Grundrechtsträgern angestrebt. Im Rahmen einer solchen Konversation übernehmen regelmäßig beide beziehungsweise alle Beteiligten alternierend den aktiven Part. Es entsteht also ein Gespräch beziehungsweise Chat, bei dem die Datenflüsse visuell auf den jeweiligen Bildschirmen dargestellt werden. In diesem Gespräch können lediglich zwei Personen miteinander kommunizieren. In der Regel sind aber mehrere Personen bis hin zu einer kaum noch bestimmbaren Anzahl an Kommunikationspartnern beteiligt.

Die Gesprächsthemen in Webforen sind häufig im Titel vorgegeben[575]. Der daran folgende Strang, auch als „Thread" bezeichnet, gibt die einzelnen Beiträge der Beteiligten wieder. Dadurch entwickelt sich, zumindest bei interessanten Themen, eine Diskussion unter den Beteiligten oder die Nutzer berichten über ihre persönlichen Erfahrungen. Im Rahmen dieser Kommunikationsbeziehung kann jeder Nutzer durch seine Textbeiträge aktiv den Gesprächsverlauf mitbestimmen. Häufig beginnen diese Threads mit einem bestimmten Thema und verändern dieses im Laufe der Kommunikation. Dadurch gestaltet jeder Gesprächsbeitrag den Verlauf und das Diskussions-

574 BVerfGE 120, 274, Absatz 311.

575 So ein Titel kann beispielsweise lauten: „Politiker XY beim Fahren unter Alkoholeinfluss erwischt". Häufig sind die Titel aber noch banaler und betreffen private Bereiche oder Hobbies.

thema. In Chats wird oft ohne konkretes Thema, etwa über die Vorkommnisse des Tages etc., miteinander kommuniziert.

2.3.1.4.2.2 Pseudonymisierung

Die Besonderheit bei diesen Kommunikationsbeziehungen im Internet ist, dass in vielen Fällen die Identität des jeweiligen Gesprächspartners nicht bekannt ist, da unter Pseudonymen, den sogenannten Nicknames, kommuniziert wird. Den Nickname kann jeder Nutzer selbst wählen. Häufig spiegeln sich im Nickname bestimmte Informationen des Nutzers wider oder lassen Rückschlüsse auf seine Interessen zu[576]. Welche Person hinter einem Pseudonym auftritt, kann im Regelfall einer der Beteiligten, der über keine besonderen (staatlichen) Befugnisse verfügt, nicht auflösen. Selbst der Anbieter des Dienstes wird nicht immer den wahren Nutzer bestimmen können, da die Nutzer oft nur ihre E-Mail-Adresse zur Registrierung angeben müssen.

2.3.1.4.2.3 Staatliche Identitätstäuschung

Aus diesen mangelnden Überprüfungsmechanismen zieht das Bundesverfassungsgericht den Schluss, dass dadurch die Schutzwürdigkeit des Vertrauens eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner – selbst bei langfristigen Kommunikationsbeziehungen – wegfalle und damit die staatliche Kommunikationsteilnahme unter einer Legende legitimiert werde[577]. Allein aus dieser faktischen Möglichkeit zur Identitätstäuschung darf aber nicht gefolgert werden, dass für eine staatliche Stelle eine Identitätstäuschung rechtlich zulässig ist[578]. Eine staatliche Stelle handelt nämlich bei ihrer Internetkommunikation mit Grundrechtsträgern verdeckt. Das Bundesverfassungsgericht zieht sogar selbst die Parallele zum Einsatz eines Verdeckten Ermittlers[579].

---

576 Bei dem Nickname „Melanie 1984“ liegt zumindest der Schluss nahe, dass die Nutzerin des Nicknames 1984 geboren wurde und weiblich ist. Der Nickname „VW-Fan“ deutet zumindest auf eine gewisse Vorliebe des Nutzers zu Fahrzeugen der Volkswagen AG hin.

577 Vgl. BVerfGE 120, 274, Absätze 310 ff.

578 *Eifert*, NVwZ 2008, 521, 522; Brunst, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 788; *Brunst*, Anonymität im Internet, 2009, S. 246 ff.; *Malek*, Strafsachen im Internet, 2005, S. 108; *Kant*, Bürgerrechte und Polizei/CILIP 71 (1/2002), 29, 35; ähnlich auch *Hornung*, CR 2008, 299, 305, der zumindest bei längeren Kommunikationsbeziehungen die These des Bundesverfassungsgerichts für angreifbar hält. Bereits kritisch *Jacob*, 17. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz 1997/1998, BT-Drs 14/850, S. 111; *ders.*, 18. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz 1999/2000, BT-Drs 14/5555, S. 105.

579 BVerfGE 120, 274, Absatz 310; vgl. auch *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 133; *Valerius*, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, 2004, S. 124 ff.; *Warntjen*, in: Roggan, Online-Durchsuchungen, 2008, S. 65; *Eifert*, NVwZ 2008, 521, 522; *Kudlich*, GA 2011, 193,

Verdeckte Ermittler sind Polizeibeamte, die unter Geheimhaltung ihrer wahren Identität polizeiliche Aufgaben wahrnehmen[580]. Sie werden unter einer Legende, also unter falscher Identität, in Milieus eingeschleust, um sämtliche verwertbaren Informationen weiterzugeben[581]. Der Einsatz eines Verdeckten Ermittlers im „analogen" Bereich wird nach allgemeiner Ansicht als Grundrechtseingriff gewertet[582]. Da Verdeckte Ermittler die Daten nicht offen erheben und sogar über ihre Identität täuschen, bedarf ihr Einsatz einer qualifizierten Gefahrenlage[583].

Bei den im Internet durchgeführten Polizeistreifen wird es sich zwar nicht stets um Verdeckte Ermittler handeln, da sie nicht immer unter einer auf Dauer angelegten Legende kommunizieren[584]. Für eine auf Dauer angelegte Legende wird man mehr verlangen müssen als die Nutzung eines Nicknames als Pseudonym[585]. Allerdings wird man in diesen Fällen die ermittelnden Beamten zumindest als „nicht offen ermittelnde Polizeibeamte" (noeP) qualifizieren müssen[586], da sie sich verdeckt an der Kommunikation beteiligen. Je differenzierter die Legende aufgefächert und untermauert werden muss, desto größer ist die Gefahr, dass die vom Bundesverfassungsgericht entwickelte Grenze zur Ausnutzung eines schutzwürdigen Vertrauens des Betroffenen in die Identität und die Motivation seines Kommunikationspartners überschritten wird[587].

199; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 519 ff.; *Soiné*, NStZ 2003, 225, 226 ff.

580 Vgl. beispielsweise § 22 Abs. 1 Nr. 4 BWPolG.

581 *Son*, Heimliche polizeiliche Eingriffe in das informationelle Selbstbestimmungsrecht, 2006, S. 215.

582 Vgl. *Murswiek*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 2, Rdnr. 88b; *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 176; *Makrutzki*, Verdeckte Ermittlungen im Strafprozess, 2000, S. 104 ff.; *Baron*, Zur Frage der Zulässigkeit des Einsatzes verdeckt ermittelnder Personen und Vorschlag einer umfassenden gesetzlichen Regelung, 2002, S. 77 ff.; *Duttge*, JZ 1996, 556, 562 ff.; *Lammer*, Verdeckte Ermittlungen im Strafprozess, 1992, S. 25 ff.; *VGH Mannheim*, DVBl 1995, 367, 368; *Knemeyer*, Polizei- und Ordnungsrecht, 11. Aufl., 2007, Rdnr. 197; vgl. insgesamt zur rechtlichen Entwicklung auch *Nitz*, Einsatzbedingte Straftaten Verdeckter Ermittler, 1997, S. 29 ff.

583 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 626; *Schenke*, Polizei- und Ordnungsrecht, 5. Aufl., 2007, Rdnr. 198.

584 Vgl. *Nack*, in: Karlsruher Kommentar zur StPO, 6. Aufl., 2008, § 110a, Rdnr. 7.

585 Vgl. *Böckenförde*, Die Ermittlung im Netz, 2003, S. 231 ff.

586 Vgl. *Nack*, in: Karlsruher Kommentar zur StPO, 6. Aufl., 2008, § 110a, Rdnr. 6 ff.; vgl. zu den rechtlichen Grenzen der Ermittlungen eines noeP BGHSt 55, 138 ff.; zur Abgrenzung der Verdeckten Ermittler von noeP siehe *Schmitz*, Rechtliche Probleme des Einsatzes Verdeckter Ermittler, 1996, S. 147; *Baron*, Zur Frage der Zulässigkeit des Einsatzes verdeckt ermittelnder Personen und Vorschlag einer umfassenden gesetzlichen Regelung, 2002, S. 12 ff.

587 Vgl. *Kochheim*, Verdeckte Ermittlungen im Internet, Stand: März 2012, S. 44, abzurufen unter *http://cyberfahnder.de*.

Prinzipiell müssen staatliche Stellen offen gegenüber den Bürgern auftreten. Im Polizeirecht gilt der Grundsatz der offenen Datenerhebung[588]. Bereits aus der staatlichen Neutralitätspflicht (Art. 5 Abs. 1 GG) lässt sich, bezogen auf das Internet, die grundsätzliche Offenlegung staatlicher Beiträge in Kommunikationsforen ableiten[589]. Die Verdeckung, um die Datenerhebung im Internet zu ermöglichen oder zu erleichtern, wirkt zudem auf die Situation ein, in der der Betroffene seine Daten preisgibt, und intensiviert dadurch den Eingriff in das Recht auf informationelle Selbstbestimmung[590]. Nur ausnahmsweise ist der verdeckte, getarnte oder sonst nicht offene Zugriff erlaubt[591]. Die verdeckte Datenerhebung ist folglich als Ausnahme vom Grundsatz der Offenheit der Datenerhebung anzusehen mit entsprechend hohen Anforderungen[592]. Zudem ist unbestritten, dass heimliche Maßnahmen eine stärkere Eingriffsintensität besitzen[593]. Für die rechtliche Beurteilung macht es einen entscheidenden Unterschied, ob beispielsweise eine polizeiliche Befragung offen als Befragung durch die Polizei durchgeführt wird oder ob der befragten Person Zweck und Behördenzugehörigkeit verheimlicht werden[594].

Während im „analogen" Bereich die verdeckten Datenerhebungen durch den Einsatz von V-Leuten oder Verdeckten Ermittlern allgemein als Grundrechtseingriffe gewertet werden, ist die Ansicht des Bundesverfassungsgerichts nicht nachvollziehbar, weshalb im virtuellen Bereich den Kommunikationsteilnehmern die Schutzwürdigkeit abgesprochen wird[595]. Auch

588 Vgl. z. B. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 566 ff.; *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., 2008, 6. Abschn. § 17 Rdnr. 63; *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 6. Aufl., 2010, S. 202; *Kugelmann*, Polizei- und Ordnungsrecht, 2006, S. 189; *Knemeyer* spricht in diesem Zusammenhang vom „Prinzip des offenen Visiers", *Knemeyer*, Polizei- und Ordnungsrecht, 11. Aufl., 2007, Rdnr. 199.

589 *Eifert*, in: Ladeur, Innovationsoffene Regulierung des Internets, 2003, S. 146; *ders.*, NVwZ 2008, 521, 522.

590 *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 495, 519 ff.

591 *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 786.

592 Vgl. beispielsweise § 19 Abs. 2 PolG BW, *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 567; *Würz*, Polizeiaufgaben und Datenschutz in Baden-Württemberg, 1993, Rdnr. 91 ff.

593 Vgl. z. B. BGHSt 51, 211; *Valerius*, JR 2007, 275, 278 ff.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, 494 ff., 519; *Schulz/Hoffmann*, CR 2010, 131, 134; vgl. auch zum qualitativen Unterschied zwischen offenen und heimlichen Maßnahmen *Krey/Haubrich*, JR 1992, 309, 313; *Kutscha*, NJW 1994, 85, 87; *Kretschmer*, Jura 1997, 581, 584.

594 *Albers*, Informationelle Selbstbestimmung, 2005, S. 441 ff.; siehe auch *Gusy*, NVwZ 1991, 614, 619 ff.

595 So sieht beispielsweise *Schaar* in der getarnten Beteiligung an Chat-Foren stets einen Ermittlungseingriff, *Schaar*, Datenschutz im Internet, 2002, Rdnr. 784. Ähnlich *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, BKAG, 2000, § 7, Rdnr. 6, für verdeckte Maßnahmen allgemein. Ahlf spricht bei verdeckten Maßnahmen im Internet sogar von einem gezielten Brechen des erkennbaren Willens des Kommunikationspartners.

außerhalb des Internet kann ein Polizist unproblematisch über seine Identität täuschen. Ein Polizist wird beispielsweise nicht im Rahmen von Scheinaufkäufen von Drogen seine wahre Identität offenlegen. Dennoch liegt ein verdecktes Handeln vor, wenn er ohne Aufdeckung seiner dienstlichen Tätigkeit sein Interesse an den Drogen vorgibt[596].

Die Argumentation des Bundesverfassungsgerichts, dass in den Kommunikationsdiensten des Internet in weitem Umfang keinerlei Überprüfungsmechanismen für die Identität und Wahrhaftigkeit der Kommunikationspartner bereitstünden[597], ist aus zwei Gründen angreifbar. Zum einen kann wieder die Parallele zum „analogen" Bereich gezogen werden[598]: Auch dort hat ein Bürger außerhalb staatlicher Eingriffsrechte nur wenige Möglichkeiten, die genaue Identität einer Person zu überprüfen[599]. Gerade bei lediglich flüchtigen Bekanntschaften wird er kaum die wahre Identität überprüfen können. Er wird also in der Regel weder den wirklichen Namen noch sonstige Angaben seines Gesprächspartners verifizieren können. Eine Täuschung über die Identität und Wahrhaftigkeit eines Kommunikationspartners ist folglich auch im realen Leben leicht möglich. Dass diese Täuschungshandlungen im Internet einfacher durchzuführen sind, kann aber nicht dazu führen, die Schutzwürdigkeit der Beteiligten generell, selbst bei langfristigen Kommunikationsbeziehungen, abzulehnen.

Zum anderen ist die Argumentation des Bundesverfassungsgerichts damit angreifbar, dass im Internet keine uneingeschränkte Anonymität herrscht[600]. In bestimmten Bereichen, wie beispielsweise Sozialen Netzwerken wie Xing oder eingeschränkt auch Facebook, wird gerade mit den Klarnamen und eher selten unter Pseudonymen kommuniziert. So bezeichnet Matthias Bäcker zutreffend die Ansicht des Bundesverfassungsgerichts, dass im Internet anonyme Kommunikationsformen vorherrschen würden, allenfalls als eine „Momentaufnahme"[601]. Auch die vermeintlich anonymen Kommunikationsdienste des Internet sind dies selbstredend nicht, da andernfalls die staatlichen Ermittlungen zwecklos wären[602]. IP-Adressen, E-Mail-Adressen oder sonstige Daten können in der Regel auf bestimmte natürliche Personen oder zumindest Personenkreise zurückgeführt werden. Diese Prüfungsme-

596 Vgl. zu diesem Beispiel *Valerius*, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, 2004, S. 137.

597 Vgl. BVerfGE 120, 274, Absatz 311.

598 *Singelnstein* bezweifelt ebenfalls, ob eine unterschiedliche Behandlung von Kommunikationsbeziehungen im Internet und im „analogen" Bereich der Netzkultur gerecht wird, *Singelnstein*, NStZ 2012, 593, 600.

599 Vgl. *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 788.

600 Vgl. *Rosengarten/Römer*, NJW 2012, 1764, 1766; vgl. auch zum Anonymitätsverlust durch IPv6 *Hoeren*, ZRP 2010, 251, 252 ff.

601 *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 134.

602 Vgl. *Schulz/Hoffmann*, CR 2010, 131, 134.

chanismen stehen zwar zumeist nur den Anbietern der verschiedenen Dienste und insbesondere staatlichen Stellen zu, jedoch kann die Identität eines Kommunikationsbeteiligten häufig aufgeklärt werden. Daher ist sich jeder Nutzer dieser Dienste bewusst, dass seine Beiträge, falls er nicht entsprechende Vorkehrungen getroffen hat, seiner Person beziehungsweise seinem Rechner zugeordnet werden können.

Gegen die vorbehaltlose Genehmigung einer staatlichen Identitätstäuschung im Internet sprechen ferner die tatsächlichen Abläufe im Rahmen der virtuellen Kommunikation. Die Besonderheit bei der aktiven Teilnahme staatlicher Stellen an der Internetkommunikation, beispielsweise in Chats oder Webforen, liegt darin, dass die staatliche Stelle nicht lediglich Daten abgreift, sondern vielmehr selbst erzeugt beziehungsweise daran mitwirkt. Ein Polizeibeamter kann so ein virtuelles Gespräch aktiv auf bestimmte, gegebenenfalls strafrechtlich relevante Themen lenken und eventuell den beteiligten Nutzer zu bestimmten Äußerungen bewegen[603]. Damit ist sogar zu rechnen, da die Polizisten sicherlich nicht stundenlang über rechtlich zur Gefahrenabwehr und Strafverfolgung unbedeutende Sachverhalte diskutieren wollen. Zudem werden die staatlichen Behörden wahrscheinlich bevorzugt die Chats, Webforen und sonstigen Kommunikationsdienste aufsuchen, die ein besonderes Gefahrenpotenzial darstellen. In diesen Foren können die Polizisten eher mit strafrechtlich bedeutsamen Sachverhalten rechnen. Die Behörden agieren in diesen Kommunikationsbeziehungen wie die anderen, nicht-staatlichen Kommunikationsteilnehmer. Allerdings erheben die Polizisten die personenbezogenen Daten verdeckt, da die anderen Kommunikationsteilnehmer sich nicht bewusst sind, dass eine staatliche Stelle an der Kommunikationsbeziehung aktiv beteiligt ist[604].

Ferner liegt es nahe, dass im Rahmen von Kommunikationsbeziehungen im Internet mit aktiver staatlicher Beteiligung relativ leicht personenbezoge Daten nicht bei dem Betroffenen selbst, sondern bei einem Dritten erhoben werden. Für Datenerhebungen gilt der Grundsatz der Unmittelbarkeit, gemäß dem personenbezogene Daten vorrangig beim Betroffenen selbst zu erheben sind[605]. Gerade in den Fällen, in denen die personenbezogenen Daten noch nicht von Beginn an allgemein zugänglich sind, sondern erst im kommunikativen Zusammenspiel der Beteiligten entstehen, besteht hier eine besondere Gefährdung des Unmittelbarkeitsgrundsatzes.

Kritisch gesehen werden kann zudem der Umstand, dass das Bundesverfassungsgericht selbst bei langfristigen Kommunikationsbeziehungen den Beteiligten kein schutzwürdiges Vertrauen dahingehend zugesteht, dass

603 Diese Gefahr sieht auch *Perrey*, Gefahrenabwehr und Internet, 2003, S. 148.

604 Siehe dazu auch *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 519 ff.

605 Vgl. beispielsweise § 19 Abs. 1 Satz 1 PolG BW, gemäß dem Daten grundsätzlich bei dem Betroffenen zu erheben sind, vgl. insgesamt dazu *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 564 ff.

kein Repräsentant einer staatlichen Stelle Mitglied der elektronischen Gemeinschaft ist[606]. Die langen Beziehungen unter Pseudonymen können außerdem die Realität der Beteiligten verändern, was „von der Rechtsordnung zu akzeptieren und als Grundrechtsausübung insoweit auch von staatlichen Stellen zu respektieren“ ist[607].

Im Ergebnis kann die Eingrenzung des Eingriffsbegriffs über die Schutzwürdigkeit des kommunikativen Vertrauens, wie vom Bundesverfassungsgericht vertreten, nicht vollends überzeugen. Nur weil im Internet die Möglichkeit der Identitätstäuschung relativ einfach ist und gerade auf Grund der Pseudonymisierung in Kommunikationsforen die wahren Identitäten regelmäßig verdeckt bleiben, kann damit gerade nicht die rechtliche Zulässigkeit einer staatlichen Identitätstäuschung begründet werden[608]. Vielmehr lässt sich sogar so argumentieren, dass auf Grund der geringen Möglichkeiten, im Internet die Identität und Absicht des Kommunikationspartners zu überprüfen, die Autonomie der Selbstdarstellung höher gefährdet ist, womit eine aktive staatliche Identitätstäuschung noch stärker wiegt[609].

2.3.1.5 Eingrenzung über die Art der Erhebung

Für eine differenzierte Eingrenzung des Eingriffsbegriffs ist für das Recht auf informationelle Selbstbestimmung danach zu unterscheiden, auf welche Art die staatliche Stelle die personenbezogenen Daten im Internet erhebt. Im Folgenden soll versucht werden, die verschiedenen Maßnahmen der Polizei im Rahmen der verdachtsunabhängigen Ermittlungen im virtuellen Raum zu typisieren und Fallgruppen zu bilden[610]. Diese Fallgruppen müssen allerdings entwicklungsoffen und anhand grundlegender Charakteristika unterscheidbar sein. Andernfalls könnten die gegenwärtigen und zukünftigen Entwicklungen des Internet mit seinen unterschiedlichen Diensten und Verknüpfungen dieser Dienste untereinander, die einem raschen Wandel unterliegen, später nur schwerlich einer Fallgruppe zugeordnet werden.

Wie bereits oben festgestellt wurde, liegt in der Datenerhebung aus öffentlich zugänglichen Bereichen des Internet grundsätzlich kein Eingriff in das Recht auf informationelle Selbstbestimmung[611]. Von diesem Grundsatz gibt es allerdings verschiedene Ausnahmen. Zweifelsohne ist – wie das Bundesverfassungsgericht zutreffend feststellt – dann die Eingriffsschwelle überschritten, wenn die staatliche Stelle allgemein zugängliche Daten gezielt

606 So stellen *Rosengarten/Römer* klar, dass auch im Internet Vertrauen entstehen kann, gerade in Sozialen Netzwerken, vgl. *Rosengarten/Römer*, NJW 2012, 1764, 1766.

607 *Schulz/Hoffmann*, CR 2010, 131, 133 (Fn. 24); vgl. auch *Schulz*, DuD 2009, 601, 604.

608 Ebenso *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 788; *Brunst*, Anonymität im Internet, 2009, S. 246 ff.

609 *Brunst*, Anonymität im Internet, 2009, S. 247.

610 So schlägt dies auch *Bäcker* vor, ohne vertieft darauf einzugehen, vgl. *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 134.

611 Vgl. auch BVerfGE 120, 274, Absatz 308.

zusammenträgt, speichert und gegebenenfalls unter Hinzuziehung weiterer Daten auswertet und sich daraus eine „besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt“[612]. Bei diesem „Datenerhebungsexzess“ werden die Rechte des Betroffenen erheblich verletzt, weshalb eine rechtfertigende Ermächtigungsnorm für diesen Eingriff notwendig ist.

Wenn das Bundesverfassungsgericht in seinem Urteil allerdings vom gezielten Zusammentragen, Speichern und Auswerten spricht, ist dies als Eingriffsvoraussetzung etwas ungenau. Das Recht auf informationelle Selbstbestimmung schützt vor jeder Form der Erhebung, schlichter Kenntnisnahme, Speicherung, Verwendung, Weitergabe oder Veröffentlichung von persönlichen Daten[613]. Bereits die gezielte Erhebung von personenbezogenen Daten einer bestimmten Person aus dem allgemein zugänglichen Bereich des Internet kann grundsätzlich einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen, soweit sich daraus eine „besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt“. Regelmäßig wird in einem solchen Fall die Speicherung und Verwendung der Daten, etwa indem ein Nutzerprofil erstellt wird, mit der Erhebung einhergehen[614]. Entscheidendes Element, ab wann für diese Fälle die Eingriffsschwelle überschritten wird, ist die besondere Gefahrenlage für die Persönlichkeit des Betroffenen. In welchen Fällen eine besondere Gefahrenlage für die Persönlichkeit eines Betroffenen besteht, kann nur einzelfallbezogen entschieden werden[615]. Maßgeblich sind beispielsweise die Intensität und die Dauer der staatlichen Datenerhebungen. Eine langfristige Überwachung der Beiträge des Betroffenen in Webforen kann zum Beispiel bereits zu einer besonderen Gefahrenlage für die Persönlichkeit des Betroffenen führen.

Ferner liegt ausnahmsweise ein Eingriff in das Recht auf informationelle Selbstbestimmung durch die verdachtsunabhängigen Ermittlungen der Polizei im Internet vor, wenn die staatliche Stelle verdeckt aktiv mit den Nutzern eines Webforums, Chats usw. kommuniziert. Wie bereits oben näher dargestellt wurde, sind die staatlichen Stellen im Internet grundsätzlich nicht zu einer Identitätstäuschung berechtigt. Schon aus der staatlichen

612 BVerfGE 120, 274, Absatz 309; *Bär*, MMR 2008, 325, 326 ff.; *Schulz/Hoffmann*, CR 2010, 131, 132 m. w. N.

613 Vgl. *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 176 m. w. N.

614 Bereits das Volkszählungsurteil sah den engen Zusammenhang zwischen Erhebung und Verwendung personenbezogener Daten, vgl. BVerfGE 65, 1, 41 ff.; vgl. auch *Perrey*, Gefahrenabwehr und Internet, 2003, S. 145.

615 *Henrichs* geht von der besonderen Gefährdungslage bei den gezielten Maßnahmen „mit polizeilicher Zielrichtung“ aus, vgl. *Henrichs*, Kriminalistik 2011, 622 (Fn. 5); *Brenneisen/Staack* beziehen sich auf die Rechtsprechung des Bundesverwaltungsgerichts (BVerwG vom 21.07.2010, 6 C 22/09), welches einen Grundrechtseingriff annimmt, wenn die zielgerichtete Erhebung öffentlich zugänglicher Daten „durch ihre systematische Erhebung, Sammlung und Erfassung einen zusätzlichen Aussagewert“ erhält, vgl. *Brenneisen/Staack*, Kriminalistik 2012, 627, 628.

Neutralitätspflicht (Art. 5 Abs. 1 GG) lässt sich die generelle Offenlegung staatlicher Beiträge in Kommunikationsforen des Internet ableiten[616]. Durch die Identitätstäuschung handeln die staatlichen Stellen im Rahmen der Kommunikationsbeziehung verdeckt, was den Eingriff in das Recht auf informationelle Selbstbestimmung verschärft[617]. Außerdem wird der Eingriff intensiviert, da die Betroffenen regelmäßig keinen Anlass für die Datenerhebung geschaffen haben[618]. Die verdachtsunabhängigen Ermittlungen der Polizei können praktisch jeden Nutzer der beobachteten Dienste des Internet treffen.

Entscheidend für die Frage, ob ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt, ist somit die Art, wie die staatliche Stelle die personenbezogenen Daten im Internet erhebt. Das konkrete Verhalten des Polizeibeamten und seine Vorgehensweise im Internet bestimmen, wann ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt. Die Grenze zum Grundrechtseingriff ist dann überschritten, wenn der Polizeibeamte seinen Kommunikationspartner aktiv über seine Identität, Funktion oder Motivation täuscht[619]. Diese aktive Täuschung liegt bereits dann vor, wenn er unter Verdeckung seiner Behördenzugehörigkeit mit anderen Teilnehmern in den Internetdiensten kommuniziert, also über seinen Beobachtungsstatus hinausgeht und selbst Beiträge verfasst. Konkret bedeutet dies für die einzelnen bekannten Maßnahmen der Polizei im Rahmen der verdachtsunabhängigen Ermittlungen im Internet, dass in bestimmten Fällen ein Grundrechtseingriff vorliegt.

2.3.1.5.1 Einsatz von Suchmaschinen

Die staatlichen Stellen setzen für ihre verdachtsunabhängigen Ermittlungen im Internet allgemeine Suchmaschinen, wie beispielsweise Google, sowie ihre eigenen Suchmaschinen (z. B. INTERMIT) ein. Die Abfrage von Suchmaschinen, Registern und ähnlichen Informationsdiensten im Internet stellt gewöhnlich keinen Grundrechtseingriff dar[620]. Die Suchmaschinen werten

616 *Eifert*, in: Ladeur, Innovationsoffene Regulierung des Internets, 2003, S. 146; *ders.*, NVwZ 2008, 521, 522.

617 Vgl. auch *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 519 ff.

618 Vgl. zu höheren Eingriffsintensität von Informationserhebungen gegenüber Personen, die den Eingriff durch ihr Verhallten nicht veranlasst haben, beispielsweise BVerfGE 120, 378, 402; 115, 320, 354.

619 So *Bäcker*, der allerdings anscheinend dann keine aktive Täuschung annähme, wenn lediglich eine allgemeine Kommunikationsbereitschaft ausgenutzt würde, *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 134.

620 Vgl. z. B. *Kudlich*, GA 2011, 193, 198; siehe insgesamt zur datenschutzrechtlichen Problematik von Suchmaschinen, mit denen nach Personen gesucht werden kann, *Seidel/Nink*, CR 2009, 666, 668 ff.; *Weichert*, MR-Int 2007, 188; *ders.*, „Suchmaschinen sind im Prinzip rechtswidrig", Handelsblatt vom 03.02.2008, abzurufen unter *http://www.handelsblatt.com/suchmaschinen-sind-im-prinzip-rechtswidrig/2918060.html*.

in der Regel die öffentlich zugänglichen Bereiche des Internet aus. Für ihre Nutzer und auch die Polizisten stellen sie eine Arbeitserleichterung dar. Daher handeln die staatlichen Stellen eingriffslos, soweit sie Suchmaschinen und Register nach Reizwörtern abfragen[621].

Bei der Abfrage einer Suchmaschine liegt auch keine verdeckte Ermittlungsmaßnahme vor. Erst wenn die staatliche Stelle direkt mit einem Kommunikationspartner in Kontakt tritt, wird eine Unterscheidung zwischen einer verdeckten und offenen Ermittlung möglich[622]. Der Suchmaschineneinsatz läuft so ab, dass die wahre Identität des Nutzers irrelevant ist. Der Adressat der Suchanfrage ist nicht daran interessiert, welche natürliche Person hinter der Suchanfrage steht. Dem steht auch nicht entgegen, dass für die Suchanfrage der Absender durch seine IP-Adresse ermittelbar wäre. Aus technischer Sicht muss der Absender genau zuzuordnen sein, da ansonsten die Anfrage nicht beantwortet werden könnte. Selbst wenn die Behörde diese Dienste bewusst mit einer Adresse nutzen würde, die nicht mit ihrer Behördeneigenschaft in Zusammenhang zu bringen wäre, läge keine verdeckte Maßnahme vor. Diese anonyme Kommunikationsbeziehung benötigt lediglich aus technischer Sicht bestimmte Daten des Absenders und liefert automatisiert das Ergebnis der Suchanfrage. Eine aktive Identitätstäuschung ist folglich seitens der staatlichen Stelle kaum möglich.

Allenfalls in den Fällen, in denen beispielsweise ein Suchmaschinenbetreiber die Anfragen bestimmter Behördenadressen herausfiltern würde, um diese nicht zu beantworten, könnte in der Nutzung einer behördenfremden Adresse eine verdeckte Ermittlungsmaßnahme liegen[623]. Entsprechende Fälle sind allerdings in der Praxis nicht bekannt. Daher kann diese besondere Fallkonstellation vernachlässigt werden. Die anonym-öffentliche Nutzung einer Suchmaschine ist somit als keine verdeckte Datenerhebung zu qualifizieren.

Eine Grenze findet der Einsatz von Suchmaschinen in den Fällen, in denen die staatliche Stelle die Suchmaschinen dazu nutzt, allgemein zugängliche Daten gezielt zusammenzutragen und sich daraus eine „besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt“[624]. Dieser „Datenerhebungsexzess“ kann beispielsweise dann vorliegen, wenn eine Behörde eine Suchmaschine einsetzt, um systematisch personenbezogene Daten einer bestimmten Person zu sammeln. Allein die Eingabe eines Klarnamens bei einer Suchmaschine, eventuell noch ergänzt um weitere Identifikationsmerkmale wie den Namen des Wohnorts oder des Arbeitgebers des Betroffenen, reichen für eine besondere Gefahrenlage für die Persönlichkeit

621 *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 511.

622 *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 519.

623 Vgl. insgesamt dazu *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 519 ff.

624 Vgl. zu diesem „Datenerhebungsexzess“ BVerfGE 120, 274, Absatz 309.

des Betroffenen noch nicht aus[625]. Wenn jedoch die staatliche Stelle gezielt und längerfristig das virtuelle Verhalten einer bestimmten Person überwacht, indem sie beispielsweise die Ergebnisse der Anfragen bei einer Suchmaschine zu dieser Person aufruft und die Daten zielgerichtet zusammenträgt, liegt darin ein Eingriff in das Recht auf informationelle Selbstbestimmung. Soweit dies beachtet wird, darf die Polizei auch selbst entwickelte Suchmaschinen einsetzen.

Die Polizei könnte im Rahmen ihrer verdachtsunabhängigen Ermittlungen aus den öffentlich zugänglichen Bereichen des Internet erhobene personenbezogene Daten untereinander oder mit anderen Datensätzen verknüpfen. Dieses sogenannte „Data Mining" führt die Polizei nach aktuellem Informationsstand nicht durch[626]. Die Möglichkeiten des Data Mining, beispielsweise umfassende Verhaltens- und Bewegungsprofile zu erstellen, können Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen[627], wenn sich daraus eine „besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt"[628]. Diese besondere Gefahrenlage wird durch die Masse der personenbezogenen Daten, die im Internet frei zugänglich erhoben werden könnten, verstärkt. Eine systematische Erhebung und Auswertung dieser Daten sowie die Verknüpfung mit weiteren Datensätzen würde die Eingriffsschwelle sehr schnell überschreiten. Ferner könnten die Resultate des Data Mining durch gezielte Veröffentlichung von unzutreffenden Daten im Internet manipuliert werden.

Im Ergebnis wird der gewöhnliche Einsatz von Suchmaschinen im Rahmen der verdachtsunabhängigen Ermittlungen der Polizei im Internet regelmäßig keinen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen.

2.3.1.5.2 Aufruf öffentlich zugänglicher Inhalte

Zu den öffentlich zugänglichen Bereichen des Internet werden die Webseiten gezählt, die Inhalte „an jedermann oder zumindest einen nicht weiter abgegrenzten Personenkreis" richten, also beispielsweise allgemein zugängliche Seiten im World Wide Web[629]. Ein Großteil der Webseiten im Internet gehört zu diesen öffentlich zugänglichen Bereichen. Diese Bereiche unterliegen keiner Zugangsbeschränkung. Nutzer können sie ohne Registrierung

625 *Petri* warnt allerdings, dass bei der Verwendung von Suchmaschinen die personenbezogenen Daten eines Betroffenen im Extremfall zu vollständigen Persönlichkeitsbildern kumulieren können. Dies spreche für den Eingriffscharakter dieser Maßnahmen, so *Petri*, in: Lisken/Denninger, HbPolR, 4. Aufl., 2007, Kap. H, Rdnr. 154.

626 Vgl. für das BKA die Antwort der Bundesregierung auf eine Kleine Anfrage, BT-Drs 17/6587, S. 7; fortführend die weitere Kleine Anfrage u. a. zum Data Mining mit Antwort der Bundesregierung, BT-Drs 17/11582.

627 Vgl. *Koch*, ITRB 2011, 158.

628 Vgl. zu diesem „Datenerhebungsexzess" BVerfGE 120, 274, Absatz 309.

629 BVerfGE 120, 274, Absatz 308.

oder sonstige Berechtigung unbeschränkt besuchen. Die Polizei darf diese Inhalte, wie jeder andere Nutzer auch, grundsätzlich aufrufen, ohne in das Recht auf informationelle Selbstbestimmung einzugreifen. Nutzer, die personenbezogene Daten in diesen Bereichen des Internet veröffentlichen, müssen mit der Beobachtung durch staatliche Stellen rechnen. Ihnen steht insoweit kein schutzwürdiges Vertrauen zu.

Selbst wenn Dritte personenbezogene Daten von anderen Betroffenen veröffentlichen und diese öffentlich zugänglich sind, liegt grundsätzlich kein Eingriff durch die Datenerhebung der Behörde vor[630]. Dies gilt selbst für gefälschte Daten, da entscheidend für die fehlende Eingriffsqualität die freie Zugänglichkeit der Quelle ist[631]. Ein Polizist wird häufig nicht genau erkennen können, ob die Daten von dem Betroffenen selbst oder einem Dritten veröffentlicht wurden. Falls offensichtlich erkennbar ist, dass ein Dritter die Daten eines anderen Betroffenen im Internet zugänglich gemacht hat, können zudem bereits die weitergehenden Vorschriften aus dem Polizeirecht oder sogar der Strafprozessordnung einschlägig sein, die einen möglichen Eingriff rechtfertigen würden.

Die Polizeibeamten dürfen beispielsweise Webseiten im Internet aufrufen, die Informationen zu Unternehmen, Vereinen oder sonstigen Gruppen enthalten. Angebote von Zeitschriften und Zeitungen oder sonstige frei zugängliche Inhalte von Presseorganen dürfen die staatlichen Stellen ebenfalls einsehen. Für die Arbeit der Polizei können dabei die Kommentarfunktionen zu Artikeln relevant sein. Durch die Kommentarfunktionen können Leser des Artikels – oft ohne vorherige Registrierung und Angabe ihres Klarnamens – den Inhalt des Artikels kommentieren. Den Polizeibeamten ist es auch nicht verwehrt, private Webseiten und Blogs aufzurufen, soweit diese ohne Zugangsbeschränkungen einsehbar sind.

Vor den Entwicklungen des Web 2.0, also der erweiterten Nutzung des Internet zur Interaktivität, müssen sich die staatlichen Stellen nicht verschließen. Sie dürfen sich zum Beispiel Videofilme, Bilder oder Podcasts[632] anschauen und/oder anhören. Im Ergebnis dürfen die Behörden im öffentlich zugänglichen Bereich des Internet so agieren, wie es jedem anderen Nutzer möglich ist. Zukünftige Entwicklungen neuer Dienste oder Verknüpfungen verschiedener Dienste im Internet beeinflussen dieses staatliche Recht grundsätzlich nicht.

Begrenzt werden die eingriffslosen staatlichen Befugnisse für die Fälle, in denen die Behörde allgemein zugängliche Daten gezielt zusammenträgt und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffe-

630 *Petri* wirft diese Frage auch auf, lässt sie aber offen, *Petri*, DuD 2010, 25, 29.

631 Vgl. insgesamt dazu *Perrey*, Gefahrenabwehr und Internet, 2003, S. 149 ff. (Fn. 634).

632 Podcasts sind Radiosendungen, die unabhängig von Sendezeiten über das Internet abgerufen werden können. Soweit es sich um Videomaterial handelt, spricht man auch von Vodcasts oder Vidcasts.

nen ergibt. Eine solche Situation kann beispielsweise vorliegen, wenn die Behörde einen Blog systematisch und längerfristig überwacht.

2.3.1.5.3 Aufruf geschützter Inhalte

Bestimmte Bereiche des Internet sind nicht öffentlich zugänglich. Zu diesen Bereichen können beispielsweise bestimmte Mitgliederbereiche auf Webseiten gehören[633]. Der Zugang zu diesen Bereichen kann auf unterschiedliche Weise beschränkt sein. Regelmäßig wird der Modus der Zugangsbeschränkung darin bestehen, dass der Zutritt nur mit einem Benutzernamen oder einer Benutzeridentifikation sowie dem zugehörigen Passwort möglich ist. In welchen Fällen die Polizei dabei im Rahmen der verdachtsunabhängigen Ermittlungen im Internet das Recht auf informationelle Selbstbestimmung verletzen kann, muss differenziert betrachtet werden.

Häufig wird der interessierte Nutzer bei dem geschützten Internet-Angebot neben einem Benutzernamen zur Registrierung seine E-Mail-Adresse angeben müssen. Daraufhin wird automatisch an die angegebene E-Mail-Adresse entweder das Passwort für den Abruf der geschützten Inhalte oder aber, soweit der Nutzer bereits bei seiner Registrierung ein eigenes Passwort gewählt hat, ein Link zur Authentifizierung des Nutzers gesandt. Der Nutzer kann dann diesen Link abrufen, womit sein Zugang authentifiziert und freigeschaltet ist. Die Erteilung der Zugangsberechtigung kann auf unterschiedliche andere Weisen erfolgen[634]. Gemeinsam ist den meisten dieser Zugangsberechtigungssysteme, dass der Diensteanbieter die Angaben des interessierten Nutzers nicht näher verifiziert. Zu diesen geforderten Angaben des interessierten Nutzers gehören teilweise über den Namen und die E-Mail-Adresse hinausgehende Daten, wie etwa das Alter, das Geschlecht oder die Adresse des Nutzers.

Staatliche Stellen dürfen sich bei solchen Diensten registrieren und damit die geschützten Inhalte einsehen. Hierbei liegt regelmäßig kein Eingriff in das Recht auf informationelle Selbstbestimmung vor, wenn die staatliche Stelle ihre Identität nicht offenlegt. In den meisten Fällen erfolgt der Zugang zu diesen geschützten Bereichen des Internet automatisiert, so dass keine natürliche Person zwischengeschaltet ist. Eine direkte Täuschung durch den Polizeibeamten scheidet folglich in diesen Fällen aus. Unabhängig davon, dass bei dieser Art von Zugangsbeschränkung die Angabe eines falschen Namens zur Identitätsverschleierung zumeist nicht notwendig ist, liegt selbst darin kein Grundrechtseingriff. Der Diensteanbieter führt keine konkrete Identitätskontrolle durch. Die persönlichen Angaben des interessierten Nutzers werden nicht hinreichend verifiziert. Soweit also ein Polizist statt seines Klarnamens einen anderen Namen eingibt und seine Behördenzugehörigkeit verschweigt, greift er bei einem Aufruf der geschützten

633 Näher dazu *Böckenförde*, Die Ermittlung im Netz, 2003, S. 197.

634 Vgl. insgesamt *Böckenförde*, Die Ermittlung im Netz, 2003, S. 197 ff.

Inhalte nicht in das Recht auf informationelle Selbstbestimmung ein. Der Diensteanbieter und etwaige weitere Personen, die die Informationen im geschützten Bereich hinterlegt haben, können ohne besondere Identitätskontrollen nicht darauf vertrauen, dass keine staatliche Stelle diese Informationen abruft. Für den Anbieter des Dienstes ist es nicht entscheidend, welche Person sich den Zugang zu den Inhalten verschafft. Ohne besondere Identitätskontrollmechanismen steht der Diensteanbieter den Nutzern indifferent gegenüber und hat daher kein schutzwürdiges Vertrauen hinsichtlich der wahren Identität der Nutzer. Gleiches gilt für etwaige weitere Personen, die geschützte Inhalte durch diesen Diensteanbieter veröffentlichen lassen.

Anders ist die Rechtslage zu beurteilen, wenn der Diensteanbieter besondere Schutzmechanismen zur Identitätsfeststellung vorsieht, mit denen er die Identität der interessierten Nutzer sicher feststellen kann. Zur Authentifizierung kann der Diensteanbieter beispielsweise Chipkarten, Ausweise, das sogenannte Post-Ident-Verfahren[635], biometrische Verfahren oder in Zukunft den elektronischen Personalausweis einsetzen[636]. Je nach Ausgestaltung des Authentifizierungsvorganges hat der Diensteanbieter die Angaben des Nutzers genau verifiziert. Wenn beispielsweise der Personalausweis oder ein vergleichbares Dokument direkt oder in beglaubigter Kopie vorzulegen sind, genügt ein Anbieter den Identifizierungsanforderungen. Der Diensteanbieter wird in diesen Fällen bei jedem interessierten Nutzer die Daten abgleichen und gegebenenfalls einzelfallbezogen entscheiden, ob der Interessent eine Zugangsberechtigung für den geschützten Bereich erhält. Der zugangsberechtigte Personenkreis ist damit identifiziert. Der unberechtigte Zugang zu solchen geschützten Inhalten nach einem hinreichend bestimmten Identifizierungsprozess greift damit in das Recht auf informationelle Selbstbestimmung ein[637].

Unberechtigt handelt eine staatliche Stelle etwa dann, wenn sie Zugangsschlüssel eines anderen Berechtigten nutzt[638]. Insoweit kommt es für den Eingriff in das Recht auf informationelle Selbstbestimmung nicht darauf an, ob die staatliche Stelle den Zugangsschlüssel ohne Wissen oder gegen den Willen des Berechtigten erhalten hat[639]. Der Diensteanbieter will durch seine Schutzmechanismen sicherstellen, dass nur bestimmte, identifizierte

635 Bei dem Post-Ident-Verfahren muss der Empfänger des Briefes, welcher z. B. das Passwort enthält, beim Postamt seinen Personalausweis oder Reisepass vorlegen, um den Brief zu erhalten, vgl. dazu *Möller*, NJW 2005, 1605 ff.; siehe zur Erzeugung von Nichtöffentlichkeit im Internet durch das Post-Ident-Verfahren *Henrichs*, Kriminalistik 2011, 622, 625.

636 *Schulz/Hoffmann*, CR 2010, 131, 132; vgl. auch *Böckenförde*, Die Ermittlung im Netz, 2003, S. 200 ff.

637 So auch *Böckenförde*, Die Ermittlung im Netz, 2003, S. 200 ff.

638 Vgl. bereits *Zöller*, GA 2000, 563, 570; *Bär*, MMR 1998, 463, 465.

639 Anders aber das BVerfG für einen Eingriff in das Telekommunikationsgeheimnis, siehe BVerfGE 120, 274, Absätze 291 ff.

Personen die geschützten Informationen einsehen dürfen. Sein Vertrauen und gegebenenfalls auch das Vertrauen weiterer Personen, die Inhalte durch den Diensteanbieter veröffentlichen lassen, ist schutzwürdig. Die staatliche Stelle würde Daten erheben können, indem sie das schutzwürdige Vertrauen der Betroffenen in die Identität des vermeintlich berechtigten Nutzers ausnutzt. Darin läge ein Grundrechtseingriff.

Die Behörde würde aber ebenfalls unberechtigt handeln, wenn sie bei der Datenabfrage des Diensteanbieters unrichtige Daten oder Daten einer anderen Person angeben würde. In diesen Fällen würde allerdings die Authentifizierung, soweit nicht etwa gefälschte Ausweispapiere vorgelegt würden, scheitern. Ein Polizeibeamter unterliegt für den Zugang zu den geschützten Bereichen des Internet, für die der Diensteanbieter die Identität des interessierten Nutzers verifiziert, sogar einer Offenbarungspflicht seiner Behördenzugehörigkeit. Der Diensteanbieter hat durch sein strenges Zugangsverfahren als vertrauensbildende Maßnahme den berechtigten Personenkreis beschränkt[640]. Der berechtigte Personenkreis vertraut also darauf, dass nur diejenigen Personen Zutritt erhalten, die der Diensteanbieter anhand der allen vorgegebenen Kriterien ausgewählt hat. Indem der Polizist seine Behördenzugehörigkeit verschwiege, würde er den Diensteanbieter durch Unterlassen dieser relevanten Angabe täuschen. Er würde also die geschützten Daten durch Vortäuschen einer behördenfremden Identität erhalten. Seine Datenerhebung wäre damit nicht offen, sondern er würde vielmehr verdeckt die geschützten Daten erheben. Der Staat darf auf Grund seiner weitreichenden Machtmittel im Hinblick auf die späteren Datenverarbeitungsmöglichkeiten gerade nicht über seine Identität täuschen[641]. Die faktische Möglichkeit einer Identitätstäuschung berechtigt staatliche Stellen nicht eingriffslos zur Identitätstäuschung, da die Erwartungen der Bürger hinsichtlich staatlicher Datenerhebungen wegen der Kompetenzgebundenheit des Staates durch die Rechtslage geprägt sind[642]. Gerade wenn ein Diensteanbieter besondere Schutzmechanismen zur Identitätsfeststellung vorsieht, ist sein Vertrauen und gegebenenfalls das weiterer Betroffener schutzwürdig, dass keine staatliche Stelle den geschützten Bereich heimlich betritt.

Soweit die Behördenzugehörigkeit für den Diensteanbieter kein Zugangshindernis ist, darf er eine staatliche Stelle dazu berechtigen, die dann in der Regel eingriffslos handelt. Etwas anderes kann allerdings dann gelten, wenn der Ausschluss staatlicher Kontrollen Wesensgehalt des geschützten Bereiches ist und neben dem Diensteanbieter weitere Personen betroffen sind. Dies kann beispielsweise dann vorliegen, wenn sich die Mitglieder einer

640 Vgl. zur Vertrauensbildung im Internet *Boehme-Neßler*, MMR 2009, 439 ff.
641 Vgl. *Perrey*, Gefahrenabwehr und Internet, 2002, S. 149.
642 *Eifert*, NVwZ 2008, 521, 522.

politischen Gruppierung bewusst einer staatlichen Überwachung – etwa in einem zugangsgeschützten Webforum – entziehen wollten. In dem Zugang zum geschützten Bereich, selbst bei freiwilliger Berechtigung durch den jeweiligen Diensteanbieter, läge bei der Erhebung personenbezogener Daten ein Eingriff in das Recht auf informationelle Selbstbestimmung.

Zu diesem Ergebnis kommt man auch, wenn der Diensteanbieter auf Grund persönlicher Kontakte oder Begegnungen die Zugangsberechtigungen vergibt[643]. Eine solche Konstellation liegt beispielsweise vor, wenn die Mitarbeiter eines Unternehmens den Zugang zu einem geschützten Bereich des Internet, etwa auf der eigenen Webseite des Unternehmens angelegt, erhalten. Ferner kann dies im privaten Umfeld relevant sein, wenn Vereine, Parteien oder sonstige Personengruppen digitalisierte Informationen für ihre Mitglieder zugangsgeschützt im Internet bereithalten. Das Mitlesen eines privaten Blogs könnte nur bestimmten Personen, die vom Blogger auf Grund des persönlichen Kontaktes ein Passwort bekommen haben, ermöglicht werden. In den genannten Fällen überträgt der Diensteanbieter die Vertrauenswürdigkeit zu bestimmten Personen aus dem realen Leben in die virtuelle Welt. Die Identitäten der Nutzer sind damit hinreichend verifiziert. Den geschützten Freiraum, den sich bestimmte Personengruppen innerhalb des Internet geschaffen haben, muss auch der Staat grundsätzlich respektieren. Ein unberechtigter Zugang greift daher in das Recht auf informationelle Selbstbestimmung ein.

Anders kann dies zu beurteilen sein, wenn Nutzer Kreditkarten- oder Personalausweisdaten angeben müssen[644]. Vor dem Zugang zu den geschützten Informationen muss ein interessierter Nutzer hierbei seine Kreditkarten- oder Personalausweisdaten eintragen. Entgeltpflichtige Webseiten mit beispielsweise kinderpornografischen oder gewaltverherrlichenden Inhalten sichern sich durch die Angabe der Kreditkartendaten ihre Einnahmen. Der interessierte Nutzer muss dafür etwa den Namen des Kreditkarteninhabers und des Kreditkartenunternehmens, die Kreditkartennummer, das Ablaufdatum und zusätzlich eventuell die Prüfziffer übermitteln. Durch die Angabe dieser Daten könnte ein schutzwürdiges Vertrauen des Diensteanbieters in die Identität des interessierten Nutzers entstehen, da der Kreditkarteninhaber im Vorfeld seine Daten verifizieren musste, um die Kreditkarte zu erhalten. Gegen ein schutzwürdiges Vertrauen spricht allerdings, dass der Diensteanbieter die Daten zur Prüfung der Zahlungsfähigkeit des Interessenten und zu Abrechnungszwecken verlangt. Zusätzlich kann der interessierte Nutzer als Karteninhaber seine Volljährigkeit nachweisen, die für viele Anbieter altersbeschränkter Inhalte relevant ist. Dem Diensteanbieter geht es also nicht darum, welche genaue Person den Zugang will, son-

643 Vgl. dazu auch *Böckenförde*, Die Ermittlung im Netz, 2003, S. 201.

644 Vgl. insgesamt dazu auch *Böckenförde*, Die Ermittlung im Netz, 2003, S. 201 ff.

dern lediglich um die Bonität dieser Person und gegebenenfalls ihr Alter. Es fehlt die individualisierende, persönliche Identifizierung des interessierten Nutzers[645]. Das Vertrauen, dass keine staatliche Stelle die Zugangsberechtigung erhält, ist damit nicht schutzwürdig. Soweit ein Polizist durch Angabe von Kreditkartendaten und unter Verschweigung seiner Behördeneigenschaft diese Zugangskontrolle überwindet, liegt bei einer anschließenden Datenerhebung kein Eingriff in das Recht auf informationelle Selbstbestimmung vor.

Teilweise verlangen Diensteanbieter vor einem Zutritt zu den geschützten Inhalten die Angabe bestimmter Personalausweisdaten[646]. Dadurch soll sichergestellt werden, dass der interessierte Nutzer volljährig ist. Der Bundesgerichtshof hat bereits festgestellt, dass ein solches Altersverifikationssystem für den Zugang zu Webseiten unzureichend ist[647]. Der interessierte Nutzer muss dafür in der Regel drei Zahlenblöcke (Nummer der ausstellenden Behörde/Geburtsdatum/Ablaufdatum) angeben. Diese Zahlen sind jeweils durch eine Prüfziffer am Ende des Zahlenblockes getrennt. Zusätzlich steht eine Gesamtprüfziffer am Ende der Zahlenreihe. Die Angabe dieser Zahlenblöcke dient nicht der genauen Identifizierung der Person, sondern lediglich der Alterskontrolle. Eine genaue Identifizierung der Person kann ein privater Diensteanbieter mangels Zugriff auf die Personalausweisdaten gar nicht vornehmen. Anhand der Zahlenreihe kann er lediglich die Gültigkeit des Personalausweises und das Alter des Personalausweisinhabers erkennen. Aber auch dies kann leicht manipuliert werden, indem ein interessierter Nutzer Personalausweisdaten einer anderen Person oder potentiell gültige Personalausweisdaten einer möglichen Person berechnet und einträgt. Die mathematische Berechnung dieser Personalausweisdaten wird beispielsweise in frei zugänglichen Büchern und im Internet erklärt[648]. Im Ergebnis berührt die Überwindung dieses Zugangshindernisses nicht das Recht auf informationelle Selbstbestimmung.

2.3.1.5.4 Kommunikationsdienste ohne Registrierung

Bei den Kommunikationsdiensten im Internet tauschen die Nutzer direkt Informationen in ihren Beiträgen aus. Die Anzahl der Kommunikationsdienste im Internet, die für eine aktive Teilnahme keiner Registrierung bedürfen, ist relativ niedrig. Bei diesen Kommunikationsdiensten kann von einer Person ohne staatliche Befugnisse nicht erkannt werden, welche genaue Person einen Beitrag verfasst hat beziehungsweise von welchem Rechner der Beitrag versandt wurde. Da sich ein Nutzer nicht registrieren

645 *Böckenförde*, Die Ermittlung im Netz, 2003, S. 203.

646 Vgl. insgesamt dazu *Böckenförde*, Die Ermittlung im Netz, 2003, S. 204.

647 BGH, Urteil vom 18.10.2007, I ZR 102/05.

648 Die Berechnung kann beispielsweise hier nachgelesen werden: *http://www.pruefziffernberechnung.de/P/Personalausweis-DE.shtml*.

muss, fehlt eine genaue Zuordnung der Beiträge zu einer bestimmten Person. Die Nutzer veröffentlichen ihre Nachrichten entweder ganz anonym, also ohne jegliche Nennung eines Namens oder Pseudonyms, oder unter einem Pseudonym. Soweit ein Nutzer allerdings ein Pseudonym wählt, kann theoretisch jeder andere Nutzer unter diesem Pseudonym Beiträge verfassen, da sich die Nutzer nicht registrieren mussten. In der Praxis spielen Kommunikationsdienste, die für eine aktive Beteiligung keiner Registrierung bedürfen, keine große Rolle.

Weit wichtiger sind die Kommunikationsdienste, die zwar für die aktive Kommunikationsteilnahme eine Registrierung des Nutzers erfordern, jedoch für die reine Beobachtung keine Registrierung verlangen. Viele Webforen sind beispielsweise so konzipiert, dass ein interessierter Nutzer die Beiträge der anderen Nutzer lesen kann, ohne sich vorher anmelden zu müssen. Erst wenn er selbst aktiv in den Kommunikationsverlauf durch eigene Beiträge eingreifen möchte, muss er sich vorher registrieren. Die Beiträge der Nutzer in diesen Webforen kann folglich jeder Nutzer auf dem dafür vorgesehenen technischen Weg ohne Zugangsbeschränkung lesen. Teilweise kann er sich sogar die einzelnen Beiträge eines bestimmten Nutzers über die Suchfunktion in dem Webforum anzeigen lassen. Außerdem kann er, soweit die Suchfunktion ohne vorherige Registrierung verwendbar ist, das Forum nach bestimmten Reizwörtern durchsuchen.

Die Polizeibeamten dürfen im Rahmen ihrer verdachtsunabhängigen Ermittlungen im Internet Kommunikationsdienste ohne vorherige Registrierung grundsätzlich frei nutzen, ohne in das Recht auf informationelle Selbstbestimmung einzugreifen. Für die Beobachtung dieser Kommunikationsdienste gelten die obigen Ausführungen zum Aufruf öffentlich zugänglicher Inhalte entsprechend. Letztendlich handelt es sich bei der Beobachtung dieser Kommunikationsdienste um öffentlich zugängliche Webseiten, die zwar durch die ständig neuen Beiträge einem stetigen Wandel unterliegen, jedoch für alle Nutzer ohne Zugangsbeschränkung aufrufbar sind. Erst in den Fällen, in denen die staatliche Stelle zielgerichtet allgemein zugängliche Daten aus dem Kommunikationsdienst zusammenträgt und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen entwickelt, liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor.

2.3.1.5.5 Kommunikationsdienste mit Registrierung

Kommunikationsdienste mit Registrierung benötigen vor einer Nutzung die Anmeldung des Nutzers. Viele Webforen (z. B. Foren für bestimmte Interessensgebiete, wie Uhren- oder Autoforen) verlangen eine solche Registrierung, für die ein Nutzer beispielsweise ein Pseudonym und ein Passwort wählen muss sowie seine E-Mail-Adresse anzugeben hat. Die unterschiedlichen Möglichkeiten des Registrierungsvorgangs entsprechen denen, die

beim Aufruf geschützter Inhalte denkbar sind. In welchen Fällen bei Kommunikationsdiensten mit vorheriger Registrierung ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegen kann, muss differenziert betrachtet werden.

Soweit die staatliche Stelle offen die Daten erhebt, also innerhalb des Kommunikationsdienstes unter Bezeichnung der Dienststelle und gegebenenfalls weiterer notwendiger Angaben auftritt, liegt kein Eingriff vor[649]. Die Kommunikationspartner sind sich dessen bewusst, dass sie einer staatlichen Stelle gegenüber persönliche Daten eröffnen. Sie willigen somit in die Datenerhebung ein. Für eine offene Datenerhebung muss der Polizist in seinem Profil die genauen Angaben zu seiner Dienststelle etc. aufführen[650]. Ferner wird er nicht unter einem Pseudonym auftreten dürfen, sondern bereits aus seinem Nickname muss sich die Behördenzugehörigkeit ergeben[651]. Da von den Nutzern eines Kommunikationsdienstes nicht erwartet werden kann, dass sie stets das Profil aufrufen, um eine mögliche Behördeneigenschaft zu erkennen, muss sich dies bereits aus dem Pseudonym ergeben[652]. Außerdem sehen nicht alle Kommunikationsdienste vor, ein detailliertes Profil anzulegen. Die Behördenzugehörigkeit muss eindeutig aus dem gewählten Pseudonym sichtbar sein, um offen zu ermitteln.

Im „analogen" Leben ermittelt ein Polizeibeamter dann offen, wenn seine Behördenzugehörigkeit erkennbar ist. Da ein im Internet agierender Polizeibeamter weder eine Uniform trägt noch durch sonstige Umstände die Behördenzugehörigkeit für virtuelle Kommunikationspartner sichtbar ist, muss er diese für eine offene Datenerhebung in seinem Pseudonym eröffnen. Auf Nachfragen dazu muss der Polizist zudem wahrheitsgemäß antworten. Als eine verdeckte Ermittlung ist es bereits zu werten, wenn der ermittelnde Polizist zwar „richtige" Angaben, etwa Name und Wohnort, macht, dabei jedoch seine Behördenzugehörigkeit verschweigt oder verschleiert[653]. Um offen und eingriffsfrei zu ermitteln, muss der Polizist unmissverständlich seine wahre Identität offenbaren, so dass sich die Nutzer der Kommunikationsdienste darauf einstellen können.

Ein Eingriff in das Recht auf informationelle Selbstbestimmung kann selbst bei einer offenen Datenerhebung vorliegen, wenn die staatliche Stelle die Daten nicht unmittelbar beim Betroffenen, sondern bei einem Dritten

649 Ebenso *Perrey*, Gefahrenabwehr und Internet, 2002, S. 147.

650 Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 520.

651 Dies könnte beispielsweise derart erfolgen: „POK Schulz (LKA NRW)".

652 A. A. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 520, der es ausreichen lässt, wenn die Angaben zum Echtnamen im Profil stimmen.

653 Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 520; *Malek*, Strafsachen im Internet, 2005, S. 108.

erhebt[654]. Ein solcher Fall liegt beispielsweise vor, wenn ein ermittelnder Polizist seinen Kommunikationspartner in einem Chat über eine bestimmte Person ausfragt, die in diese Datenerhebung nicht eingewilligt hat.

Wenn die Behörde verdeckt auftritt, ist zunächst danach zu unterscheiden, ob der Diensteanbieter besondere Schutzmechanismen zur Identitätsfeststellung vorsieht, mit denen er die Identität der Nutzer sicher überprüfen kann, oder ob er die Angaben der Nutzer nicht näher verifiziert. Relativ deutlich lässt sich der Eingriff in das Recht auf informationelle Selbstbestimmung begründen, wenn der Diensteanbieter zur Identitätsfeststellung ein verlässliches Verfahren, wie beispielsweise das Post-Ident-Verfahren einsetzt. Soweit der Polizist seine Behördenzugehörigkeit – unabhängig davon, ob er konkret danach gefragt wurde – verschweigt, liegt ein Eingriff vor. Diese Konstellation ist vergleichbar mit dem Aufruf geschützter Inhalte, weshalb auf das Ergebnis der obigen Ausführungen verwiesen werden kann[655]. Die Nutzer eines Kommunikationsdienstes mit einem sicheren Schutzmechanismus zur Identitätsfeststellung dürfen darauf vertrauen, dass der Diensteanbieter die Identität des interessierten Nutzers verifiziert und entsprechend den für alle geltenden Kriterien über seine Zugangsberechtigung entscheidet. Die Täuschung einer staatlichen Stelle durch Verschleierung ihres Ermittlungsinteresses in diesem geschützten Bereich würde das schutzwürdige Vertrauen des Diensteanbieters sowie der Beteiligten an dem Kommunikationsdienst untergraben. Damit läge ein Grundrechtseingriff vor.

Soweit der Diensteanbieter lediglich eine einfach ausgestaltete Registrierung ohne hinreichende Identitätskontrolle vorsieht und der Polizist seine Behördenzugehörigkeit verschweigt, muss genauer unterschieden werden zwischen dem Verhalten des Polizisten innerhalb des Kommunikationsdienstes. Zunächst kann der Polizist als reiner Beobachter auftreten, ohne sich aktiv an der Kommunikation zu beteiligen. Er greift also lediglich die von anderen Kommunikationsteilnehmern entwickelten Daten ab, ohne selbst Beiträge zu verfassen. Ähnlich wie bereits oben für den Aufruf geschützter Inhalte können der Diensteanbieter sowie die Kommunikationsbeteiligten sich nicht auf ein schutzwürdiges Vertrauen berufen. Der Registrierungsvorgang läuft zumeist automatisiert ab, ohne dass eine natürliche Person zwischengeschaltet ist. Der Diensteanbieter steht auf Grund seiner geringen Anforderungen an die Registrierung und seiner fehlenden Authentifizierungsmechanismen den Personen, die Zugang zum Kommunikationsdienst erhalten wollen, indifferent gegenüber. Die Registrierung soll in der Regel lediglich ermöglichen, dass hinter einem gewählten Nickname immer eine bestimmte Person steht. Damit sind die einzelnen Beiträge bestimmten

654 Ähnlich *Perrey*, Gefahrenabwehr und Internet, 2003, S. 149 ff. (insbesondere Fn. 634).
655 Siehe Ziffer 2.3.1.5.3.

Personen zuzuordnen. Gerade bei Webforen ist dies ein wesentlicher Bestandteil, da die Beteiligten so über den langfristigen Zeitraum Informationen über die einzelnen Beteiligten erhalten und Meinungen einordnen können. Den Kommunikationsteilnehmern steht gleichfalls kein schutzwürdiges Vertrauen zu. Sie sind sich dessen bewusst, dass durch die simplen Registrierungsanforderungen quasi jede Person Zugang zu dem Forum erhalten kann. Häufig werden sie noch nicht einmal erkennen können, welcher ebenfalls angemeldete Nutzer gerade ihre Beiträge liest. Das passive Beobachten ohne eigene Aktivitäten des Polizisten greift daher nicht in das Recht auf informationelle Selbstbestimmung ein.

Dies gilt selbst dann, wenn die Polizisten ihre Behördenzugehörigkeit nicht offenlegen und ein unverfängliches Pseudonym wählen. Die Kommunikationsbeteiligten sind nicht schutzwürdig in ihrem Vertrauen, dass keine staatliche Stelle ihre Einträge liest, wenn keine entsprechenden Vorkehrungen durch den Diensteanbieter getroffen wurden. Der Polizist täuscht in diesem Fall die Kommunikationsbeteiligten nicht direkt über seine Identität, da er nicht aktiv mit ihnen kommuniziert.

Anders könnte die Rechtslage zu beurteilen sein, wenn der ermittelnde Beamte aktiv mit den anderen Nutzern des Dienstes kommuniziert. Dies bedeutet, dass er selbst Beiträge in einem Chat, einer Newsgroup oder einem Webforum verfasst und entsprechend virtuelle Gespräche führt. Im Rahmen einer solchen Konversation übernehmen regelmäßig beide beziehungsweise alle Beteiligten alternierend den aktiven Part. Ein Polizeibeamter kann dadurch aktiv auf bestimmte, gegebenenfalls strafrechtlich relevante Themen lenken und eventuell die beteiligten Kommunikationspartner zu bestimmten Äußerungen bewegen[656]. Indem der Polizist seine Behördenzugehörigkeit nicht offenlegt, täuscht er die anderen Beteiligten über seine wahre Identität. Die Identität des Kommunikationspartners ist zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung hochrelevant[657]. Dass eine Identitätstäuschung im Internet auch einer Behörde sehr leicht gemacht wird, darf nicht zu ihrer Legitimation führen. Allein aus einer faktischen Möglichkeit zur Identitätstäuschung darf gerade nicht gefolgert werden, dass für eine staatliche Stelle eine Identitätstäuschung rechtlich zulässig ist[658].

656 Diese Gefahr sieht auch *Perrey*, Gefahrenabwehr und Internet, 2003, S. 148.

657 *Eifert*, NVwZ 2008, 521, 522.

658 *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 788; *Brunst*, Anonymität im Internet, 2009, S. 246 ff.; *Kant*, Bürgerrechte und Polizei/CILIP 71 (1/2002), 29, 35; ähnlich auch *Hornung*, CR 2008, 299, 305, der zumindest bei längeren Kommunikationsbeziehungen die These des Bundesverfassungsgerichts für angreifbar hält. Bereits kritisch *Jacob*, 17. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz 1997/1998, BT-Drs 14/850, S. 111; *ders.*, 18. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz 1999/2000, BT-Drs 14/5555, S. 105.

Wenn das Bundesverfassungsgericht in seiner Entscheidung zur Internet-Aufklärung die Frage nach dem Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner aufwirft[659], stellt sich die weitergehende Frage, ob auch der Staat die einfachen Möglichkeiten der Identitätstäuschung ausnutzen darf. Gerade weil im Internet Täuschungen leicht möglich sind und den Kommunikationspartnern keine Überprüfungsmechanismen zur Verfügung stehen, sollte es vielmehr Aufgabe des Staates sein, im Internet Vertrauen zu schaffen[660]. Staatliche Stellen dürfen sich auf Grund ihrer Neutralitätspflicht (Art. 5 Abs. 1 GG) nicht auf eine Stufe mit den Bürgern stellen[661] und verdeckt Meinungen in Foren bilden sowie – was weitaus schwerwiegender ist – ihre Kommunikationspartner in ihren Aussagen beeinflussen. Für tatprovozierendes Verhalten polizeilicher Lockspitzel setzt das Rechtsstaatsprinzip enge Grenzen[662]. Das Täuschungsverbot des § 136a Abs. 1 Satz 1 StPO für Vernehmungen eines Beschuldigten verbietet zudem die bewusste Irreführung des Vernommenen[663].

Bei den verdachtsunabhängigen Ermittlungen im Internet kommuniziert die Polizei noch nicht einmal mit konkreten Beschuldigten, sondern mit unverdächtigen Personen. Entsprechend dem Recht auf informationelle Selbstbestimmung sollen die Betroffenen selbst die Kontrolle über die Preisgabe ihrer personenbezogenen Daten haben[664]. Zudem dient das Recht auf informationelle Selbstbestimmung „auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß“[665]. Dies bedeutet, dass der Betroffene die Kontrolle über die Preisgabe seiner persönlichen Daten gegenüber einem konkreten und gerade nicht beliebigen Kommunikationspartner haben soll[666]. Wenn eine staatliche Stelle aktiv mit einem Betroffenen im Internet kommuniziert, besteht die berechtigte Gefahr, dass der Betroffene die Kontrolle über die Preisgabe seiner Daten verliert. Er weiß nicht, dass sein Gegenüber zu einer ermittelnden Behörde gehört.

659 Vgl. BVerfGE 120, 274, Absätze 310 ff.

660 Vgl. zur Rolle des Rechts zur Vertrauensbildung im Internet *Boehme-Neßler*, MMR 2009, 439 ff.

661 Vgl. *Eifert*, NVwZ 2008, 521, 522.

662 Siehe beispielsweise BGHSt 45, 321, 324 ff.; 32, 345, 346 ff.

663 Vgl. BGHSt 31, 395, 399 ff.; 37, 48, 53; zur einschränkenden Auslegung siehe BGHSt 42, 139, 149; *Lesch*, in: Kleinknecht/Müller/Reitberger, StPO, § 136a, Rdnr. 28 ff.

664 BVerfGE 65, 1, 43.

665 BVerfGE 113, 29, 46.

666 Vgl. *Eifert*, NVwZ 2008, 521, 522.

Da die meisten Kommunikationsbeziehungen in Webforen und Chats so ausgerichtet sind, dass quasi in Echtzeit miteinander kommuniziert wird, kann es durchaus sein, dass sich ein Kommunikationspartner durch den verdeckt ermittelnden Polizisten zu unüberlegten Aussagen hinreißen lässt. Soweit der Kommunikationsdienst dann keine Editierfunktion[667] vorsieht, bleibt der Inhalt zudem bis zur Löschung durch den Diensteanbieter im Internet abrufbar. Wenn sich ein Polizist verdeckt ohne unmissverständliche Offenbarung seiner Behördenzugehörigkeit in einem Kommunikationsdienst mit Registrierung aktiv beteiligt und selbst Beiträge verfasst, liegt in seiner Datenerhebung ein Eingriff in das Recht auf informationelle Selbstbestimmung.

Ein solcher Eingriff liegt auch vor, wenn ein Polizist für die Datenerhebungen seine Behördenzugehörigkeit nur gegenüber dem Diensteanbieter offengelegt und der Diensteanbieter ihn dennoch zum Kommunikationsdienst zugelassen hat. Gefährdet sind für diesen Fall die Grundrechtsträger, die mit dem ermittelnden Polizisten kommunizieren.

2.3.1.5.6 Soziale Netzwerke

Soziale Netzwerke wie Facebook, StudiVZ oder Xing sind ein spezieller Unterfall der Kommunikationsdienste mit Registrierung. Auf Grund ihres zunehmenden Einflusses im virtuellen Kommunikationsverhalten sollen sie hier separat begutachtet werden, da für sie einige Besonderheiten bestehen[668]. Die Sozialen Netzwerke spielen zudem in der Arbeit der Polizei eine stetig wachsende Rolle[669]. Indem sich beispielsweise Bilder mit Personen verknüpfen lassen, können weitere Bilder dieser Person zugeordnet werden, weshalb der Auswertung Sozialer Netzwerke zukünftig eine besondere Relevanz für Ermittlungsmaßnahmen beigemessen wird[670].

Grundsätzlich gelten die obigen rechtlichen Ausführungen zu Kommunikationsdiensten mit Registrierung im Wesentlichen auch für die Sozialen Netzwerke entsprechend. Entgegen anderer Webforen und Chats kommunizieren die Beteiligten in den Sozialen Netzwerken häufig über ihre richtigen Klarnamen. Die Diensteanbieter sehen aber in der Regel keine besonderen

667 Bei einer Editierfunktion können die Nutzer nach Veröffentlichung ihrer Beiträge diese noch verändern oder sogar löschen.

668 Vgl. zu den polizeilichen Ermittlungen in Sozialen Netzwerken *Henrichs/Wilhelm*, Kriminalistik 2010, 30, 32 ff.; *Graf*, in: Beck´scher Online-Kommentar StPO, § 100a, Rdnr. 32c ff.; zu den besonderen Gefahren Sozialer Netzwerke für Kinder und Jugendliche siehe *Jandt/Roßnagel*, MMR 2011, 637 ff.

669 *Henrichs/Wilhelm*, Kriminalistik 2010, 30, 32 ff. Siehe dazu auch den 23. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die Jahre 2009 und 2010 vom 12.04.2011, S. 86. Nach Auskunft der Bundesregierung auf eine Kleine Anfrage ermitteln die Polizeibehörden des Bundes und insbesondere das BKA jedoch nicht anlassunabhängig in den Sozialen Netzwerken, vgl. BT-Drs 17/6587, S. 2.

670 Vgl. *Singelnstein*, NStZ 2012, 593, 599.

Schutzmechanismen zur Identitätsfeststellung vor, mit denen sie bei der Registrierung die Identität der Nutzer sicher überprüfen können.

Auf ihren individuellen Seiten der Sozialen Netzwerke veröffentlichen die Nutzer, soweit keine Zugangsbeschränkung herrscht für jeden Nutzer einsehbar, eine Vielzahl an persönlichen Daten und sonstigen Inhalten. Eine Überprüfung, ob die Daten und Inhalte richtig sind, findet nicht statt[671].

Die Sozialen Netzwerke zeichnen sich dadurch aus, dass die Kommunikationsbeziehungen stabiler sind und in einem größeren Maß auf persönlichem Vertrauen beruhen[672]. Wenn das Bundesverfassungsgericht in seiner Entscheidung zur Internet-Aufklärung davon spricht, dass das Vertrauen der Beteiligten in die Identität und Wahrhaftigkeit ihrer Kommunikationspartner selbst bei langen Kommunikationsbeziehungen nicht schutzwürdig ist[673], trifft dies auf Soziale Netzwerke nicht zu[674]. Bei diesen gefestigten Kommunikationsbeziehungen vertrauen die Nutzer durchaus darauf, dass sich beispielsweise hinter einem für den Betroffenen bekannten Namen gerade nicht verdeckt eine staatliche Stelle verbirgt. Soweit die Behörde also einen „Identitätsdiebstahl" beginge und unter dem vertrauten Namen einer anderen Person aufträte, läge zweifelsohne ein Grundrechtseingriff vor, wenn dadurch personenbezogene Daten erhoben würden. Dies würde auch gelten, wenn ein Polizist unter Verschleierung seiner Behördenzugehörigkeit aktiv mit den Nutzern im Sozialen Netzwerk kommuniziert[675].

Ein Sonderfall im Gegensatz zu anderen Kommunikationsdiensten mit Registrierung besteht aber dann, wenn der ermittelnde Polizist nur passiv beobachtet, sich diese Möglichkeit allerdings durch eine Identitätstäuschung ermöglicht hat. Ein solcher Fall liegt etwa vor, wenn der Polizist erst nach einer positiv beschiedenen sogenannten „Freundschaftsanfrage" geschützte Bereiche eines Betroffenen einsehen kann. Der Betroffene hat in diesem Fall bestimmte Bereiche seines Profils im Sozialen Netzwerk für die Öffentlichkeit verborgen. Nur seine „Freunde", also von ihm ausgewählte Nutzer, können diese Bereiche einsehen. Wenn der ermittelnde Beamte im Rahmen seiner dienstlichen Tätigkeit eine „Freundschaftsanfrage" an den Betroffenen sendet, ohne dabei seine Behördenzugehörigkeit zu eröffnen, und der Betroffene diese annimmt, verletzt der Polizist bei seiner Datener-

671 *Jandt/Roßnagel*, MMR 2011, 637.

672 Vgl. *Hornung*, CR 2008, 299, 305.

673 BVerfGE 120, 278, Absatz 311.

674 Ebenfalls kritisch zur Ansicht des Bundesverfassungsgerichts *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 99; *Hornung*, CR 2008, 299, 305; *Schulz/Hoffmann*, CR 2010, 131, 133.

675 Problematisch ist in diesem Zusammenhang auch, dass nach Angaben von *Henrichs/Wilhelm*, Kriminalistik 2010, 30, 34, die Polizisten anscheinend unter ihrem Privataccount ermitteln. Hier verschwimmen die Grenzen zwischen staatlicher Ermittlungstätigkeit und privater Kommunikation, was sehr bedenklich ist.

hebung im geschützten Bereich das Recht auf informationelle Selbstbestimmung des Betroffenen[676]. Dem Betroffenen ist nicht klar, dass eine staatliche Stelle Einsicht in seine personenbezogenen Daten nimmt. Selbst wenn der Polizist mit seinem Klarnamen handelt, kann dem Betroffenen nicht zugemutet werden, eigene Recherchen über die Tätigkeit des anfragenden Polizisten zu betreiben. Bei den teils sehr hohen Anzahlen der „Freunde" in diesen Sozialen Netzwerken wird man dies auch kaum erwarten können.

2.3.1.5.7 Datenverwendung

Neben der Datenerhebung kann die Datenverwendung, also die Verarbeitung und Nutzung der personenbezogenen Daten, einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen[677]. Indem die staatliche Stelle die erhobenen personenbezogenen Daten speichert, verändert oder nutzt, kann sie zusätzlich in die Grundrechte der Betroffenen eingreifen. Wenn bereits die Datenerhebung als Eingriff in das Recht auf informationelle Selbstbestimmung zu werten ist, muss die weitere Datenverwendung erst recht als Eingriff angesehen werden[678].

Auch bei eingriffslos erhobenen Daten kann die weitere Verwendung einen Grundrechtseingriff darstellen. Wenn die staatliche Stelle allgemein zugängliche Daten gezielt zusammenträgt, speichert und gegebenenfalls unter Hinzuziehung weiterer Daten auswertet und sich daraus eine „besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt", überschreitet dies nach Ansicht des Bundesverfassungsgerichts die Eingriffsschwelle[679]. Ein solcher Fall kann beispielsweise vorliegen, wenn die staatliche Stelle gezielt Daten über eine bestimmte Person im Internet sammelt, diese speichert und ein Profil über diese Person anlegt.

Zusätzlich kann eine Zweckänderung erhobener Daten für den Betroffenen einen Grundrechtseingriff bedeuten[680]. Generell unterliegen personenbezogene Daten dem Zweckbindungsgebot[681]. In Konkretisierung des Grundsatzes der Zweckbestimmtheit personenbezogener Daten sieht das Zweckbindungsgebot vor, dass diese Daten grundsätzlich nur zu dem Zweck gespeichert, verändert oder genutzt werden dürfen, zu dem die

676 Wohl anderer Ansicht *Graf*, in: Beck´scher Online-Kommentar StPO, § 100a, Rdnr. 32i; *Brenneisen/Staack* nehmen einen Grundrechtseingriff an bei legendierten Freundschaftsanfragen, um so personenbezogene Daten zu erhalten, die die staatliche Stelle andernfalls nicht erhielte, vgl. *Brenneisen/Staack*, Kriminalistik 2012, 627, 629.

677 Vgl. BVerfGE 78, 77, 84 ff.; *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 630; *Gusy*, Polizei- und Ordnungsrecht, 7. Aufl., 2009, Rdnr. 268.

678 So auch *Perrey*, Gefahrenabwehr und Internet, 2003, S. 150.

679 BVerfGE 120, 274, Absatz 309; vgl. auch *Bär*, MMR 2008, 325, 326 ff.; *Schulz/Hoffmann*, CR 2010, 131, 132 m. w. N.

680 *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 638.

681 Vgl. beispielsweise § 37 Abs. 2 Satz 1 PolGBW.

Daten erlangt worden sind[682]. Damit soll verhindert werden, dass die zu einem bestimmten Zweck erhobenen Daten zu einem anderen Zweck verwertet werden[683]. Hierin könnte gegebenenfalls bei der anschließenden Verwertung der im Rahmen der Polizeistreifen im Internet erhobenen Daten ein weiterer Eingriff in das Recht auf informationelle Selbstbestimmung liegen.

2.3.2 Zwischenergebnis

Der beinahe allumfassende Schutzbereich des Rechts auf informationelle Selbstbestimmung erfordert für die Ermöglichung einer effektiven Gefahrenabwehr im Internet die Einschränkung des Eingriffsbegriffs. Nicht jede Form der Erhebung von personenbezogenen Daten kann einen Eingriff darstellen. Bei der Begrenzung des Schutzes durch das Recht auf informationelle Selbstbestimmung muss auf der Eingriffsebene angesetzt werden, um nicht die Systematik dieses Rechts vollends zu verwerfen. Hierbei kann nicht nur auf die Schutzwürdigkeit des Vertrauens der Kommunikationsbeteiligten im Internet abgestellt werden, sondern vielmehr muss sich die Einschränkung nach der Art der Erhebung richten. Entscheidend ist somit die konkrete Maßnahme des ermittelnden Beamten, die sich am Recht auf informationelle Selbstbestimmung zu messen hat.

In den meisten Fällen greifen die unterschiedlichen Maßnahmen der Polizei im Rahmen ihrer verdachtsunabhängigen Ermittlungen im Internet nicht in das Recht auf informationelle Selbstbestimmung ein. Bei allen Maßnahmen müssen die staatlichen Stellen allerdings die Intensität ihrer Ermittlungen beachten. Bereits die gezielte Erhebung von personenbezogenen Daten einer bestimmten Person aus den allgemein zugänglichen oder aus den geschützten Bereichen des Internet kann einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen, soweit sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt[684]. Für den Einsatz von Suchmaschinen oder den Aufruf von öffentlich zugänglichen Inhalten müssen die ermittelnden Beamten außer dieser Einschränkung keine weiteren Vorgaben beachten, um eingriffslos zu handeln.

Differenzierter sind der Aufruf geschützter Inhalte sowie die Nutzung von Kommunikationsdiensten mit Registrierung zu betrachten. Je nach Ausgestaltung der Schutzmechanismen des Diensteanbieters zur Authentifizierung der Nutzerangaben können die staatlichen Stellen nach dem Ver-

682 Vgl. zu dieser Problematik z. B. für die Umwidmung präventiv erhobener Daten zu Zwecken der Strafverfolgung *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 641 ff.; *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 6. Aufl., 2010, § 15, Rdnr. 13 ff.; *Belz/Mußmann*, PolGBW, 7. Aufl., 2009, § 37, Rdnr. 25; *Ruder/Schmitt*, Polizeirecht, 7. Aufl., 2011, Rdnr. 476 ff.

683 Vgl. zum Streitstand, wann keine Zweckänderung vorliegt, *Wolf/Stephan/Deger*, PolGBW, 6. Aufl., 2009, § 37, Rdnr. 14 ff.

684 So zutreffend BVerfGE 120, 274, Absatz 309.

schweigen ihrer Behördeneigenschaft bei den folgenden Datenerhebungen in das Recht auf informationelle Selbstbestimmung des Diensteanbieters und der anderen Nutzer eingreifen. Eine verdeckte, aktive Kommunikation der ermittelnden Beamten mit anderen Kommunikationspartnern kann nicht eingriffslos stattfinden. Der Staat darf gerade nicht sämtliche Möglichkeiten im Internet frei nutzen, die allen Bürgern offenstehen. Eine staatliche Identitätstäuschung im Rahmen einer aktiven Kommunikation im Internet überschreitet den Rechtsrahmen eines eingriffsfreien Handelns. Zudem muss eine ermittelnde Behörde die Besonderheiten der Sozialen Netzwerke beachten, in denen sich stabile und auf Vertrauen basierende Kommunikationsbeziehungen entwickeln.

3. Schutz der Privatsphäre

Das allgemeine Persönlichkeitsrecht gewährleistet in seiner Ausprägung als Schutz der Privatsphäre „dem Einzelnen einen räumlich und thematisch bestimmten Bereich, der grundsätzlich frei von unerwünschter Einsichtnahme bleiben soll“[685]. Der Einzelne soll sich in einem geschützten Bereich dem Einblick des Staates und auch Dritter entziehen können und sich nicht der öffentlichen Kontrolle unterwerfen müssen[686]. In diesem Bereich kann er seine Individualität entwickeln und wahren[687]. Diese engere Persönlichkeitssphäre kann in Anknüpfung an die „Sphärentheorie“ noch weiter in eine Intimsphäre und eine Privat- oder Geheimsphäre unterteilt werden[688]. Das Bundesverfassungsgericht unterscheidet einen absolut geschützten Kernbereich als unantastbaren Intimbereich und einen Bereich privater Lebensgestaltung, der im überwiegenden Interesse der Allgemeinheit unter strenger Wahrung des Verhältnismäßigkeitsgebots eingeschränkt werden darf[689].

Vom Schutzbereich der Privatsphäre können auch personenbezogene Daten im Internet umfasst sein[690]. Die personenbezogenen Daten wird man danach differenzieren müssen, ob sie die engere Persönlichkeitssphäre betreffen. Wenn der Nutzer eines Kommunikationsdienstes beispielsweise über Details aus seinem Privatleben berichtet, kann dies in den Schutzbereich der Privatsphäre fallen. Noch stärker wird der Bezug zur engen Persönlichkeitssphäre, soweit ein Blogger in seinem Blog über sein Leben

685 BVerfGE 120, 274, Absatz 197 m. w. N.

686 *Murswiek*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 2, Rdnr. 69.

687 Vgl. BVerfGE 79, 256, 268; *Manssen*, Staatsrecht II, 7. Aufl., 2010, Rdnr. 229.

688 Vgl. dazu mit den unterschiedlichen Ausprägungen nur *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 149 ff.; *Starck*, in: v. Mangoldt/Klein/Starck, Grundgesetz, Bd. 1, 6. Aufl., 2010, Art. 2 Abs. 1, Rdnr. 86 ff.

689 Vgl. BVerfGE 96, 56, 61; 80, 367, 374; siehe zu Intimsphäre und Kernbereichsschutz zudem *Desoi/Knierim*, DÖV 2011, 398 ff.

690 Vgl. ausführlich dazu *Perrey*, Gefahrenabwehr und Internet, 2003, S. 136 ff.

berichtet. Bei den genannten und auch weiteren Nutzungsmöglichkeiten des Internet können die Privatsphäre oder sogar die Intimsphäre einer Person betroffen sein[691].

In welchen Fällen ein Eingriff in die Privatsphäre vorliegt, ist differenziert zu betrachten. Da die personenbezogenen Daten der Privat- und Intimsphäre dem Schutz des Rechts auf informationelle Selbstbestimmung unterfallen, kann für mögliche Eingriffe auf die obigen Ausführungen zum Recht auf informationelle Selbstbestimmung verwiesen werden. Für Daten aus der Privat- oder Intimsphäre steigt aber die Eingriffsintensität, soweit ein Eingriff vorliegt.

Insbesondere bei Datenerhebungen aus frei zugänglichen Quellen des Internet greift ein ermittelnder Polizist aber noch nicht in die engere Persönlichkeitssphäre des Betroffenen ein[692]. Allenfalls bei einer erkennbar unberechtigten Veröffentlichung von Daten durch einen Dritten aus der Privat- oder Intimsphäre einer anderen Person könnte ein weitergehender Schutz durch diese Ausprägung des allgemeinen Persönlichkeitsrechts vorliegen[693]. Ein solcher Fall könnte beispielsweise gegeben sein, wenn das Tagebuch einer Person durch einen Dritten unberechtigt im Internet veröffentlicht würde und dies für einen ermittelnden Polizisten offensichtlich wäre. In diesem Fall ständen dem Polizisten aber bereits weitere polizeirechtliche Befugnisse zur Datenerhebung zu, die einen möglichen Eingriff zur Gefahrenabwehr oder sogar zur Strafverfolgung rechtfertigen würden.

4. Recht am eigenen Wort

Durch das Recht am eigenen Wort als Ausprägung des allgemeinen Persönlichkeitsrechts wird das nichtöffentlich gesprochene Wort einer Person geschützt[694]. In der Rechtsprechung des Bundesverfassungsgerichts ist anerkannt, dass das Recht am eigenen Wort die Selbstbestimmung über die eigene Darstellung der Person in der Kommunikation mit anderen gewährleistet[695]. Geschützt wird die Möglichkeit, „sich in der Kommunikation nach eigener Einschätzung situationsangemessen zu verhalten und sich auf die jeweiligen Kommunikationspartner einzustellen“[696]. Die sprechende Person darf also auswählen, wer Zuhörer sein soll.

691 Siehe insgesamt zum Schutz des Individuums in der modernen Mediengesellschaft *Schertz*, NJW 2013, 721 ff.

692 Vgl. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 513; *Perrey*, Gefahrenabwehr und Internet, 2003, S. 147.

693 *Petri* wirft diese Frage auf, lässt sie aber auf Grund der komplexen Problemstellung offen, *Petri*, DuD 2010, 25, 29.

694 *Starck*, in: v. Mangoldt/Klein/Starck, Grundgesetz, Bd. 1, 6. Aufl., 2010, Art. 2 Abs. 1, Rdnr. 92 ff.

695 Vgl. BVerfGE 106, 28, 39; 54, 148, 155.

696 BVerfGE 106, 28, 39.

Relevant sein könnte das Recht am eigenen Wort bei den sogenannten Podcasts im Internet. Ein Eingriff durch die verdachtsunabhängigen Ermittlungen der Polizei wird für Podcasts oder andere Veröffentlichungen mit Wortbeiträgen allerdings regelmäßig ausscheiden, da die Betroffenen selbst die Veröffentlichung im Internet veranlasst haben und sich die Wortbeiträge gerade an eine unbestimmte Anzahl von Personen richten sollen. Die Betroffenen haben sich selbst dazu entschieden, ihre aufgenommene Stimme anderen zu offenbaren. Damit liegt kein nichtöffentlich gesprochenes Wort vor. Ein Eingriff in das Recht am eigenen Wort scheidet aus.

Diese Einschätzung lässt sich für die verdachtsunabhängigen Ermittlungen der Polizei auf Videoaufnahmen oder andere Bildaufzeichnungen im Internet übertragen, bei denen ein Eingriff in das Recht an eigenen Aufzeichnungen und am eigenen Bild auf Grund der freiwilligen Veröffentlichung abzulehnen ist[697].

Eine analoge Anwendung des Rechts am eigenen Wort auf die Kommunikationsdienste des Internet, etwa Webforen oder Chats, ist nicht erforderlich. Zwar entstehen bei Echtzeit-Kommunikationen ähnliche Abläufe wie bei Gesprächen, indem die Beteiligten direkt ihre Beiträge schriftlich verfassen. Jedoch bietet das Recht auf informationelle Selbstbestimmung für diese Kommunikationsformen im Internet bereits einen ausreichenden Schutz.

5. Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Mit seiner Entscheidung zur Online-Durchsuchung, die auch die Internet-Aufklärung behandelt, läutete das Bundesverfassungsgericht die Geburtsstunde eines neuen Grundrechts, des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, ein[698]. Die Frage der rechtlichen Zulässigkeit der Online-Durchsuchung beschäftigte bereits im Vorfeld der Entscheidung die wissenschaftliche Diskussion[699]. Nicht nur in der Wissenschaft, sondern auch in der Öffentlichkeit gewann die Diskussion an Fahrt, da mit den Begriffen „Online-Durchsuchung“ oder auch „Bundestrojaner“[700] Unklarheiten hinsichtlich des technisch Machba-

697 Vgl. zum Recht an eigenen Aufzeichnungen und am eigenen Bild beispielsweise *Starck*, in: v. Mangoldt/Klein/Starck, Grundgesetz, Bd. 1, 6. Aufl., 2010, Art. 2 Abs. 1, Rdnr. 95 ff.

698 BVerfGE 120, 274.

699 Vgl. z. B. *Gercke*, CR 2007, 245 ff.; *Buermeyer*, HRRS 2007, 329 ff.; *Hornung*, DuD 2007, 575; *ders.*, JZ 2007, 828; *Kutscha*, NJW 2007, 1169; *Rux*, JZ 2007, 285; *Schaar/Landwehr*, K&R 2007, 202; *Schlegel*, GA 2007, 648; *Warntjen*, Jura 2007, 581; *Jahn/Kudlich*, JR 2007, 57 ff.; *Meininghaus*, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, 2007, 182 ff.

700 Der Begriff „Bundestrojaner“ hat es zumindest auf den 8. Platz bei der Wahl zum „Wort des Jahres“ gebracht, vgl. Pressemitteilung der Gesellschaft für deutsche Sprache (GfdS) vom 07.12.2007.

ren und Möglichen zusammenhingen[701]. Der Erste Senat des Bundesverfassungsgerichts entwickelte daraufhin in seinem Urteil zur Online-Durchsuchung das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Ausprägung des allgemeinen Persönlichkeitsrechts[702].

Bei der Online-Durchsuchung greift die staatliche Behörde heimlich auf ein informationstechnisches System zu[703]. Auf diesen informationstechnischen Systemen, also beispielsweise einem Rechner, können sich im Arbeitsspeicher und auf den Speichermedien eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden[704]. Der heimliche Zugriff auf den Rechner geschieht, indem eine Schadenssoftware zur Ausspähung („Trojaner") auf dem Rechner installiert wird. Technisch kann dies beispielsweise durch manipulierte Webseiten, getarnte E-Mail-Anhänge, die Ausnutzung von Sicherheitslücken beim Zielrechner oder durch manuelle Installation erfolgen[705]. Mittels des „Trojaners" kann die Behörde die vorhandenen Daten auf dem infiltrierten Rechner ausspähen oder manipulieren. Der Zugriff betrifft damit Daten, die noch nicht oder nicht mehr Gegenstand einer laufenden Kommunikation sind[706]. Diese Daten sind nicht durch das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG geschützt, da sie nicht die Inhalte oder Umstände einer laufenden Telekommunikation betreffen[707]. Da auch Art. 13 Abs. 1 GG[708] sowie die bisherigen Ausprägungen des allgemeinen Persönlichkeitsrechts, insbesondere die Gewährleistung des Schutzes der Privatsphäre und des Rechts auf informationelle

701 Vgl. *Böckenförde*, JZ 2008, 925.

702 BVerfGE 120, 274. Vgl. weiterführend *Herrmann*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, 2010; *Sachs/Krings*, JuS 2008, 481; *Roggan*, Online-Durchsuchung, 2008; *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 118 ff.; *Wegener/Muth*, Jura 2010, 847; *Leisner*, NJW 2008, 2902; *Volkmann*, DVBl. 2008, 590 ff.; *Britz*, DÖV 2008, 411; *Kutscha*, NJW 2008, 1042; *Böckenförde*, JZ 2008, 925; *Bartsch*, CR 2008, 613; *Hornung*, CR 2008, 299; *Stögmüller*, CR 2008, 435; *Heckmann*, in: Kluth u. a., FS Rolf Stober, 2008, S. 615; *Bär*, MMR 2008, 325; *Roßnagel/Schnabel*, NJW 2008, 3534 ff.; *Hoffmann-Riem*, JZ 2008, 1009 ff.

703 Siehe zu den Ermächtigungsgrundlagen nach dem Polizeirecht des Bundes und der Länder *Soiné*, NVwZ 2012, 1585 ff.

704 BVerfGE 120, 274, Absatz 178.

705 Vgl. *Hsieh*, E-Mail-Überwachung zur Gefahrenabwehr, 2011, S. 53.

706 Vgl. zur Abgrenzung der Online-Durchsuchung von der Quellen-Telekommunikationsüberwachung die Begründung zum BKA-Gesetz, BT-Drs 16/9588, S. 26 ff.

707 Vgl. BVerfGE 120, 274, Absätze 183 ff.

708 Eine Verletzung des Art. 13 Abs. 1 GG lehnt das Bundesverfassungsgericht zutreffend ab, da informationstechnische Systeme mobil sein können (z. B. Notebooks, Mobiltelefone) und Art. 13 Abs. 1 GG zudem nicht vor der durch Infiltrierung des Systems ermöglichten Erhebung der Daten auf den Speichermedien des Rechners, der sich in einer Wohnung befindet, schützt, vgl. BVerfGE 120, 274, Absätze 194 ff.

Selbstbestimmung, nicht in ausreichendem Maße dem besonderen Schutzbedürfnis des Nutzers eines informationstechnischen Systems genügen[709], greift das Bundesverfassungsgericht auf das neue Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zurück[710].

Für den schwerwiegenden Eingriff durch die Online-Durchsuchung verlangt das Bundesverfassungsgericht zur verfassungsrechtlichen Zulässigkeit tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut[711]. Überragend wichtig seien dabei Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren[712].

Die verdachtsunabhängigen Ermittlungen der Polizei im Internet greifen nicht in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein, da die staatlichen Stellen nicht die auf den Rechnern separat gespeicherten Daten ausspähen oder manipulieren[713]. Die ermittelnden Polizisten nutzen lediglich die direkt über das Internet abrufbaren Dienste. Damit scheidet eine Verletzung des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus.

VI. Sonstige Grundrechte

Durch die verdachtsunabhängigen Ermittlungen der Polizei im Internet können weitere Grundrechte verletzt werden. Beispielsweise kann bei Kommunikationsdiensten die Glaubens- und Gewissensfreiheit (Art. 4 GG) betroffen sein, wenn die Polizei ein religiöses Webforum überwacht. Soweit bei den Inhalten des Internet weitergehend andere Grundrechte mit besonderem Schutzgehalt, wie etwa Art. 6 GG, zu beachten sind, können polizeiliche Maßnahmen in diese Grundrechte eingreifen[714]. Für den virtuellen Bereich ergeben sich bei diesen Grundrechten keine erheblichen Unterschiede zum Schutzumfang im „analogen" Leben. Daher wird nicht vertieft auf mögliche Verletzungen sonstiger Grundrechte eingegangen.

Unter Umständen könnten durch die Ermittlungen der Polizei die über Art. 2 Abs. 1 GG geschützte Gewerbefreiheit, die Berufsfreiheit (Art. 12 GG) sowie das durch Art. 14 Abs. 1 GG geschützte Eigentum der Dienstean-

709 Vgl. BVerfGE 120, 274, Absätze 196 ff.; kritisch dazu z. B. *Eifert*, NVwZ 2008, 521.
710 Siehe dazu auch *Luch*, MMR 2011, 75 ff.
711 Vgl. BVerfGE 120, 274, Absätze 247 ff.; weiterführend dazu *Soiné*, NVwZ 2012, 1585 ff.
712 Vgl. BVerfGE 120, 274, Absatz 247.
713 Vgl. die Antwort der Bundesregierung vom 14.07.2011 auf eine Kleine Anfrage zur Nutzung Sozialer Netzwerke zu Fahndungszwecken, BT-Drs 17/6587.
714 Vgl. *Schulz/Hoffmann*, CR 2010, 131, 136.

bieter betroffen sein[715]. Für eine Verletzung dieser Grundrechte bereits durch die verdachtsunabhängigen Ermittlungen der Polizei im Internet bestehen keine Anhaltspunkte. Diese Grundrechte können aber bei späteren Maßnahmen, wie etwa der Sperrung von Webseiten, relevant sein[716].

VII. Ergebnis

Die Maßnahmen der Polizei bei ihren verdachtsunabhängigen Ermittlungen im Internet greifen in der Regel nicht in Grundrechte ein. Lediglich das Recht auf informationelle Selbstbestimmung kann – abgesehen von besonderen Ausnahmefällen, in denen in andere Grundrechte eingegriffen wird – durch bestimmte Maßnahmen betroffen sein. Allerdings stellt nicht jede Form der Erhebung von personenbezogenen Daten einen Eingriff dar. Entscheidend für die Frage, wann ein Grundrechtseingriff vorliegt, ist die konkrete Maßnahme des ermittelnden Beamten, die sich am Recht auf informationelle Selbstbestimmung zu messen hat.

In den meisten Fällen greifen die unterschiedlichen Maßnahmen der Polizei im Rahmen ihrer verdachtsunabhängigen Ermittlungen im Internet nicht in das Recht auf informationelle Selbstbestimmung ein. Bei allen Maßnahmen müssen die staatlichen Stellen die Intensität ihrer Ermittlungen beachten. Bereits die gezielte Erhebung von personenbezogenen Daten einer bestimmten Person aus den allgemein zugänglichen oder aus den geschützten Bereichen des Internet kann in das Recht auf informationelle Selbstbestimmung eingreifen, soweit sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt[717]. In welchen Fällen eine besondere Gefahrenlage für die Persönlichkeit eines Betroffenen besteht, kann nur einzelfallbezogen entschieden werden. Maßgeblich sind beispielsweise die Intensität und die Dauer der staatlichen Datenerhebungen. Eine langfristige Überwachung der Beiträge des Betroffenen in Webforen kann zum Beispiel zu einer besonderen Gefahrenlage für die Persönlichkeit des Betroffenen führen. Für den Aufruf von öffentlich zugänglichen Inhalten des Internet oder den Einsatz von Suchmaschinen müssen die ermittelnden Beamten außer der Einschränkung, dass sich keine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt, keine weiteren Vorgaben beachten, um eingriffslos zu handeln.

Die Nutzung von Kommunikationsdiensten mit Registrierung ist differenzierter zu betrachten. Je nach Ausgestaltung der Schutzmechanismen des Diensteanbieters zur Authentifizierung der Nutzerangaben können die

715 *Bär*, MMR 1998, 463, 465, der aber davon ausgeht, dass die Polizisten mit einer fremden Kennung unberechtigt auf Daten zugreifen. Dies wird allerdings im Rahmen der verdachtsunabhängigen Ermittlungen der Polizei nach dem letzten Kenntnisstand nicht gemacht.

716 Vgl. beispielsweise *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, S. 61 ff.

717 So zutreffend BVerfGE 120, 274, Absatz 309.

staatlichen Stellen bei einem Verschweigen ihrer Behördeneigenschaft bei den folgenden Datenerhebungen in das Recht auf informationelle Selbstbestimmung des Diensteanbieters und der anderen Nutzer eingreifen. Die Behörde kann keine verdeckte, aktive Kommunikation mit anderen Kommunikationspartnern eingriffslos durchführen. Eine staatliche Identitätstäuschung im Rahmen einer aktiven Kommunikation im Internet überschreitet den zulässigen Rechtsrahmen für die verdachtsunabhängigen Ermittlungsmaßnahmen. In den Sozialen Netzwerken müssen die ermittelnden Polizisten außerdem die Besonderheiten der Sozialen Netzwerke beachten, in denen sich stabile und auf Vertrauen basierende Kommunikationsbeziehungen entwickeln.

E.
Rechtliche Zulässigkeit der verdachtsunabhängigen Ermittlungen im Internet

Durch das Internet sind neben der Übertragung bekannter Gefahren aus dem „analogen" Leben in die virtuelle Welt zusätzliche Gefahrenpotenziale entstanden, die von den Polizeibehörden weitestmöglich beherrscht werden sollten. Der Gesetzgeber muss den staatlichen Stellen mit entsprechenden Gesetzen zur effektiven und unverzüglichen Abwehr solcher Gefahren Werkzeuge an die Hand geben, die innerhalb der verfassungsrechtlichen Grenzen auch im Internet einen bestmöglichen Schutz privater und staatlicher Interessen sichern. Entsprechend dem Schwerpunkt der vorliegenden Abhandlung wird der rechtliche Rahmen für präventive Maßnahmen der Länderpolizeibehörden und des Bundeskriminalamtes unter Ausschluss anderer Behörden, wie etwa Bundesnachrichtendienst und Zollkriminalamt, untersucht.

Nachdem festgestellt wurde, dass bestimmte Maßnahmen der Polizei im Rahmen der verdachtsunabhängigen Ermittlungen im Internet Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen, wird im Folgenden geprüft, ob diese Eingriffe durch die bestehenden gesetzlichen Bestimmungen gerechtfertigt sind.

I. Polizeirechtliche Ermächtigungsgrundlagen

Für die polizeilichen Maßnahmen, die keine Grundrechtseingriffe darstellen, wird keine spezielle Ermächtigungsgrundlage benötigt. Bereits die gesetzlichen Aufgabenzuweisungsnormen[718] sind die ausreichenden Rechtsgrundlagen für alle der Gefahrenabwehr dienenden Tätigkeiten der Polizei, die keine Eingriffe in die Sphäre der Rechte Einzelner, insbesondere keine Grundrechtseingriffe, darstellen[719]. Aus diesem Grund sind nur für bestimmte verdachtsunabhängige Ermittlungsmaßnahmen der Polizei im Internet gesetzliche Ermächtigungsgrundlagen notwendig. Dies sind insbesondere die verdeckten Datenerhebungen der staatlichen Stellen, die in besonders zugangsgesicherten Bereichen des Internet oder bei der aktiven

718 Vgl. z. B. § 1 Abs. 1 Satz 1 PolG BW.

719 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 544 (Fn. 38); *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 36 ff.; *Zöller*, GA 2000, 563, 569; *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., 2008, § 7, Rdnr. 7; *Kugelmann*, Polizei- und Ordnungsrecht, 2006, S. 181; so auch die Bundesregierung auf eine Kleine Anfrage zur Nutzung Sozialer Netzwerke zur Fahndungszwecken, BT-Drs 17/6587, S. 3.

Beteiligung von ermittelnden Polizeibeamten in Kommunikationsdiensten erfolgen können.

1. Allgemeine Anforderungen an eine Ermächtigungsgrundlage

Der Staat ist zur Wahrnehmung der ihm obliegenden Aufgaben in hohem Maße auf personenbezogene Informationen angewiesen. Personenbezogene Daten sind beispielsweise eines der wesentlichen Elemente in der polizeilichen Gefahrenabwehr und Strafverfolgung[720]. Aus diesem Grund muss das Recht auf informationelle Selbstbestimmung Einschränkungen hinnehmen, um dem legitimen Informationsbedarf in Staat und Gesellschaft Rechnung zu tragen[721]. Eingriffe in dieses Recht bedürfen nach Art. 2 Abs. 1 GG einer verfassungsgemäßen gesetzlichen Grundlage[722]. Zwar wird für das Recht auf informationelle Selbstbestimmung als dogmatischer Ausgangspunkt, wie für das allgemeine Persönlichkeitsrecht, nach heute allgemeiner Ansicht Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG angesehen[723]. Die Verbindung von Art. 2 Abs. 1 GG und Art. 1 Abs. 1 GG hat allerdings nicht zur Folge, dass das Recht auf informationelle Selbstbestimmung uneinschränkbar ist[724]. Als subjektives Recht ist das allgemeine Persönlichkeitsrecht auf Art. 2 Abs. 1 GG zurückzuführen, während Art. 1 Abs. 1 GG auf die Rolle als Auslegungsmaßstab für die Ermittlung des Inhalts und der Reichweite des Schutzumfangs begrenzt ist[725].

Der Einzelne muss solche Beschränkungen seines Rechts hinnehmen, die durch überwiegende Allgemeininteressen gerechtfertigt sind[726]. Die Höhe der Anforderungen an die Ermächtigungsgrundlage richtet sich nach der Art und der Intensität des Grundrechtseingriffs[727]. Neben den rechtsstaatlichen Geboten der Normenklarheit und der Normenbestimmtheit kommt dem Grundsatz der Verhältnismäßigkeit eine besondere Bedeutung zu[728]. Durch das Bestimmtheitsgebot soll sichergestellt werden, dass der „demo-

720 Vgl. *Son*, Heimliche polizeiliche Eingriffe in das informationelle Selbstbestimmungsrecht, 2006, S. 83 ff.

721 *Lorenz*, in: BK, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 336.

722 BVerfGE 120, 378, 401.

723 Beispielsweise BVerfGE 27, 1, 6; 54, 148, 153; mit einer Vielzahl an weiteren Nachweisen *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 128.

724 In die Würde des Menschen im Sinne des Art. 1 Abs. 1 Satz 1 GG darf als „Wurzel aller Grundrechte“ nicht eingegriffen werden, vgl. BVerfGE 93, 266, 293.

725 Vgl. *Murswiek*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 2, Rdnr. 63; *Starck*, in: v. Mangoldt/Klein/Starck, Grundgesetz, Bd. 1, 6. Aufl., 2010, Art. 2 Abs. 1, Rdnr. 15; *Di Fabio*, in: Maunz/Dürig, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 128 m. w. N.

726 BVerfGE 115, 320, 344 ff.

727 BVerfGE 120, 378, 401; *Jarass*, in: Jarass/Pieroth, Grundgesetz, 12. Aufl., 2012, Art. 2, Rdnr. 58a.

728 Vgl. *Dreier*, in: Dreier I, 2. Aufl., 2004, Art. 2 Abs. 1, Rdnr. 86 ff.; *Lorenz*, in: BK, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 339.

kratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte eine wirksame Rechtskontrolle durchführen können“[729].

Zudem wird durch die Bestimmtheit und Klarheit des Gesetzes gewährleistet, dass sich der betroffene Bürger auf mögliche belastende Maßnahmen einstellen kann[730]. Besonders beachten muss der Gesetzgeber, dass er Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festlegt[731]. Insgesamt sind die Anforderungen an das einschränkende Gesetz relativ hoch. Je umfassender die erhobenen Daten benutzt werden sollen und je tiefer sie in den Persönlichkeitsbereich hineinreichen, desto höhere Anforderungen erfordern die Bestimmtheit und der Gesetzeszweck[732]. Die Ermächtigungsgrundlagen, die die Eingriffe in das Recht auf informationelle Selbstbestimmung rechtfertigen sollen, müssen sich an diesen strengen Maßstäben messen.

2. Bundesrechtliche Ermächtigungsgrundlagen

Das Bundeskriminalamt führt neben den Polizeibehörden der einzelnen Bundesländer verdachtsunabhängige Ermittlungen im Internet durch. Das Bundeskriminalamt als Zentralstelle darf auch im präventiv-polizeilichen Bereich Aufgaben wahrnehmen[733]. Für die verdachtsunabhängigen Ermittlungen ist zu prüfen, ob einschlägige Ermächtigungsgrundlagen im Bundeskriminalamtgesetz (BKAG) vorhanden sind und diese den strengen Anforderungen des Bundesverfassungsgerichts für Informationseingriffe genügen.

2.1 Aufgabenzuweisungsnorm (§ 2 Abs. 2 Nr. 1 i. V. m. § 2 Abs. 1 BKAG)

Als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei unterstützt das Bundeskriminalamt gemäß § 2 Abs. 1 BKAG die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung. Zur Wahrnehmung dieser Aufgabe hat das

729 BVerfGE 120, 378, 407.

730 BVerfGE 113, 348, 375 ff.; 110, 33, 52 ff.

731 BVerfG, 1 BvR 1299/05 vom 24.01.2012 (Absatz 169); BVerfGE 118, 168, 186 ff.; 110, 33, 53; 100, 313, 359 ff.

732 Vgl. *Murswiek*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 2, Rdnr. 121 m. w. N.; ähnlich *Gurlit*, NJW 2010, 1035, 1038; *Poppenhäger*, NVwZ 1992, 149 ff.

733 Vgl. die ausführliche Begründung von *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, BKAG, 2000, § 2, Rdnr. 20 ff.

Bundeskriminalamt alle hierfür erforderlichen Informationen zu sammeln und auszuwerten (vgl. § 2 Abs. 2 Nr. 1 BKAG).

Durch die Regelung in § 2 Abs. 2 Nr. 1 BKAG könnte das Bundeskriminalamt ermächtigt sein, Daten im Internet im Rahmen der verdachtsunabhängigen Ermittlungen zu erheben. § 2 Abs. 2 Nr. 1 BKAG spricht vom „Sammeln von erforderlichen Informationen". Der Begriff „Informationen" ist als umfassender Oberbegriff zu werten, weshalb auch personenbezogene Daten eingeschlossen sind[734]. Der Begriff des „Sammelns" ist noch nicht abschließend geklärt. Grundsätzlich umfasst das „Sammeln" von Informationen die Entgegennahme von Informationen, die andere Stellen bereits erhoben haben[735]. Damit wäre die aktive Datenerhebung durch das Bundeskriminalamt gemäß § 2 Abs. 2 Nr. 1 i. V. m. § 2 Abs. 1 BKAG im Internet nicht zulässig. Der Begriff des „Sammelns" ist aber in seiner ursprünglichen Auslegung zu eng gefasst. Soweit in keine Grundrechte eingegriffen wird, muss dem Bundeskriminalamt die erweiterte Möglichkeit zum „Sammeln" von Informationen zugesprochen werden. Für die eingriffslosen Fälle würde zudem bereits die grundsätzliche Aufgabenzuweisungsnorm des § 2 Abs. 2 Nr. 1 i. V. m. § 2 Abs. 1 BKAG ausreichen.

Im Ergebnis darf das Bundeskriminalamt bei seinen verdachtsunabhängigen Ermittlungen im Internet personenbezogene Daten erheben, soweit kein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt[736]. Einen Grundrechtseingriff kann diese allgemeine Aufgabenzuweisungsnorm aber nicht rechtfertigen[737].

2.2 Datenerhebung gemäß § 7 Abs. 2 Satz 1 BKAG

Gemäß § 7 Abs. 2 Satz 1 BKAG darf das Bundeskriminalamt, soweit dies zur Erfüllung seiner Aufgabe als Zentralstelle nach § 2 Abs. 2 Nr. 1 BKAG erforderlich ist, Daten zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung mittels Auskünften und Anfragen bei öffentlichen oder nicht-öffentlichen Stellen erheben.

734 Vgl. *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, BKAG, 2000, § 2, Rdnr. 32.

735 Vgl. bereits *Ahlf*, Das Bundeskriminalamt als Zentralstelle, 1985, S. 310 ff. m. w. N.; *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, BKAG, 2000, § 2, Rdnr. 33.

736 Vgl. *Schmidt-Jortzig*, Ermittlungskompetenzen des BKA, 2009, S. 54; *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, BKAG, 2000, § 7, Rdnr. 6, der sich ausdrücklich auf das „Surfen im Internet" bezieht.

737 So auch *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, BKAG, 2000, § 7, Rdnr. 6. Dessen ist sich das Bundeskriminalamt auch selbst bewusst, vgl. die Informationen zur Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) unter *http://www.bka.de/*. Darin heißt es: „Das gezielte Umgehen von Zugangsbeschränkungen mittels besonderer Techniken und/oder die Erhebung von Informationen mittels verdeckter Ermittlungen gleichzusetzender Methoden sind durch § 2 Abs. 1 und 2 BKAG nicht gedeckt und sind daher keine Mittel der anlassunabhängigen Recherche."

Diese Ermächtigungsgrundlage kann die verdachtsunabhängigen Ermittlungen der Polizei im Internet aus verschiedenen Gründen nicht rechtfertigen. Zunächst darf das Bundeskriminalamt die Daten nur „zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung" erheben. Für die erste Alternative müssen beim Bundeskriminalamt bereits entsprechende Informationen („vorhandene Sachverhalte") vorliegen, die ergänzungsbedürftig sind[738]. Da die Ermittlungen des Bundeskriminalamts verdachtsunabhängig sind, liegen diese erweiterungsbedürftigen Informationen in der Regel gerade noch nicht vor. Vielmehr sollen erst Daten im Internet erhoben werden.

Die zweite Alternative sieht die Datenerhebung zu Zwecken der Auswertung vor. Davon sind keine Datenerhebungen im Rahmen von Polizeistreifen im Internet einbezogen, da der Sinn und Zweck der Vorschrift dies nicht umfasst. Die Überschrift des § 7 BKAG „Führung kriminalpolizeilicher personenbezogener Sammlungen der Zentralstelle" deutet bereits darauf hin, dass mit § 7 Abs. 2 Satz 1 BKAG keine weitgehenden Datenerhebungen legitimiert werden sollen. Die Datenerhebungen sollen durch Auskünfte und Anfragen bei öffentlichen und nicht-öffentlichen Stellen erfolgen. Daraus ergibt sich, dass die Datenerhebung zu Zwecken der Auswertung, etwa zur Anfertigung von Statistiken oder Berichten, erfolgen soll. Das Bundeskriminalamt soll so beispielsweise Finanz- und Steuerbehörden, das Ausländerzentralregister, Fluggesellschaften oder andere private Unternehmen und Verbände unmittelbar um Auskünfte ersuchen[739]. Eine verdachtsunabhängige Erhebung personenbezogener Daten im Internet, bei der zudem noch in den Kommunikationsdiensten Daten erst erzeugt werden, ist von dem Auswertungszweck nicht mehr erfasst[740].

Dass § 7 Abs. 2 Satz 1 BKAG für die möglichen Grundrechtsverletzungen im Rahmen der verdachtsunabhängigen Ermittlungen im Internet keine Ermächtigungsgrundlage darstellen kann, ergibt sich auch aus der Art der Erhebung. Das Bundeskriminalamt erhebt die Daten mittels „Auskünften oder Anfragen". In beiden Fällen liegt eine offene Datenerhebung vor. Eine verdeckte Datenerhebung, wie sie durch die aktive Teilnahme von Polizisten in Webforen beispielsweise erfolgen kann, wäre keinesfalls gerechtfertigt[741].

738 Vgl. *Ahlf*, in: Ahlf/Daub/Lersch/Störzer, BKAG, 2000, § 7, Rdnr. 9.

739 *Würtenberger*, Das Polizei- und Sicherheitsrecht vor den Herausforderungen des Terrorismus, in: Masing/Jouanjan, Terrorismusbekämpfung, Menschenrechtsschutz und Föderation, 2008, S. 31.

740 Vgl. dazu auch *Hofmann*, der in der durch die Novellierung des BKAG vereinfachten Datenerhebung für Auswerteprojekte lediglich die Beschleunigung dieser Aufgaben, aber gerade keine neuen Informationserhebungskompetenzen für das BKA sieht, *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Hopfauf, Grundgesetz, 12. Aufl., 2011, Art. 1, Rdnr. 57.

741 Vgl. *Kant*, CILIP 71 (1/2002), 29, 35.

Die Regelung des § 7 Abs. 2 Satz 1 BKAG passt insgesamt auf Grund ihrer Tatbestandsvoraussetzungen nicht zu den verdachtsunabhängigen Maßnahmen des Bundeskriminalamts im Internet. Zudem kann sie nicht den strengen Vorgaben des Bundesverfassungsgerichts zur Rechtfertigung von Eingriffen in das Recht auf informationelle Selbstbestimmung genügen, da sie den hohen Anforderungen an Normenklarheit und Normenbestimmtheit nicht genügt.

2.3 Datenerhebungen zur Terrorismusabwehr (§ 20a ff. BKAG)

Durch § 4a BKAG wurde dem Bundeskriminalamt als neue Aufgabe die Abwehr von Gefahren des internationalen Terrorismus zugewiesen[742]. Gemäß § 4a Abs. 1 BKAG kann das Bundeskriminalamt die Aufgabe der Abwehr von Gefahren des internationalen Terrorismus in Fällen wahrnehmen, in denen eine länderübergreifende Gefahr vorliegt (Nr. 1), die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist (Nr. 2) oder die oberste Landesbehörde um eine Übernahme ersucht (Nr. 3).

Die meisten der Befugnisregelungen zur Terrorismusabwehr gehen von dem Bestehen einer Gefahr aus[743]. Die Gefahr im Sinne des Unterabschnitts 3a „Abwehr von Gefahren des internationalen Terrorismus“ des BKAG wird gemäß § 20a BKAG als „eine im Einzelfall bestehende Gefahr für die öffentliche Sicherheit im Zusammenhang mit Straftaten gemäß § 4a Abs. 1 Satz 2 BKAG“ definiert. Damit muss es sich um eine konkrete Gefahr handeln[744]. Für die mit Grundrechtseingriffen verbundenen verdachtsunabhängigen Ermittlungen des Bundeskriminalamts im Internet scheiden die Ermächtigungsnormen des BKAG zur Terrorismusabwehr aus, die von einer Gefahr ausgehen. Eine konkrete Gefahr besteht gerade noch nicht im Rahmen der verdachtsunabhängigen Ermittlungen, sondern kann allenfalls entdeckt werden.

Fraglich ist, ob Maßnahmen der Verdachtsgewinnung, zu denen die verdachtsunabhängigen Ermittlungen der Polizei im Internet gehören, an die Voraussetzungen einer konkreten Gefahr gebunden sind. Insoweit wird vertreten, dass gerade noch keine konkrete Gefahr eingetreten sein muss, da die Maßnahmen zunächst der Verdachtsgewinnung dienen[745]. Einschränkend wird aber auch nach dieser Ansicht verlangt, dass eine über eine „allge-

742 Vgl. insgesamt dazu *Bäcker*, Terrorismusabwehr durch das Bundeskriminalamt, 2009; *Baum/Schantz*, ZRP 2008, 137 ff.; *Schmidt-Jortzig*, Ermittlungskompetenzen des BKA, 2009, S. 134 ff.; *Wolff*, DÖV 2009, 597 ff.; *Roggan*, NJW 2009, 257 ff.

743 Vgl. dazu auch *Schmidt-Jortzig*, Ermittlungskompetenzen des BKA, 2009, S. 134.

744 Vgl. die Begründung zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 17.06.2008, BT-Drs 16/9588, S. 20; *Bäcker*, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 65.

745 Vgl. *Bull*, Grundsatzentscheidungen zum Datenschutz bei den Sicherheitsbehörden, in: Möllers/van Ooyen, Bundesverfassungsgericht und Öffentliche Sicherheit, 2011, 65, 86; *Welsing*, Das Recht auf informationelle Selbstbestimmung im Rahmen der Terrorabwehr, 2009, S. 323.

meine Bedrohungslage“ hinausgehende Situation vorliegen muss, die weitere Tatsachen enthält, „aus denen sich eine konkrete Gefahr, etwa für die Vorbereitung oder Durchführung terroristischer Anschläge“, ergibt[746]. Für die verdachtsunabhängigen Ermittlungen im Internet liegen noch keine Tatsachen vor, aus denen sich eine konkrete Gefahr ergibt. Vielmehr werden erst Tatsachen, die eine konkrete Gefahr begründen können, durch die Datenerhebungen im Internet gesammelt. Daher wäre der selbst eingeschränkte Begriff der konkreten Gefahr hier nicht einschlägig.

Die Befragung gemäß § 20c Abs. 1 Satz 1 BKAG kommt nicht in Betracht, da für die Befragung einer Person Tatsachen die Annahme rechtfertigen müssen, dass die Person sachdienliche Angaben für die Erfüllung der dem Bundeskriminalamt nach § 4a Abs. 1 Satz 1 BKAG obliegenden Aufgabe machen kann. Entsprechend der Gesetzesbegründung ist eine ungezielte Befragung ohne konkreten Anlass oder eine allgemeine Ausforschung nach der Vorschrift nicht zulässig[747]. Bei einer verdachtsunabhängigen Ermittlung liegen noch keine Tatsachen vor, die sachdienliche Angaben einer bestimmten Person erwarten lassen. Zudem ist die Befragung eine offene und keine verdeckte Datenerhebung[748].

Die weiteren Rechtsgrundlagen für Datenerhebungen des Unterabschnitts 3a „Abwehr von Gefahren des internationalen Terrorismus“ des BKAG setzen zumeist entweder eine konkrete Gefahr voraus oder andere besondere Tatbestandsmerkmale, die für verdachtsunabhängige Ermittlungen des Bundeskriminalamts eindeutig nicht vorliegen.

Für die Datenerhebungen des Bundeskriminalamts im Internet könnte § 20b Abs. 1 BKAG die notwendige Rechtsgrundlage darstellen. Danach kann das Bundeskriminalamt, sofern in dem Unterabschnitt 3a nichts anderes bestimmt ist, personenbezogene Daten erheben, soweit dies zur Erfüllung der ihm nach § 4 Abs. 1 BKAG obliegenden Aufgabe erforderlich ist. § 20b BKAG ist für die Erhebung personenbezogener Daten durch das Bundeskriminalamt im Bereich der Terrorismusabwehr die Grundnorm[749]. Mit dieser allgemeinen Generalklausel werden dem Bundeskriminalamt weitreichende Maßnahmen zur Datenerhebung ermöglicht. Nach Ansicht von Bäcker muss die Datenerhebung zwar dem Ziel der Terrorismusabwehr dienen, jedoch ist nicht Voraussetzung, dass eine solche Straftat im Einzelfall absehbar ist[750]. Damit könnte diese Generalklausel zur Datenerhebung

746 *Bull*, Grundsatzentscheidungen zum Datenschutz bei den Sicherheitsbehörden, in: Möllers/van Ooyen, Bundesverfassungsgericht und Öffentliche Sicherheit, 2011, 65, 86.

747 Vgl. die Begründung zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 17.06.2008, BT-Drs 16/9588, S. 21.

748 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 579 ff.

749 Vgl. die Begründung zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 17.06.2008, BT-Drs 16/9588, S. 20.

750 *Bäcker*, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 70.

grundsätzlich die Vorfeldmaßnahmen des Bundeskriminalamts auf dem Gebiet der Terrorismusabwehr im Internet rechtfertigen.

§ 20b Abs. 3 BKAG verweist allerdings auf § 21 Abs. 3 und 4 Bundespolizeigesetz (BPolG), der entsprechend gelten soll. Nach § 21 Abs. 3 Satz 3 BPolG ist eine Datenerhebung, die nicht als Maßnahme der Bundespolizei erkennbar ist, nur zulässig, wenn auf andere Weise die Erfüllung der der Bundespolizei obliegenden Aufgaben erheblich gefährdet wird oder wenn anzunehmen ist, dass dies dem überwiegenden Interesse der betroffenen Person entspricht. § 21 Abs. 3 Satz 3 BPolG gilt damit für verdeckte Maßnahmen und entsprechend für die Datenerhebungen des Bundeskriminalamts gemäß § 20b BKAG. Da die verdeckten Maßnahmen der verdachtsunabhängig ermittelnden Beamten im Internet nicht dem überwiegenden Interesse der Betroffenen entsprechen, müsste ohne die verdeckten Maßnahmen die Erfüllung der Aufgaben des Bundeskriminalamts erheblich gefährdet werden. Eine Gefährdung der Aufgabenerfüllung liegt dann vor, soweit eine hinreichende Wahrscheinlichkeit besteht, dass sich durch die Datenerhebung beim Betroffenen eine abzuwehrende Gefahr verwirklichen würde[751]. Da für die verdeckten Maßnahmen sogar eine „erhebliche" Gefährdung der Aufgabenerfüllung gegeben sein muss, liegt eine noch höhere Wahrscheinlichkeitsstufe der Gefahrverwirklichung vor. Für verdachtsunabhängige Ermittlungen, bei denen noch kein Gefahrenverdacht vorliegt, kann daher eine verdeckte polizeiliche Datenerhebung zur Terrorismusabwehr nicht auf § 20b Abs. 1 BKAG gestützt werden. Insgesamt kann die Generalklausel des § 20b Abs. 1 BKAG außerdem nur Eingriffe in das Recht auf informationelle Selbstbestimmung von geringem Gewicht rechtfertigen[752].

Im Ergebnis sind verdeckte verdachtsunabhängige Ermittlungen des Bundeskriminalamts im Internet auf dem Gebiet der Terrorismusabwehr nicht gerechtfertigt.

2.4 Datenerhebungen zum Schutz von Mitgliedern der Verfassungsorgane (§ 22 Satz 1 BKAG)

Das Bundeskriminalamt kann gemäß § 22 Satz 1 BKAG personenbezogene Daten erheben, soweit dies zur Erfüllung seiner Aufgaben nach § 5 BKAG erforderlich ist. § 22 Satz 2 BKAG verweist wieder auf eine entsprechende Geltung des § 21 Abs. 3 und 4 BPolG. Damit müsste zur Rechtfertigung verdeckter Maßnahmen eine erhebliche Gefährdung der Aufgabenerfüllung des Bundeskriminalamts vorliegen, die für verdachtsunabhängige Ermittlungen im Internet nicht gegeben ist. Außerdem ermitteln die Beamten im Internet nach derzeitigem Kenntnisstand nicht verdachtsunabhängig zum Personenschutz von Mitgliedern der Verfassungsorgane.

751 Vgl. *Blümel/Drewes/Malmberg/Walter*, BPolG, 3. Aufl., 2006, § 21, Rdnr. 31.
752 Vgl. *Bäcker*, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 70.

2.5 Ergebnis

Die verdeckten verdachtsunabhängigen Maßnahmen im Internet, die einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen, sind nach dem geltenden BKAG unzulässig. Das Bundeskriminalamt darf aber die öffentlich zugänglichen Inhalte des Internet überwachen und Suchmaschinen nutzen. Zudem darf es offen die geschützten Bereiche des Internet einsehen. Kommunikationsdienste ohne besondere Verifizierungsverfahren dürfen die ermittelnden Beamten beobachten, ohne ihre Behördenzugehörigkeit offenzulegen. Dies gilt auch für die sonstigen geschützten Internetinhalte, die keine qualifizierten Registrierungsverfahren mit Verifizierung der Angaben des interessierten Nutzers vorsehen. Eine verdeckte, aktive Kommunikation der ermittelnden Beamten mit anderen Kommunikationspartnern in den Kommunikationsdiensten des Internet ist für Beamte des Bundeskriminalamts im Rahmen der verdachtsunabhängigen Ermittlungen nicht zulässig[753]. Bei allen Maßnahmen müssen die staatlichen Stellen zudem die Intensität ihrer Ermittlungen beachten. Bereits die gezielte Erhebung von personenbezogenen Daten einer bestimmten Person aus den allgemein zugänglichen oder aus den geschützten Bereichen des Internet kann einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen, soweit sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt[754]. Hierfür sieht das BKAG für verdachtsunabhängige Ermittlungen keine Ermächtigungsgrundlage vor.

3. Landesrechtliche Ermächtigungsgrundlagen

Für die verschiedenen Bundesländer sehen die jeweiligen Polizeigesetze unterschiedliche Ermächtigungsgrundlagen für Datenerhebungen vor. Nur für die Maßnahmen der ermittelnden Polizisten im Internet, die einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen, wird eine spezielle Ermächtigungsnorm benötigt. Für die eingriffslosen Datenerhebungen stellen bereits die gesetzlichen Aufgabenzuweisungsnormen ausreichende Rechtsgrundlagen für alle der Gefahrenabwehr dienenden Tätigkeiten der Polizei dar[755].

753 Bereits die Mitarbeiter der Projektgruppe unter dem Arbeitstitel „Erfordernis, Organisation und Koordination von anlassunabhängigen Recherchen im Internet“, die auf Grund eines Beschlusses der Innenministerkonferenz vom Mai 1998 eingesetzt wurde, kamen zu dem Ergebnis, dass das BKAG keine rechtliche Grundlage für diese verdeckten Datenerhebungen vorsehen würde, vgl. *Siegert*, Das Internet – Grundlagenwissen für die Polizei, 2002, S. 232.

754 So zutreffend BVerfGE 120, 274, Absatz 309.

755 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 544 (Fn. 38); *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 36 ff.; *Zöller*, GA 2000, 563, 569; *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., 2008, § 7, Rdnr. 7; *Kugelmann*, Polizei- und Ordnungsrecht, 2006, S. 181. Vgl. zur Aufgabenzuweisung an das LKA die §§ 10 ff. DVO PolG BW.

3.1 Baden-Württemberg

Für die Polizeibehörden kommen zunächst die besonderen Bestimmungen für Datenerhebungen im 3. Unterabschnitt des Polizeigesetzes Baden-Württemberg (PolG BW) in Betracht. In § 19 PolG BW werden die allgemeinen Regeln der Datenerhebung dargestellt. Gemäß § 19 Abs. 1 Satz 1 PolG BW sind personenbezogene Daten, soweit sie nicht aus allgemein zugänglichen Quellen entnommen werden, bei dem Betroffenen mit seiner Kenntnis zu erheben. § 19 Abs. 1 Satz 1 PolG BW macht also eine Ausnahme von dem Unmittelbarkeitsgrundsatz für Datenerhebungen, wenn die Daten aus einer allgemein zugänglichen Quelle erhoben werden. Eine Quelle ist allgemein zugänglich, wenn sie technisch geeignet und dazu bestimmt ist, der Allgemeinheit, das heißt einem individuell nicht bestimmten Personenkreis, Informationen zu beschaffen[756]. Zu diesen Quellen zählen Medien aller Art[757]. Damit sind auch die offen zugänglichen Quellen des Internet umfasst.

§ 19 Abs. 2 Satz 1 PolG BW entspricht dem Grundsatz der offenen Datenerhebung[758]. Eine verdeckte Datenerhebung ist nur zulässig, „wenn sonst die Wahrnehmung der polizeilichen Aufgabe gefährdet oder nur mit unverhältnismäßig hohem Aufwand möglich oder wenn anzunehmen ist, dass dies den überwiegenden Interessen des Betroffenen entspricht“[759]. § 19 PolG BW selbst stellt keine eigene Ermächtigungsgrundlage dar, sondern gibt allgemeine Grundsätze vor, die bei Anwendung der nachfolgenden Regelungen grundsätzlich zu beachten sind[760].

Für die verdachtsunabhängigen Ermittlungen im Internet ist daher zu prüfen, ob die polizeirechtlichen Bestimmungen zur Datenerhebung die möglichen Grundrechtseingriffe rechtfertigen können. Hierfür kommen verschiedene Ermächtigungsgrundlagen in Betracht.

3.1.1 Datenerhebung unter Einsatz Verdeckter Ermittler (§ 22 Abs. 3 PolG BW)

Gemäß § 22 Abs. 3 PolG BW in seiner ersten Alternative kann der Polizeivollzugsdienst personenbezogene Daten durch den Einsatz Verdeckter Ermittler zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit und Freiheit einer Person oder für bedeutende fremde Sach- und Vermögenswerte über die in § 20 Abs. 2 PolG BW genannten Personen erheben, wenn andernfalls die Wahrnehmung seiner Aufgaben gefährdet oder erheblich erschwert würde.

---

756 BVerfGE 103, 44, 60; 27, 71, 83; *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 19, Rdnr. 4.

757 *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 19, Rdnr. 4.

758 Siehe dazu auch *Tischer*, Das System der informationellen Befugnisse der Polizei, 2004, S. 350 ff.

759 § 19 Abs. 2 Satz 2 PolG BW.

760 *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 19, Rdnr. 3; *Belz/Mußmann*, PolG BW, 7. Aufl., 2009, § 19, Rdnr. 1.

Bei der verdeckten Teilnahme der Polizei in den Kommunikationsforen handelt es sich zwar nicht unbedingt um Verdeckte Ermittler, jedoch wären die verdeckten Maßnahmen dann erst recht zulässig, wenn selbst der Einsatz eines Verdeckten Ermittlers rechtmäßig wäre. Insgesamt führt der Einsatz der besonderen Mittel zur Datenerhebung zu intensiveren Grundrechtseingriffen, die höhere Zulässigkeitsvoraussetzungen notwendig machen[761]. Daher setzt der Einsatz besonderer Mittel im Sinne des § 22 Abs. 3 Nr. 1 PolG BW zumindest eine konkrete Gefahr voraus[762]. Für die verdachtsunabhängigen Ermittlungen im Internet liegt gerade noch keine konkrete Gefahr vor, weshalb § 22 Abs. 3 Nr. 1 PolG BW als Ermächtigungsgrundlage für die verdeckten Datenerhebungen der Polizei ausscheidet. Zudem wird in der Regel auch keine der Tatbestandsalternativen für eine qualifizierte Gefahr, wie etwa für Leben, Gesundheit und Freiheit einer Person, vorliegen. Während die Polizei beispielsweise ein Webforum überwacht, kann sich aber die Lage zu einer konkreten Gefahr entwickeln, die den Einsatz eines Verdeckten Ermittlers rechtfertigt. Zu Beginn der verdachtsunabhängigen Datenerhebungen ist eine solche Gefahrenlage aber noch nicht gegeben.

Die zweite Alternative in § 22 Abs. 3 PolG BW sieht den Einsatz eines Verdeckten Ermittlers zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung über die in § 20 Abs. 3 Nr. 1 und 2 PolG BW genannten Personen als besonderes Mittel zur Datenerhebung vor. Diese Datenerhebungen im Vorfeld der Gefahr dürfen nur eingesetzt werden, um Daten über künftige Straftäter nach § 20 Abs. 3 Nr. 1 PolG BW und deren Kontakt- und Begleitpersonen nach § 20 Abs. 3 Nr. 2 PolG BW zu erheben[763]. Hierfür müssen die polizeilichen Zielpersonen konkret oder zumindest ausreichend konkretisierbar benannt werden[764]. Da für die verdachtsunabhängigen Ermittlungen im Internet noch keine konkreten Indizien und erst recht noch keine bestimmten Zielpersonen bekannt sind, kann sich die Polizei für diese Ermittlungsmaßnahmen nicht auf § 22 Abs. 3 Nr. 2 PolG BW berufen[765].

3.1.2 Befragung (§ 20 Abs. 1 PolG BW)

Die Polizei kann gemäß § 20 Abs. 1 PolG BW jede Person befragen, wenn anzunehmen ist, dass sie sachdienliche Angaben machen kann, die zur Wahrnehmung einer bestimmten polizeilichen Aufgabe erforderlich sind (§ 20 Abs. 1 Satz 1 PolG BW). Für die verdeckten Ermittlungen der Polizei im Internet, beispielsweise die aktive Teilnahme in Webforen, scheidet

761 Vgl. *Belz/Mußmann*, PolG BW, 7. Aufl., 2009, § 22, Rdnr. 25.

762 Vgl. *Ruder/Schmitt*, Polizeirecht, 7. Aufl., 2011, Rdnr. 440; *Belz/Mußmann*, PolG BW, 7. Aufl., 2009, § 22, Rdnr. 26.

763 Vgl. dazu auch *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 22, Rdnr. 22 ff.

764 Vgl. VGH BW, DVBl. 1995, 367; BVerwG, NJW 1997, 2534.

765 Zusätzlich sucht die Polizei im Internet auch nicht nur nach möglichen Straftaten von erheblicher Bedeutung. Vgl. dazu den Straftatenkatalog unter § 22 Abs. 5 PolG BW.

diese Ermächtigungsgrundlage aus, da die Befragung eine offene Datenerhebung darstellt[766]. Zudem müssen die Angaben zur Wahrnehmung einer bestimmten polizeilichen Aufgabe sein. Dies setzt zwar keine konkrete Gefahr voraus, aber eine konkrete aktuelle Aufgabe, also den Bezug zu einem bestimmten Anlass[767]. Ferner ist anzunehmen, dass die befragte Person sachdienliche Angaben zu dem bestimmten Anlass machen kann. Eine grundlose Befragung „ins Blaue hinein" ist dementsprechend unzulässig[768]. Soweit die ermittelnde Stelle beispielsweise in einem Kommunikationsdienst des Internet mit anderen Beteiligten kommuniziert, wird zumindest zu Beginn der Kommunikation noch kein bestimmter Anlass gegeben sein, zu dem der Kommunikationspartner sachdienliche Angaben machen könnte. Insgesamt kann sich die Polizei bei den verdeckten Maßnahmen im Internet nicht auf § 20 Abs. 1 Satz 1 PolG BW berufen.

3.1.3 Datenerhebungsgeneralklausel zur Gefahrenabwehr (§ 20 Abs. 2 PolG BW)

Die Polizei kann gemäß § 20 Abs. 2 PolG BW Daten von Handlungs- und Zustandsstörern (§§ 6 und 7 PolG BW) sowie anderen Personen erheben, soweit dies zur Abwehr einer Gefahr oder zur Beseitigung einer Störung der öffentlichen Sicherheit oder Ordnung erforderlich ist und die Befugnisse der Polizei nicht anderweitig geregelt sind. Durch diese zentrale Ermächtigungsgrundlage der Datenerhebung im Polizeirecht Baden-Württembergs besitzt die Polizei ein umfassendes Datenerhebungsrecht zur Gefahrenabwehr und Störungsbeseitigung[769]. Da für die verdachtsunabhängigen Ermittlungen der Polizei im Internet noch keine Störung[770] vorliegt, die beseitigt werden soll, sondern erst eine Gefahrenverdachtssuche durchgeführt wird, scheidet diese Alternative aus.

Damit die Grundrechtseingriffe der Polizei im Internet gerechtfertigt werden könnten, müssten die Datenerhebungen „zur Abwehr einer Gefahr" erfolgen. § 20 Abs. 2 PolG BW verlangt somit das Vorliegen einer „konkreten Gefahr"[771]. Eine konkrete Gefahr „ist eine Sachlage, die bei ungehindertem, nach Prognose der Polizei zu erwartendem Geschehensablauf in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einem Schaden führen

766 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 579 ff.

767 *Belz/Mußmann*, PolG BW, 7. Aufl., 2009, § 20, Rdnr. 8.

768 *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 20, Rdnr. 4; *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 581; ähnlich *Rachor*, in: Lisken/Denninger, HbPolR, 5. Aufl., 2012, Kap. E, Rdnr. 205.

769 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 586.

770 Eine Störung kann definiert werden als „die Minderung eines vorhandenen normalen Bestands von Rechtsgütern oder die Verletzung der vom Begriff der öffentlichen Ordnung umfassten sozialen Normen", vgl. *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009.

771 Vgl. *Belz/Mußmann*, PolG BW, 7. Aufl., 2009, § 20, Rdnr. 36; *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 20, Rdnr. 14.

kann“[772]. Die Datenerhebung setzt folglich eine im Einzelfall und keine allgemein bestehende Gefahr voraus. Für die verdachtsunabhängigen Ermittlungen im Internet liegt noch keine im Einzelfall bestehende, also konkrete Gefahr vor. Auch Tatsachen, aus denen sich eine konkrete Gefahr ergibt, liegen regelmäßig noch nicht vor.

Daher können die Grundrechtseingriffe durch die Polizeistreifen im Internet nicht durch § 20 Abs. 2 PolG BW gerechtfertigt werden.

3.1.4 Datenerhebung zur vorbeugenden Bekämpfung von Straftaten (§ 20 Abs. 3 PolG BW)

Der Polizeivollzugsdienst kann gemäß § 20 Abs. 3 PolG BW Daten über bestimmte Personen erheben, soweit dies zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Zu diesem Personenkreis zählen Personen, bei denen Anhaltspunkte vorliegen, dass sie künftige Straftaten begehen (Nr. 1), Kontakt- und Begleitpersonen dieser Personen (Nr. 2), Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie Opfer von Straftaten werden (Nr. 3), Personen im räumlichen Umfeld einer in besonderem Maße als gefährdet erscheinenden Person (Nr. 4) oder Zeugen, Hinweisgeber oder sonstige Auskunftspersonen (Nr. 5). Nach dem Wortlaut der Norm ist damit der Betroffenenkreis sehr weit gefasst. Indem auch Daten über „Zeugen, Hinweisgeber und sonstige Auskunftspersonen“ erhoben werden dürfen, sind theoretisch alle polizeilich überhaupt in Betracht kommenden Personenkreise in der Gesamtbevölkerung eingeschlossen[773].

Der unklare Wortlaut der Vorschrift ist allerdings dahingehend einzuschränken, dass für alle Personen „tatsächliche Anhaltspunkte“ für eine künftige Straftat vorliegen müssen[774]. Aus dem Grundsatz der Erforderlichkeit der Datenerhebung ist diese Einschränkung herzuleiten, womit in der Regel Voraussetzung sein wird, dass die Auskunftsperson irgendwie in ein kriminelles Milieu eingebunden ist und dadurch die Möglichkeit hat, die Polizei bei der vorbeugenden Bekämpfung von Straftaten zu unterstützen[775]. Die verdachtsunabhängigen polizeilichen Maßnahmen im Internet können grundsätzlich jeden treffen, also auch Personen, bei denen keine tatsächlichen Anhaltspunkte einer künftigen Straftat vorliegen. Bereits aus diesem Grund kann die Polizei die verdeckten Ermittlungen im Internet ohne Anfangsverdacht nicht auf § 20 Abs. 3 PolG BW stützen.

---

772 *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 411. Vgl. zu ähnlichen Definitionen einer konkreten Gefahr z. B. *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 6. Aufl., 2010; *Götz*, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., 2008, § 6, Rdnr. 17 ff.; *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 69.

773 *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 20, Rdnr. 28.

774 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 591; *Heckmann*, VBlBW 1992, 164, 172.

775 *Wolf/Stephan/Deger*, PolG BW, 6. Aufl., 2009, § 20, Rdnr. 28.

3.1.5 Generalklausel (§§ 1, 3 PolG BW)

Da keine der oben genannten Ermächtigungsgrundlagen die Grundrechtseingriffe durch die verdachtsunabhängigen Ermittlungen der Polizei im Internet rechtfertigt, könnte die polizeirechtliche Generalklausel (§§ 1, 3 PolG BW) einschlägig sein. Unabhängig davon, ob die Eingriffe überhaupt auf die allgemeine Generalklausel gestützt werden können[776] und ob diese Generalklausel den hohen Anforderungen an eine bereichsspezifische und bestimmte Ermächtigungsgrundlage genügen kann, fehlt es an einer konkreten Gefahr. Eine konkrete Gefahr ist Voraussetzung für die Rechtfertigung einer Maßnahme durch die Generalklausel[777]. Die im Internet ermittelnden Beamten sind somit bei Grundrechtseingriffen nicht durch die Generalklausel legitimiert.

3.1.6 Ergebnis

Das Polizeirecht in Baden-Württemberg sieht für die verdachtsunabhängigen Ermittlungen im Internet, die Grundrechtseingriffe darstellen, keine Ermächtigungsgrundlage vor. Damit sind diejenigen verdeckten verdachtsunabhängigen Maßnahmen im Internet, die einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen, nach dem geltenden PolG BW unzulässig.

Die Polizei in Baden-Württemberg darf allerdings die öffentlich zugänglichen Inhalte des Internet überwachen und Suchmaschinen nutzen. Zudem darf sie offen die geschützten Bereiche des Internet einsehen. Die Kommunikationsdienste ohne besondere Verifizierungsverfahren im Internet, wie beispielsweise viele Webforen, dürfen die ermittelnden Beamten beobachten, ohne ihre Behördenzugehörigkeit offenzulegen. Dies gilt auch für die sonstigen geschützten Internetinhalte, die keine qualifizierten Registrierungsverfahren mit Verifizierung der Angaben des interessierten Nutzers vorsehen. Eine verdeckte, aktive Kommunikation der ermittelnden Beamten mit anderen Kommunikationspartnern in den Kommunikationsdiensten des Internet ist für die Polizisten im Rahmen der verdachtsunabhängigen Ermittlungen jedoch nicht zulässig.

Bei allen Maßnahmen müssen die Polizeibehörden die Intensität ihrer Ermittlungen beachten. Einen ungerechtfertigten Eingriff in das Recht auf informationelle Selbstbestimmung stellt es dar, wenn gezielt personenbezogene Daten einer bestimmten Person aus den öffentlich zugänglichen oder den geschützten Bereichen des Internet erhoben werden und sich daraus

776 Siehe dazu *Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, 1998, S. 500 ff.; *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 6. Aufl., 2010; *Gusy*, Polizei- und Ordnungsrecht, 7. Aufl., 2009, Rdnr. 312 ff.

777 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 398, 411; *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 69; weiterführend zum Begriff der Gefahr siehe z. B. *Voßkuhle*, JuS 2007, 908 ff.; *Schoch*, Jura 2003, 473 ff.; *Möstl*, Jura 2005, 48 ff.

eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt[778]. Für die verdachtsunabhängigen Ermittlungen im Internet sieht das PolG BW keine Rechtsgrundlage für diese Maßnahme vor.

3.2 Bayern

Das bayerische Polizeiaufgabengesetz (BayPAG) sieht für die Erhebung personenbezogener Daten unterschiedliche Ermächtigungsgrundlagen vor. Ähnlich wie für die Bestimmungen des PolG BW kann sich die bayerische Polizei bei ihren verdachtsunabhängigen Ermittlungen im Internet für Grundrechtseingriffe nicht auf die Ermächtigungsgrundlagen für den Einsatz Verdeckter Ermittler (Art. 33 Abs. 3, 1 Nr. 3 BayPAG) und die Auskunftspflicht (Art. 12 BayPAG), die ähnlich der Befragung im PolG BW ist, berufen.

In Betracht kommt allerdings die Generalklausel zur Datenerhebung im BayPAG. Gemäß Art. 31 Abs. 1 Nr. 1 BayPAG kann die Polizei personenbezogene Daten über die in Art. 7, 8 und 10 BayPAG genannten Personen und über andere Personen erheben, wenn dies zur Gefahrenabwehr erforderlich ist, insbesondere zur vorbeugenden Bekämpfung von Straftaten (Art. 2 Abs. 1 BayPAG), und die Art. 11 bis 48 BayPAG die Befugnisse der Polizei nicht besonders regeln. Damit wird der Polizei ein weiter Bereich zur Datenerhebung zur Gefahrenabwehr eröffnet. Für die Gefahrenabwehr verweist Art. 31 Abs. 1 Nr. 1 BayPAG auf die allgemeine Aufgabenzuweisungsnorm in Art. 2 Abs. 1 BayPAG. Danach hat die Polizei die Aufgabe, die allgemein oder im Einzelfall bestehenden Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren (vgl. Art. 2 Abs. 1 BayPAG). Indem auch die allgemein bestehenden Gefahren abgewehrt werden sollen, setzt die Datenerhebungsgeneralklausel keine konkrete Gefahr, wie etwa in Baden-Württemberg, voraus[779]. Es reicht somit eine abstrakte Gefahr[780].

Eine abstrakte Gefahr liegt dann vor, wenn nach den Erfahrungen des täglichen Lebens bei bestimmten Arten von Verhaltensweisen oder Zuständen mit hinreichender Wahrscheinlichkeit ein Schaden im Einzelfall aufzutreten pflegt[781]. An eine abstrakte Gefahr sind somit keine besonders hohen Anforderungen zu stellen. Damit besteht für die verdachtsunabhängigen Ermittlungen der Polizei im Internet eine abstrakte Gefahr, da im Einzelfall geschützte Güter, beispielsweise durch die Veröffentlichung rechtswidriger Inhalte, verletzt werden können.

778 So zutreffend BVerfGE 120, 274, Absatz 309.

779 Vgl. *Berner/Köhler/Käß*, PAG, 20. Aufl., 2010, Art. 31, Rdnr. 2; *Gallwas/Wolff*, Bayerisches Polizei- und Sicherheitsrecht, 3. Aufl., 2004, Rdnr. 736.

780 *Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, 1998, S. 498.

781 VGH Mannheim ESVGH 21, 216, 218; *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 714; vgl. auch *Hamann*, NVwZ 1994, 669 ff.; *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rdnr. 70.

Im Folgenden ist zu untersuchen, ob diese weiten Befugnisse zur Datenerhebung des BayPAG den strengen Anforderungen des Bundesverfassungsgerichts für eine normenbestimmte, bereichsspezifische und verhältnismäßige Ermächtigungsgrundlage gerecht werden können. Art. 31 Abs. 1 BayPAG verlangt für die Datenerhebung die Erforderlichkeit zur Gefahrenabwehr. Mit diesem Merkmal wird auf den Grundsatz der Verhältnismäßigkeit als wesentliche Schranke der Datenerhebung verwiesen[782]. Für einen Eingriff in das Recht auf informationelle Selbstbestimmung bedarf es daher einer hinreichend bestimmten und verhältnismäßigen gesetzlichen Grundlage[783]. Für die Höhe der Anforderungen an die Ermächtigungsgrundlage ist entscheidend, in welcher Art und mit welcher Intensität in ein Grundrecht eingegriffen wird[784]. Eine gesteigerte Eingriffsintensität mit erhöhtem Rechtfertigungsbedarf haben Maßnahmen, die ohne die Kenntnis des Betroffenen oder insgesamt heimlich erfolgen[785].

Bei den verdachtsunabhängigen Ermittlungen der Polizei im Internet handeln die Polizisten verdeckt, wenn sie sich beispielsweise aktiv in Kommunikationsdiensten beteiligen. Damit liegt ein intensiver Eingriff in das Recht auf informationelle Selbstbestimmung vor. Die überwachten Personen werden auch nicht nach Abschluss der Ermittlungen über die Maßnahme benachrichtigt, was ebenfalls die Eingriffsintensität erhöht, da ihnen so die nachträglichen Rechtsschutzmöglichkeiten genommen beziehungsweise erschwert werden[786]. Außerdem können durch die verdeckte Teilnahme an Kommunikationsdiensten personenbezogene Daten, die für die Persönlichkeit des Betroffenen hohe Relevanz haben können, erhoben werden, wodurch die Maßnahme schwerwiegender wird[787]. Ferner weisen Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind – bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben – grundsätzlich eine hohe Eingriffsintensität auf[788].

Die ermittelnden Polizisten handeln im Internet verdachtsunabhängig und erheben bereits personenbezogene Daten zu einem Zeitpunkt, in dem nicht klar ist, ob eine Gefahrensituation vorliegt beziehungsweise von dem Betroffenen ausgeht. Ein konkretes Fehlverhalten des Betroffenen, mit dem

782 Vgl. *Würtenberger/Heckmann*, Polizeirecht, 6. Aufl., 2005, Rdnr. 587.
783 Vgl. z. B. BVerfG, Beschluss vom 12.08.2010, 2 BvR 1447/10.
784 BVerfGE 120, 378, 401; *Jarass*, in: Jarass/Pieroth, Grundgesetz, 12. Aufl., 2012, Art. 2, Rdnr. 58a.
785 BVerfGE 115, 320, 353; *Lorenz*, in: BK, Grundgesetz, Bd. 1, Art. 2 Abs. 1, Rdnr. 344.
786 Vgl. BVerfGE 118, 168, 197 ff.; 115, 320, 353; 113, 348, 383 ff.
787 Vgl. BVerfGE 118, 168, 197; 107, 299, 319 ff.
788 Vgl. BVerfGE 120, 378, 402; 115, 320, 354; 100, 313, 376.

er die Ermittlungen veranlasst haben könnte, liegt in der Regel nicht vor. Grundrechtseingreifende Ermittlungen „ins Blaue hinein“ lässt die Verfassung nach der Rechtsprechung des Bundesverfassungsgerichts nicht zu[789]. Außerdem ist ein unbestimmter Personenkreis ohne Störereigenschaft, der je nach Anzahl der ermittelnden Beamten steigen wird, von den Maßnahmen betroffen. Insgesamt liegen mit den verdachtsunabhängigen Ermittlungen der Polizei im Internet dann schwerwiegende Grundrechtseingriffe vor, wenn die Polizisten verdeckt mit anderen Beteiligten aktiv kommunizieren und dabei personenbezogene Daten erheben. In diesen Fällen besteht ferner die Gefahr, dass die Kommunikationspartner der staatlichen Stelle sich selbst belasten und damit Gegenstand staatlicher Ermittlungsmaßnahmen werden[790]. Auf die Datenerhebungsgeneralklausel lassen sich nur Grundrechtseingriffe mit niedriger Intensität stützen, wobei insbesondere bei verdeckten Maßnahmen die zulässige Intensität überschritten wird[791]. Als Ermächtigungsgrundlage für diese Maßnahmen scheidet daher eine allgemeine Datenerhebungsgeneralklausel, die lediglich eine abstrakte Gefahr voraussetzt, aus[792].

Das BayPAG geht vom Grundsatz der offenen Datenerhebung aus. Gemäß Art. 30 Abs. 3 Satz 2 BayPAG ist eine verdeckte Datenerhebung nur dann zulässig, wenn die Erfüllung polizeilicher Aufgaben auf andere Weise gefährdet oder erheblich erschwert würde oder wenn anzunehmen ist, dass dies den überwiegenden Interessen des Betroffenen entspricht. Die Erfüllung polizeilicher Aufgaben wäre ohne die verdeckte Teilnahme der staatlichen Stelle an Kommunikationsdiensten im Internet weder gefährdet noch erheblich erschwert, da ausreichend polizeiliche Maßnahmen zur Verfügung stehen, die ohne Grundrechtseingriffe verdachtsunabhängige Ermittlungen im Internet ermöglichen. Soweit sich dabei konkrete Gefahren ergeben oder ein entsprechender Tatverdacht vorliegt, könnte die Polizei die entsprechenden Maßnahmen, die in Grundrechte eingreifen, anwenden.

Art. 31 Abs. 1 BayPAG genügt zudem nicht den formalen Anforderungen des Bundesverfassungsgerichts, da die Regelung als allgemeine Generalklausel Datenerhebungen erlaubt. Die für die verdachtsunabhängigen Ermittlungen im Internet notwendige bereichsspezifische und bestimmte Ermächtigungsgrundlage für die möglichen Grundrechtseingriffe von hoher Intensität kann nicht durch eine Datenerhebungsgeneralklausel ersetzt werden.

Ein Rückgriff auf die allgemeine Generalklausel des Art. 11 Abs. 1 BayPAG scheidet, unabhängig von der Frage, ob sie neben der Datenerhebungs-

789 BVerfGE 120, 378, Absatz 169; BVerfGE 115, 320, 360 ff.

790 Vgl. dazu BVerfGE 118, 168, 197.

791 *Tischer*, Das System der informationellen Befugnisse der Polizei, 2004, S. 358 ff.

792 *Gusy* verlangt für verdeckte Informationserhebungen eine ausdrückliche Erlaubnis, vgl. *Gusy*, Polizei- und Ordnungsrecht, 7. Aufl., 2009, Rdnr. 201.

generalklausel überhaupt anwendbar ist, bereits an der fehlenden konkreten Gefahr, die in Art. 11 Abs. 1 BayPAG vorausgesetzt wird, aus. Zudem würde die Generalklausel des Art. 11 Abs. 1 BayPAG für die intensiven Eingriffe in das Recht auf informationelle Selbstbestimmung die hohen formalen Anforderungen des Bundesverfassungsgerichts an eine Ermächtigungsgrundlage nicht erfüllen.

3.3 Sonstige Bundesländer

In den anderen Bundesländern sehen die entsprechenden Gesetze für polizeiliche Maßnahmen keine spezifischen Ermächtigungsgrundlagen für verdachtsunabhängige Ermittlungen im Internet vor. Soweit im Polizeigesetz eines Bundeslandes eine abstrakte Gefahr für die Datenerhebungsgeneralklausel ausreicht[793], kann diese allgemeine Ermächtigungsgrundlage die intensiven Eingriffe in das Recht auf informationelle Selbstbestimmung nicht rechtfertigen. Insoweit wird auf die obigen Ausführungen zur Rechtslage in Bayern verwiesen. Wenn in dem Polizeigesetz des Bundeslandes für die Datenerhebungsgeneralklausel eine konkrete Gefahr vorliegen muss[794], ist sie bereits mangels dieser konkreten Gefahr für die verdachtsunabhängigen Ermittlungen der Polizei im Internet nicht einschlägig. In diesem Fall wird auf die obige Prüfung der Rechtslage in Baden-Württemberg verwiesen.

4. Ergebnis

Die meisten Maßnahmen der Polizeibehörden im Rahmen ihrer verdachtsunabhängigen Ermittlungen im Internet sind bereits durch die Aufgabenzuweisungsnormen legitimiert, da die Ermittlungsmaßnahmen keine Grundrechtseingriffe darstellen. Die behördlichen Betätigungen, die allerdings in das Recht auf informationelle Selbstbestimmung eingreifen, können weder durch die Regelungen des BKAG noch die landesrechtlichen Polizeigesetze gerechtfertigt werden. Damit dürfen die Polizisten sich insbesondere nicht verdeckt aktiv in den Kommunikationsdiensten beteiligen. Soweit ein geschützter Bereich des Internet über besondere Registrierungsvorkehrungen mit Verifizierung der Angaben des interessierten Nutzers verfügt, darf der ermittelnde Beamte sich nicht unter Verheimlichung seiner Behördenzugehörigkeit dort anmelden, da mit den folgenden Datenerhebungen ungerechtfertigte Eingriffe in das Recht auf informationelle Selbstbestimmung vorlägen.

Die gezielte Datenerhebung von personenbezogenen Daten einer bestimmten Person aus den öffentlich zugänglichen oder den geschützten Bereichen des Internet ist immer dann ein Grundrechtseingriff, wenn sich

793 Beispielsweise in § 30 Abs. 1 BbgPolG, § 32 Abs. 1 ThürPAG.
794 Vgl. z. B. § 18 Abs. 1 ASOG Bln, § 13 Abs. 1 Nr. 3 HSOG.

daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt[795].

II. Exkurs: Strafprozessuale Ermächtigungsgrundlagen

Die Polizei ist aufgrund verschiedener Ermächtigungsgrundlagen zu repressiven Maßnahmen im Internet berechtigt[796]. Die Ermittlungen der Polizei im virtuellen Raum, die nach der obigen Prüfung keinen Grundrechtseingriff darstellen, lassen sich auf die Eröffnung des polizeilichen Aufgabenbereiches stützen[797]. Der Aufruf von öffentlich zugänglichen Inhalten oder der Einsatz von Suchmaschinen ist somit grundsätzlich zulässig.

Zu beachten ist jedoch die Intensität der Maßnahmen. Bereits die gezielte Erhebung von personenbezogenen Daten einer bestimmten Person aus den allgemein zugänglichen oder aus den geschützten Bereichen des Internet kann einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen, soweit sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt[798]. Die Persönlichkeit eines Betroffenen wird gerade dann besonders gefährdet sein, wenn die Datenerhebungen der Bestätigung oder Schaffung eines Anfangsverdachts im Sinne des § 152 Abs. 2 StPO dienen und gegebenenfalls in einem Ermittlungsverfahren gegen den Betroffenen verwandt werden[799].

Für die Fälle, in denen ein Grundrechtseingriff bejaht wurde, beispielsweise bei einer verdeckten, aktiven Kommunikation der ermittelnden Beamten mit anderen Kommunikationspartnern, ist für die Wahl der

795 So zutreffend BVerfGE 120, 274, Absatz 309.

796 Da der Schwerpunkt der Arbeit auf verdachtsunabhängige Präventivmaßnahmen gerichtet ist, sollen repressive Maßnahmen nur im Überblick kurz dargestellt werden.

797 Vgl. *Brenneisen/Staack*, Kriminalistik 2012, 627, 630; *Bär*, MMR 1998, 463, 464; so auch die Antwort der Bundesregierung auf eine Kleine Anfrage zur Nutzung Sozialer Netzwerke zu Fahndungszwecken, BT-Drs 17/6587, S. 3. In der Literatur wird häufig vertreten, dass die Ermittlungsgeneralklausel der §§ 161, 163 StPO einschlägig sei, welche aber für eingriffslose Maßnahmen noch nicht erforderlich ist. Vgl. zu der in der Literatur vertretenen Ansicht zur Anwendung der Ermittlungsgeneralklausel *Rosengarten/Römer*, NJW 2012, 1764, 1767; *Henrichs*, Kriminalistik 2011, 622, 626; *Henrichs/Wilhelm*, Kriminalistik 2010, 30, 36; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl., 2012, Rdnr. 762; *Hornick*, StraFo 2008, 281, 285; *Kochheim*, Verdeckte Ermittlungen im Internet, Stand: März 2012, S. 47, abzurufen unter *http://cyberfahnder.de*; *Kudlich*, GA 2011, 193, 198 m. w. N.

798 Vgl. BVerfGE 120, 274, Absatz 309.

799 *Rosengarten/Römer*, NJW 2012, 1764, 1765; *Henrichs* geht von der besonderen Gefährdungslage bei den gezielten Maßnahmen „mit polizeilicher Zielrichtung" aus, vgl. *Henrichs*, Kriminalistik 2011, 622 (Fn. 5); *Brenneisen/Staack* beziehen sich auf die Rechtsprechung des Bundesverwaltungsgerichts (BVerwG vom 21.07.2010, 6 C 22/09), welches einen Grundrechtseingriff annimmt, wenn die zielgerichtete Erhebung öffentlich zugänglicher Daten „durch ihre systematische Erhebung, Sammlung und Erfassung einen zusätzlichen Aussagewert" erhält, vgl. *Brenneisen/Staack*, Kriminalistik 2012, 627, 628.

Ermächtigungsgrundlage nach dem Grad der Eingriffsintensität zu differenzieren. Abzugrenzen ist der „nicht offen ermittelnde Polizeibeamte“ (noeP)[800] vom Verdeckten Ermittler im Sinne der §§ 110a ff. StPO[801]. Der Bundesgerichtshof nimmt dann den Einsatz eines Verdeckten Ermittlers an, wenn die Ermittlung auf Dauer angelegt ist[802]. Entscheidend dafür sei, ob der Ermittlungsauftrag über einzelne wenige, konkret bestimmte Ermittlungshandlungen hinausgehe, ob es erforderlich werden würde, eine unbestimmte Vielzahl von Personen über die wahre Identität des Ermittlers zu täuschen, und ob wegen der Art und des Umfangs des Auftrags von vornherein abzusehen sei, dass die Identität des Beamten in zukünftigen Strafverfahren auf Dauer geheimgehalten werden müsse[803].

Die von der Rechtsprechung des Bundesgerichtshofs entwickelten Differenzierungsmerkmale sind allerdings nicht umfassend auf die Ermittlungen im Internet übertragbar[804]. Vielmehr sind die vom Bundesverfassungsgericht für Ermittlungen im virtuellen Raum entwickelten Grundsätze zum schutzwürdigen Vertrauen in die Identität des Kommunikationspartners einzubeziehen[805]. Während das Bundesverfassungsgericht die Dauer der Ermittlungsmaßnahmen unter einer Legende für grundsätzlich irrelevant hält[806], stellt dies ein wesentliches Abgrenzungsmerkmal dar[807]. Neben der Dauer der Ermittlungsmaßnahme entscheiden die Intensität der mit der Legende zu überwindenden Zugangskontrolle, die Art der Datenerhebung (aktiver Kommunikationspartner oder passiver Beobachter)[808] sowie der Detaillierungsgrad der notwendigen Legende[809], ob die Vorschriften für Verdeckte Ermittler anzuwenden sind.

Während nach vorherrschender Ansicht bei einem Anfangsverdacht der Einsatz eines noeP von der Ermittlungsgeneralklausel der §§ 161, 163 StPO gerechtfertigt ist[810], sind für Verdeckte Ermittler die besonderen Vorgaben

800 *Henrichs* bezeichnet den noeP bereits als „virtuellen nicht offen ermittelnden Polizeibeamten“ (vnoeP), *Henrichs*, Krmininalistik 2012, 632, 633.

801 Vgl. auch *Henrichs*, Kriminalistik 2012, 632 ff.; *Rosengarten/Römer*, NJW 2012, 1764 ff.

802 BGHSt 41, 64, 65.

803 BGHSt 41, 64, 65.

804 Vgl. *Rosengarten/Römer*, NJW 2012, 1764, 1765.

805 Vgl. BVerfGE 120, 274, Absatz 310 ff.; siehe zu den im Schrifttum vertretenen Abgrenzungen *Rosengarten/Römer*, NJW 2012, 1764, 1766 m. w. N.

806 Vgl. BVerfGE 120, 274, Absatz 311; ebenso *Henrichs*, Kriminalistik 2012, 632, 634.

807 Vgl. *Rosengarten/Römer*, NJW 2012, 1764, 1768.

808 Diese drei Abgrenzungsmerkmale nennen auch *Rosengarten/Römer*, NJW 2012, 1764, 1768.

809 *Kochheim* sieht den Detaillierungsgrad einer Legende als wichtig an, ab wann die vom Bundesverfassungsgericht gezogene Grenze zum schutzwürdigen Vertrauen des Betroffenen überschritten ist, vgl. *Kochheim*, Verdeckte Ermittlungen im Internet, Stand: März 2012, S. 44, abzurufen unter *http://cyberfahnder.de*.

810 Vgl. z. B. *Henrichs*, Kriminalistik 2012, 632; *ders.*, Kriminalistik 2010, 30, 36; *Rosengarten/Römer*, NJW 2012, 1764 ff. m. w. N.

der §§ 110a ff. StPO einzuhalten. Verdeckte Ermittler sind insbesondere erst bei den in § 110a StPO genannten Katalogstraftaten rechtmäßig einsetzbar[811].

Der Polizei steht für verdeckte Ermittlungen im Internet eine Vielzahl an repressiven Maßnahmen zur Verfügung, die von der virtuellen Beobachtung von Verdächtigen und Beschuldigten über Auskünfte bei Diensteanbietern bis zur Überwachung der Telekommunikation reichen[812]. Die Besonderheiten des Internet sind für diese Maßnahmen jeweils zu beachten und bei der Anwendbarkeit der Ermächtigungsgrundlagen einzubeziehen[813].

811 Das BKA setzte bereits nach Anordnung der Staatsanwaltschaft Virtuelle Verdeckte Ermittler für eine längerfristige, gezielte Teilnahme an der Kommunikation in Sozialen Netzwerken ein. In der Zeit zwischen Sommer 2009 und Sommer 2011 wurden im Rahmen der Strafverfolgung in sechs Ermittlungsverfahren Virtuelle Verdeckte Ermittler eingesetzt, vgl. die Antwort der Bundesregierung auf eine Kleine Anfrage, BT-Drs 17/6587, S. 5.

812 Einen guten Überblick bietet *Kochheim*, Verdeckte Ermittlungen im Internet, Stand: März 2012, insbesondere die Übersicht auf S. 25, abzurufen unter *http://cyberfahnder.de*.

813 Siehe weiterführend dazu *Singelnstein*, NStZ 2012, 593 ff.; *Henrichs*, Kriminalistik 2012, 632 ff.; *ders.*, Kriminalistik 2011, 622 ff.; *Kochheim*, Verdeckte Ermittlungen im Internet, Stand: März 2012, abzurufen unter *http://cyberfahnder.de*; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl., 2012, Rdnr. 758 ff.; *Brunst*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rdnr. 633 ff.

F.
Das Recht auf virtuelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung wird in der virtuellen Welt neuen Belastungen und veränderten Umständen ausgesetzt. Entwickelt zu einer Zeit, in der die Datenerhebung zumeist noch eine beschwerliche Aufgabe war, stellt sich die Frage, ob das Recht auf informationelle Selbstbestimmung in der vom Medium Internet dominierten Gegenwart den Herausforderungen gewachsen ist.

I. Neue Herausforderungen für den Datenschutz

Ein gewisser Einfluss des Internet auf die zukünftigen gesellschaftlichen Entwicklungen musste schon zu Beginn des Internetzeitalters jedem klar gewesen sein. Welch enormen Einfluss allerdings das Internet auf den Persönlichkeitsschutz und mögliche Datenverarbeitungsformen haben würde, konnte wahrscheinlich niemand in den virtuellen Anfängen abschätzen. Die schier unendlichen Datenmengen im Internet, die jeder Nutzer und auch der Staat in den meisten Fällen unkompliziert erheben können, eröffnen eine Vielzahl neuer Verwertungsmöglichkeiten. Damit korrespondierend gehen Gefahren und Risiken einher, die stetig an Überschaubarkeit verlieren. Mittlerweile werden diese Themen in einer breiten gesellschaftlichen Debatte aufgegriffen, die zu einer Sensibilisierung der Bürger mit dem Umgang ihrer eigenen Daten führen sollte[814].

Die Herausforderungen, vor denen der Datenschutz durch das unaufhaltsam expandierende Internet steht, stellen die verfassungsrechtlichen Grundsätze auf eine harte Probe[815]. Allen voran das Recht auf informationelle Selbstbestimmung mit seinem verfassungsrechtlichen Schutzkonzept „von schlichter und klarer Schönheit, das gleichwohl von Weitsicht geprägt war und sich als erstaunlich haltbar erwiesen hat“[816], wird in seinen Grundfesten erschüttert. Die althergebrachten Dogmen vom Fehlen belangloser Daten und dem allumfassenden Eingriffsbegriff führen nicht zu klaren Regelungen und transparenten Formeln. Vielmehr droht durch die technischen Fortschritte und das Vordringen des Internet in immer tiefere Lebensbereiche

814 *Gramm/Pieper* bemängeln noch, dass eine breite gesellschaftliche Debatte über die Frage fehle, wie weit die Beobachtung und die datentechnische Erfassung gehen soll, *Gramm/Pieper*, Grundgesetz Bürgerkommentar, 2008, S. 88.

815 Lesenswert dazu die Ausführungen von *Becker/Blackstein* zu staatlichen Verbraucherinformationen über das Internet, *Becker/Blackstein*, NJW 2011, 490 ff.

816 *Gurlit*, NJW 2010, 1035.

eine Aufweichung des Rechts auf informationelle Selbstbestimmung – bis schlimmstenfalls zur Selbstdemontage. Wer vertraut noch auf ein Grundrecht, was von staatlicher und privater Seite ausgehöhlt wurde? Was bleibt noch von der einstigen Säule des Datenschutzes, wenn sie sich zusehends von ihrer ursprünglichen Bestimmung löst?

Zutreffend stellt Bull fest, dass die Weite und Unbestimmtheit des Begriffs der informationellen Selbstbestimmung bei den Bürgern Erwartungen entstehen lässt, die nicht erfüllt werden können, da sie mit den gerechtfertigten Erwartungen anderer oder der Allgemeinheit kollidieren[817]. Zweifelsohne wurde dieser weite Ansatz des Bundesverfassungsgerichts auch nicht immer kritiklos hingenommen[818]. Für die virtuelle Welt kann und sollte ein umfassender Schutz sämtlicher personenbezogener Daten nicht mehr verfolgt werden. Ein großer Teil der Daten im Internet wird von den Betroffenen freiwillig ins Netz gestellt. Insoweit fällt es manchmal sogar schwer, in diesem Zusammenhang überhaupt noch von „Betroffenen" im eigentlichen Sinne zu sprechen, wenn man sich in Sozialen Netzwerken das fast unbändige Bedürfnis einiger Nutzer anschaut, selbst persönlichste Daten der Öffentlichkeit mitzuteilen. Wenn die Betroffenen sogar selbst für die Veröffentlichung ihrer Daten im Internet sorgen, kann das Selbstbestimmungsprinzip sie nicht mehr schützen[819]. Vielmehr ist den Nutzern dieser Sozialen Netzwerke häufiger ihre Selbstdarstellung wichtiger als das, was mit ihren Daten passiert. Ladeur prognostizierte diesen Wandel, sicherlich zu dem Zeitpunkt noch nicht auf die Entwicklungen zum Web 2.0 gemünzt, dahingehend, dass es oft hilfreich sei, eher auf die Beschädigung eines „Images" abzustellen als allgemein nach der Verletzung von Persönlichkeitsrechten zu fragen[820].

Indem identitätsbezogene Elemente der Nutzer freiwillig aus dem „analogen" Leben in die virtuelle Welt transportiert werden und damit in der Regel leicht für jeden anderen Nutzer auslesbar sind, verändert sich das Verständnis von einem Recht auf informationelle Selbstbestimmung. Solche Datenmengen konnten früher nicht so einfach erhoben und genutzt werden. Durch die Konzeption des Internet verschwinden diese Datenberge nicht nach einer gewissen Zeit. Vielmehr sind sie, gegebenenfalls auch noch Jahrzehnte später, weltweit abrufbar. Die „Jugendsünden" eines Nutzers können ihn somit lebenslänglich verfolgen. Dies ist ein Grund, weshalb aktuell wie-

817 *Bull*, NJW 2009, 3279, 3282.

818 Vgl. etwa *Albers*, Informationelle Selbstbestimmung, 2005, S. 238, 601 ff.; *Placzek*, Allgemeines Persönlichkeitsrecht und privatrechtlicher Informations- und Datenschutz, 2006, S. 196, 212 ff.; *Ladeur*, DuD 2002, 12, 15; *Trute*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, S. 165, Rdnr. 11.

819 Vgl. *Bull*, NVwZ 2011, 257, 258, der sogar von einem Versagen des Datenschutzes spricht, wenn Menschen sich freiwillig im Netz „entblößen", *Bull*, spw 2011, 21, 26.

820 *Ladeur*, NJW 2000, 1977, 1980.

der die Einführung von „Verfallsdaten“ für Informationen diskutiert wird[821]. Ein solcher Vorschlag wird auch auf europäischer Ebene diskutiert[822]. Dadurch sollen Daten nach einer gewissen Zeit wieder aus dem Internet verschwinden. Ob dieser gutgemeinte Ansatz wirklich erfolgversprechend sein kann oder, wie so häufig bei Lösungsvorschlägen für den virtuellen Bereich, ein Kampf gegen Windmühlen sein wird, kann heute niemand abschätzen.

Die Einschränkungen des Rechts auf informationelle Selbstbestimmung, die außerhalb des Internet noch zu annehmbaren Ergebnissen führen können, lassen für den Bereich des Internet nicht nur die Konturen verwischen, sondern beinahe fehlen. Im Rahmen dieser Arbeit hat sich gezeigt, dass das Recht auf informationelle Selbstbestimmung für den virtuellen Bereich weder dem Gewicht der staatlichen Strafverfolgung und Gefahrenabwehr noch dem Selbstbestimmungsprinzip der Grundrechtsträger vollends gerecht werden kann.

II. Das Recht auf virtuelle Selbstbestimmung

Hier soll keineswegs der Anspruch erhoben werden, als Vorreiter ein neues Recht schaffen zu wollen[823]. Dennoch zeigt sich, dass die Grundlagen des Rechts auf informationelle Selbstbestimmung für den virtuellen Bereich nicht umfassend übernommen werden können. Die in den 1980er Jahren mit dem Volkszählungsurteil[824] gereiften Ansprüche an ein Selbstbestimmungsrecht konnten damals noch überzeugen. Zu der Zeit, in der die Bürger die Medien eher konsumierten als selbst über sie ihre Informationen zu verbreiten, gab es nicht diese leicht zugänglichen Datenmengen. Das ist nun anders.

Der Bürger kann nicht mehr exakt informiert sein, „wer was wann und bei welcher Gelegenheit“ über ihn weiß[825]. Wenn ein Nutzer sich selbst dazu bewusst entschlossen hat, der Welt seine Daten mitzuteilen, verlieren diese Daten ihre Schutzwürdigkeit. Dies bedeutet nicht, dass der Staat mit einem „Datenstaubsauger“ sämtliche Daten einsammeln darf, um diese zu verarbeiten und auszuwerten. Der Staat muss sich aber auch nicht vor diesen Daten verschließen. Für die staatlichen Aufgaben der Gefahrenabwehr und Strafverfolgung, die auch im Interesse eines jeden Bürgers sind, benötigen

821 Vgl. *Nolte*, ZRP 2011, 236 ff.; *Hoeren*, ZRP 2010, 251, 253; *Bull*, NVwZ 2011, 257, 260.

822 Vgl. SPIEGEL ONLINE vom 17.03.2011 unter *http://www.spiegel.de/netzwelt/web/0,1518,751424,00.html*.

823 Vgl. bereits lange vorher zu einem Recht auf virtuelle Selbstbestimmung *Heckmann*, E-commerce und @ctivity – Der virtuelle Raum als Ausübungs- und Gewährleistungsbereich grundrechtsgeschützten Verhaltens, in: Hromadka, Deutsch-Tschechisches Rechtsfestival, 2002, S. 76 ff.; *Perrey*, Gefahrenabwehr und Internet, 2003, S. 204 ff.

824 BVerfGE 65, 1.

825 Vgl. BVerfGE 65, 1, 43. Vgl. auch *Bull*, NJW 2006, 1617, 1623.

die Behörden Informationen. Dass das Internet diese relativ leicht preisgibt, ändert nichts an der Sache an sich. Vielmehr erfordern sogar die neuen Gefahren des Internet, dass auch die staatlichen Stellen das Internet aktiv für ihre Aufgaben nutzen.

Die Eingriffsschwelle in das Recht auf virtuelle Selbstbestimmung verschiebt sich somit. Nicht jede Datenerhebung oder -nutzung kann einen Eingriff darstellen. Ob ein Eingriff vorliegt, bestimmt sich insbesondere nach der Art der Erhebung. Soweit sich die öffentliche Hand passiv im Netz bewegt und Daten erhebt, geschieht dies eingriffslos. Ihre Grenze findet das staatliche Handeln bei einer Täuschungshandlung. Eine Identitätstäuschung, die im Internet keine seltene Verhaltensweise darstellt, darf dem Staat nicht grundlos ermöglicht werden. Schwerwiegend wird das Recht auf virtuelle Selbstbestimmung verletzt, wenn die Behörde aktiv mit einem Nutzer kommuniziert und dabei über ihre Behördeneigenschaft täuscht. Das, was im „analogen" Bereich eindeutig als verdeckte Datenerhebung bis hin zum Einsatz eines Verdeckten Ermittlers qualifiziert wird, kann im Internet nicht schutzlos hingenommen werden, nur weil im Internet die Wahrhaftigkeit der Identität eines Nutzers für den nichtstaatlichen Kommunikationspartner schwierig überprüfbar ist. Gerade in Sozialen Netzwerken, deren Bedeutung unaufhörlich steigt, spielt dies eine gewichtige Rolle. Die langfristig angelegten Kommunikationsbeziehungen lassen ein Vertrauen unter den Beteiligten entstehen, welches der Staat nicht ausnutzen darf.

Um in diesem Umfeld die staatlichen Aufgaben zu erfüllen, könnte unter bestimmten Voraussetzungen der Einsatz eines „Virtuellen Verdeckten Ermittlers" als neues Instrument gesetzlich zugelassen werden[826]. Die rechtlichen Voraussetzungen müssten nicht entsprechend den eines Verdeckten Ermittlers im „analogen" Bereich ausgestaltet sein[827], da die Besonderheiten des Internet zu berücksichtigen sind. Der Virtuelle Verdeckte Ermittler begegnet seinen Internet-Kommunikationspartnern nicht körperlich, sondern es werden lediglich Daten zwischen den Rechnern übertragen[828]. An die Legende eines Virtuellen Verdeckten Ermittlers sind ferner keine hohen Anforderungen zu stellen, da beispielsweise keine amtlichen Ausweise ausgestellt werden müssen und zudem ein Virtueller Verdeckter Ermittler lediglich im Internet seine wahre Identität verschleiert oder verheimlicht. Der

826 Vgl. dazu auch *Henrichs*, Kriminalistik 2012, 632 ff.; *Henrichs/Wilhelm*, Kriminalistik 2010, 30, 35.

827 Das BKA setzte bereits nach Anordnung der Staatsanwaltschaft Virtuelle Verdeckte Ermittler für eine längerfristige, gezielte Teilnahme an der Kommunikation in Sozialen Netzwerken ein. In der Zeit zwischen Sommer 2009 und Sommer 2011 wurden im Rahmen der Strafverfolgung in sechs Ermittlungsverfahren Virtuelle Verdeckte Ermittler eingesetzt, vgl. die Antwort der Bundesregierung auf eine Kleine Anfrage, BT-Drs 17/6587, S. 5.

828 So sieht *Nack* dies als ausschlaggebend für die rechtliche Beurteilung an, siehe *Nack*, in: Karlsruher Kommentar zur StPO, 6. Aufl., 2008, § 110a, Rdnr. 7.

Gesetzgeber ist gefragt, die notwendigen Ermächtigungsgrundlagen mit Inhalt und Grenzen gesetzlich zu regeln[829].

Das Recht auf virtuelle Selbstbestimmung muss selbstredend nicht nur die öffentliche Gewalt binden, sondern gleichzeitig vor der privaten Datenmacht schützen. Der Maßstab für nicht-öffentliche Stellen ist dabei aber niedriger anzusetzen[830]. Die staatliche Gewalt ist im Rahmen ihrer Maßnahmen gemäß Art. 1 Abs. 3 GG unmittelbar an die Grundrechte gebunden und kann nicht sämtliche Möglichkeiten privaten Handelns rechtmäßig nutzen. Während sich Private auf die Informationsfreiheit gemäß Art. 5 Abs. 1 Satz 1 Alt. 2 GG berufen können, bleibt dies dem informationsinteressierten Staat verwehrt[831]. Für Datenerhebungen ist die öffentliche Hand somit an strengere Regeln gebunden als private Informationsinteressierte[832].

Ein Recht auf virtuelle Selbstbestimmung kann den Bürger nur schützen, wenn er selbst eigenverantwortlich seine Daten verwaltet. Die Rolle des Staates wird dabei sein, den Bürger zu einem effektiven Selbstschutz zu befähigen, indem er ihm eine Infrastruktur zur Verfügung stellt, die es ihm erlaubt, sich zu informieren und Vertrauen zu entwickeln[833]. Zusätzlich müssen die Menschen die Zusammenhänge zwischen der Offenbarung ihrer Daten und dem, was andere daraus machen beziehungsweise machen können, erkennen und daraus ihre Schlüsse ziehen können[834]. Eine gewisse Sparsamkeit der Nutzer bei der Veröffentlichung ihrer persönlichen Daten, gerade in Sozialen Netzwerken, könnte die datenschutzrechtlichen Probleme zwar nicht beheben, aber zumindest weit einschränken.

829 So empfiehlt auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit *Peter Schaar*, die Befugnisse zur polizeilichen Recherche im Internet insgesamt spezialgesetzlich zu regeln, siehe 23. Tätigkeitsbericht zum Datenschutz für die Jahre 2009 und 2010 vom 12.04.2011, S. 18.

830 Vgl. *Perrey*, Gefahrenabwehr und Internet, 2003, S. 205.

831 *Bethge*, in: Sachs, Grundgesetz, 6. Aufl., 2011, Art. 5, Rdnr. 58; vgl. zum Konflikt des Rechts auf informationelle Selbstbestimmung und der Informationsfreiheit bereits *Gallwas*, NJW 1992, S. 2785 ff.

832 *Bull*, NJW 2009, 3279, 3282.

833 Vgl. *Boehme-Neßler*, MMR 2009, 439, 443.

834 *Bull*, NVwZ 2011, 257, 259; *Heckmann* sieht zutreffend ein Problem in der stetig abnehmenden Datenherrschaft der Nutzer über ihre Profile und bezweifelt damit einhergehend die Wirksamkeit ihrer entsprechenden Einwilligungen, *Heckmann*, NJW 2012, 2631, 2633.

Literaturverzeichnis

Abbühl, Anicee, Der Aufgabenwandel des Bundeskriminalamtes: von der Zentralstelle zur multifunktionalen Intelligence-Behörde des Bundes, Stuttgart 2010

Albers, Marion, Informationelle Selbstbestimmung, Baden-Baden 2005

– Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin 2001

– Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem, Wolfgang (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, München 2008

Ahlf, Ernst-Heinrich/Daub, Ingo/Lersch, Roland/Störzer, Hans U., Bundeskriminalamtgesetz, Stuttgart 2000

Ahlf, Ernst-Heinrich, Das Bundeskriminalamt als Zentralstelle, Wiesbaden 1985

Albrecht, Hans-Jörg/Dorsch, Claudia/Krüpe, Christiane, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg im Breisgau 2003

Albrecht, Hans-Jörg/Grafe, Adina/Kilchling, Michael, Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO, Berlin 2008

von Arnauld, Andreas, Die Freiheitsrechte und ihre Schranken, Baden-Baden 1999

Arning, Marian/Forgó, Nikolaus/Krügel, Tina, Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten, DuD 2006, S. 704 ff.

Artzt, Matthias, Die verfahrensrechtliche Bedeutung polizeilicher Vorfeldermittlungen, Frankfurt am Main 2000

Assall, Moritz/Steinke, Ron, Big Brother, We´re watching you, FoR 2008, S. 58 ff.

Aulehner, Josef, Polizeiliche Gefahren- und Informationsvorsorge, Berlin 1998

– 10 Jahre „Volkszählungs"-Urteil, CR 1993, S. 446 ff.

Bäcker, Matthias, Die Vertraulichkeit der Internetkommunikation, in: Rensen, Hartmut/Brink, Stefan (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts, Berlin 2009, S. 99 ff.

– Terrorismusabwehr durch das Bundeskriminalamt, Berlin 2009

Bär, Wolfgang, Anmerkung zum Urteil des BVerfG vom 27.02.2008, MMR 2008, S. 325 ff.

– Strafrechtliche Kontrolle in Datennetzen, MMR 1998, S. 463 ff.

– Öffentlichkeitsfahndung im Internet, CR 1997, S. 422 ff.

– Auf dem Weg zur „Internet-Polizei"?, in: Bäumler, Helmut (Hrsg.), „Polizei und Datenschutz" – Neupositionierung im Zeichen der Informationsgesellschaft, Neuwied 1999, S. 167 ff.

– Handbuch zur EDV-Beweissicherung im Strafverfahren, Stuttgart 2007

Baron, Richard, Zur Frage der grundsätzlichen Zulässigkeit des Einsatzes verdeckt ermittelnder Personen und Vorschlag einer umfassenden gesetzlichen Regelung, Hamburg 2002

Bartsch, Michael, Die Vertraulichkeit und Integrität informationstechnischer Systeme als sonstiges Recht nach § 823 Abs. 1 BGB, CR 2008, S. 613 ff.

Bartsch, Verena, Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen öffentlich zugänglicher Orte in Deutschland und den USA, Berlin 2004

Baudewin, Christian, Der Schutz der öffentlichen Ordnung im Versammlungsrecht, Frankfurt am Main 2007

Baum, Gerhart Rudolf/Schantz, Peter, Die Novelle des BKA-Gesetzes, ZRP 2008, S. 137 ff.

Baumann, Reinhold, Stellungnahme zu den Auswirkungen des Urteils des Bundesverfassungsgerichts vom 15.12.1983 zum Volkszählungsgesetz 1983, DVBl 1984, S. 612 ff.

Bäumler, Helmut, Normenklarheit als Instrument der Transparenz, JR 1984, S. 361 ff.

Bausch, Stephan, Videoüberwachung als präventives Mittel der Kriminalitätsbekämpfung in Deutschland und in Frankreich, Marburg 2004

Becker, Florian/Blackstein, Ylva, Der transparente Staat – Staatliche Verbraucherinformation über das Internet, NJW 2011, S. 490 ff.

Beißwenger, Michael (Hrsg.), Chat-Kommunikation, Stuttgart 2001

Belz, Reiner/Mußmann, Eike, Polizeigesetz für Baden-Württemberg, 7. Aufl., Stuttgart 2009

Benda, Ernst, Das Recht auf informationelle Selbstbestimmung und die Rechtsprechung des Bundesverfassungsgerichts zum Datenschutz, DuD 1984, S. 86 ff.

– Privatsphäre und „Persönlichkeitsprofil", in: Leibholz, Gerhard/Faller, Hans Joachim/Mikat, Paul/Reis, Hans (Hrsg.), Menschenwürde und freiheitliche

Rechtsordnung: Festschrift für Willi Geiger zum 65. Geburtstag, Tübingen 1974, S. 23 ff.

Bergmann, Lutz/Möhrle, Roland/Herb, Armin, Datenschutzrecht, Bd. 1, Stuttgart, Stand: April 2010

Berner, Georg/Köhler, Gerd Michael/Käß, Robert, Polizeiaufgabengesetz, 20. Aufl., Heidelberg 2010

Beulke, Werner, Strafprozessrecht, 10. Aufl., Heidelberg 2008

Beulke, Werner/Meininghaus, Florian, Verdeckte Durchsuchung eines Computers mittels heimlich installiertem Computerprogramm, StV 2007, S. 63 ff.

Billmeier, Eva, Die Düsseldorfer Sperrungsverfügung, Berlin 2007

Bizer, Johann, Web-Cookies datenschutzrechtlich, DuD 1998, S. 277 ff.

– Privacy Policy – Im Gestrüpp der Gesetze, DuD 2002, S. 386 ff.

Bleisteiner, Stephan, Rechtliche Verantwortlichkeit im Internet, Köln 1999

Blümel, Karl-Heinz/Drewes, Michael/Malmberg, Karl Magnus/Walter, Bernd, Bundespolizeigesetz Kommentar, 3. Aufl., Stuttgart 2006

Böckenförde, Thomas, Die Ermittlung im Netz, Tübingen 2003

– Auf dem Weg zur elektronischen Privatsphäre, JZ 2008, S. 925 ff.

Boehme-Neßler, Volker, CyberLaw, München 2001

– Vertrauen im Internet – Die Rolle des Rechts, MMR 2009, S. 439 ff.

Brandner, Stephan, Das allgemeine Persönlichkeitsrecht in der Entwicklung durch die Rechtsprechung, JZ 1983, S. 689 ff.

Brandt, Astrid, Zur Strafbarkeit des Phishing, Hamburg 2010

Braun, Torsten, IPnG: Neue Internet-Dienste und virtuelle Netze, Heidelberg 1999

Brenneisen, Hartmut, Informationelle Eingriffe im Vorfeld von Versammlungen, DuD 2000, S. 651 ff.

Brenneisen, Hartmut/Staack, Dirk, Die virtuelle Streife in der Welt der Social Media, Kriminalistik 2012, S. 627 ff.

Brink, Stefan/Völler, Maximilian, Big Brother is watching You – sometimes, LKRZ 2011, S. 201 ff.

Britz, Gabriele, Freie Entfaltung durch Selbstdarstellung, Tübingen 2007

– Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, S. 411 ff.

– Schutz informationeller Selbstbestimmung gegen schwerwiegende Grundrechtseingriffe – Entwicklung im Lichte des Vorratsdatenspeicherungsurteils, JA 2011, S. 81 ff.

Brunst, Phillip W., Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, Berlin 2009

Buermeyer, Ulf, Die „Online-Durchsuchung". Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, S. 329 ff.

Bull, Hans Peter, Persönlichkeitsschutz im Internet: Reformeifer mit neuen Ansätzen, NVwZ 2011, S. 257 ff.

– Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese?, NJW 2006, S. 1617 ff.

– Grundsatzentscheidungen zum Datenschutz bei den Sicherheitsbehörden, in: Möllers, Martin H. W./van Ooyen, Robert Chr. (Hrsg.), Bundesverfassungsgericht und öffentliche Sicherheit, Frankfurt am Main 2011

– Informationsrecht ohne Informationskultur?, RDV 2008, S. 47 ff.

– Sind Video-Verkehrskontrollen „unter keinem rechtlichen Aspekt vertretbar"?, NJW 2009, S. 3279 ff.

– Informationelle Selbstbestimmung – Vision oder Illusion?, Tübingen 2009

– Regulierung des Internets mit den Instrumenten des Datenschutzes?, spw 2011, S. 21 ff.

Büllesfeld, Dirk, Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze zur Kriminalitätsvorsorge, Stuttgart 2002

Bullinger, Martin/Mestmäcker, Ernst-Joachim, Multimediadienste, Baden-Baden 1997

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo, Bundesdatenschutzgesetz, 3. Aufl., Frankfurt am Main 2010

Denninger, Erhard/Hoffmann-Riem, Wolfgang/Schneider, Hans-Peter/Stein, Ekkehart (Hrsg.), Grundgesetz-Kommentar, 3. Aufl., Neuwied 2001

Denninger, Erhard, Das Recht auf informationelle Selbstbestimmung und Innere Sicherheit, KJ 1985, S. 215 ff.

Desoi, Monika/Knierim, Antonie, Intimsphäre und Kernbereichsschutz, DÖV 2011, S. 398 ff.

Determann, Lothar, Kommunikationsfreiheit im Internet, Baden-Baden 1999

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

Dingler, Andreas, Betrug bei Online-Auktionen, Aachen 2008

Dolderer, Michael, Verfassungsfragen der „Sicherheit durch Null-Toleranz", NVwZ 2001, S. 130 ff.

Dolzer, Rudolf/Graßhoff, Karin/Kahl, Wolfgang/Waldhoff, Christian (Hrsg.), Bonner Kommentar zum Grundgesetz, Bd. 1, 2 und 3, Heidelberg, Stand: November 2012

Dörr, Dieter/Kreile, Johannes/Cole, Mark D. (Hrsg.), Handbuch Medienrecht, 2. Aufl., Frankfurt am Main 2011

Dorsch, Claudia, Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, Berlin 2005

Dreier, Horst (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 2. Aufl., Tübingen 2004

Duttge, Gunnar, Strafprozessualer Einsatz von V-Personen und Vorbehalt des Gesetzes, JZ 1996, S. 556 ff.

Eckhardt, Jens, Datenschutzerklärungen und Hinweise auf Cookies, ITRB 2005, S. 46 ff.

Eckhardt, Jens/Schütze, Marc, Vorratsdatenspeicherung nach BVerfG: „Nach dem Gesetz ist vor dem Gesetz …", CR 2010, S. 225 ff.

Eckhoff, Rolf, Der Grundrechtseingriff, Köln 1992

Eichler, Alexander, Cookies – verbotene Früchte?, K&R 1999, S. 76 ff.

Eifert, Martin, Informationelle Selbstbestimmung im Internet, NVwZ 2008, S. 521 ff.

Eisenberg, Ulrich, Kriminologie, 6. Aufl., München 2005

Engel, Christoph, Inhaltskontrolle im Internet, AfP 1996, S. 220 ff.

Ennuschat, Jörg/Klestil, Stephanie, Sperrverfügungen gegen Access-Provider als Instrument zur Bekämpfung des illegalen Online-Glücksspiels?, ZfWG 2009, S. 389 ff.

Epping, Volker/Hillgruber, Christian (Hrsg.), Grundgesetz-Kommentar, München 2009

Epping, Volker, Grundrechte, 4. Aufl., Berlin 2010

Erd, Rainer, Datenschutzrechtliche Probleme sozialer Netzwerke, NVwZ 2011, S. 19 ff.

Ernst, Stefan (Hrsg.), Hacker, Cracker & Computerviren, Köln 2004

Fetzer, Thomas/Zöller, Mark A., Verfassungswidrige Videoüberwachung, NVwZ 2007, S. 775 ff.

Fiedler, Christoph, Meinungsfreiheit in einer vernetzten Welt, Baden-Baden 2002

Finke, Thorsten, Die strafrechtliche Verantwortung von Internet-Providern, Tübingen 1998

Fix, Tina, Generation Chat, München 2001

Frenz, Walter, Informationelle Selbstbestimmung im Spiegel des BVerfG, DVBl 2009, S. 333 ff.

Frey, Dieter/Rudolph, Matthias/Oster, Jan, Internetsperren und der Schutz der Kommunikation im Internet – Am Beispiel behördlicher und gerichtlicher Sperrungsverfügungen im Bereich des Glücksspiel- und Urheberrechts, MMR-Beilage zu Heft 3/2012, S. 1 ff.

Friauf, Karl Heinrich/Höfling, Wolfram (Hrsg.), Berliner Kommentar zum Grundgesetz, Berlin, Stand: Juli 2012

Fröhle, Jens, Web advertising, Nutzerprofile und Teledienstedatenschutz, München 2003

Gabel, Detlev, Neue Rahmenbedingungen für den Datenschutz im Internet, ZUM 2002, S. 607 ff.

Gallwas, Hans-Ullrich, Der allgemeine Konflikt zwischen dem Recht auf informationelle Selbstbestimmung und der Informationsfreiheit, NJW 1992, S. 2785 ff.

Gallwas, Hans-Ullrich/Wolff, Heinrich Amadeus, Bayerisches Polizei- und Sicherheitsrecht, 3. Aufl., Stuttgart 2004

Gausling,Tina, Verdachtsunabhängige Speicherung von Verkehrsdaten auf Vorrat, München 2010

Géczy-Sparwasser, Vanessa, Die Gesetzgebungsgeschichte des Internet, Berlin 2003

Gehde, Frank, Verfolgung von Straftaten im Internet, DuD 2003, S. 496 ff.

Geiger, Andreas, Verfassungsfragen zur polizeilichen Anwendung der Video-Überwachungstechnologie bei der Straftatbekämpfung, Berlin 1994

Geis, Max-Emanuel, Polizeiliche Handlungsspielräume im Vorbereich und Verlauf von außergewöhnlichen Demonstrationslagen, Die Polizei 1993, S. 293 ff.

Gercke, Marco, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, S. 245 ff.

– „Cyberterrorismus" – Aktivitäten terroristischer Organisationen im Internet, CR 2007, S. 62 ff.

– Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden, MMR 2008, S. 291 ff.

– Die Entwicklung des Internetstrafrechts 2009/2010, ZUM 2010, S. 633 ff.

– Die Entwicklung des Internetstrafrechts 2011/2012, ZUM 2012, S. 625 ff.

Gercke, Marco/Brunst, Phillip W., Praxishandbuch Internetstrafrecht, Stuttgart 2009

Gergen, Peter, Internetdienste, München 2002

Germann, Michael, Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000

Gola, Peter/Schomerus, Rudolf (Hrsg.), Bundesdatenschutzgesetz-Kommentar, 11. Aufl., München 2012

Gola, Peter/Klug, Christoph, Grundzüge des Datenschutzrechts, München 2003

Götz, Volkmar, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl., München 2008

Gounalakis, Georgios (Hrsg.), Rechtshandbuch Electronic Business, München 2003

Graf, Jürgen Peter, Beck´scher Online-Kommentar Strafprozessordnung, Edition 15, Stand: 01.10.2012

– Internet – Straftaten und Strafverfolgung, DRiZ 1999, S. 281 ff.

Gramm, Christof/Pieper, Stefan Ulrich, Grundgesetz Bürgerkommentar, Baden-Baden 2008

Greiner, Arved, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, Hamburg 2001

Grote, Rainer, Kommunikative Selbstbestimmung im Internet und Grundrechtsordnung, KritV 1999, S. 27 ff.

Gruner, Alexander, Biometrie und informationelle Selbstbestimmung, Dresden 2005

Guder, Martin André, Die repressive Hörfalle im Lichte der Europäischen Menschenrechtskonvention, Zürich 2007

Gudermann, Anne, Online-Durchsuchung im Lichte des Verfassungsrechts. Die Zulässigkeit eines informationstechnologischen Instruments moderner Sicherheitspolitik, Hamburg 2010

Gundermann, Lukas, Das neue TKG-Begleitgesetz, K&R 1998, S. 48 ff.

Gurlit, Elke, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, S. 1035 ff.

Gusy, Christoph, Polizei- und Ordnungsrecht, 7. Aufl., Tübingen 2009

– Polizeiliche Befragung am Beispiel des § 9 NRWPolG, NVwZ 1991, S. 614 ff.

Haas, Günter, Vorermittlungen und Anfangsverdacht, Berlin 2003

Habel, Oliver M., Eine Welt ist nicht genug – Virtuelle Welten im Rechtsleben, MMR 2008, S. 71 ff.

Hadamek, Ruth, Artikel 10 GG und die Privatisierung der Deutschen Bundespost, Berlin 2002

Haft, Fritjof/Eisele, Jörg, Zur Einführung – Rechtsfragen des Datenverkehrs im Internet, JuS 2001, S. 112 ff.

Hamann, Wolfram, Die Gefahrenabwehrverordnung – ein Gebrauchsklassiker des Ordnungsrechts?, NVwZ 1994, S. 669 ff.

Hannich, Rolf, Karlsruher Kommentar zur Strafprozessordnung, 6. Aufl., München 2008

Harnisch, Stefanie/Pohlmann, Martin, Der Einsatz des IMSI-Catchers zur Terrorismusbekämpfung durch das Bundeskriminalamt, NVwZ 2009, S. 1328 ff.

Härting, Niko, Datenschutz im Internet – Wo bleibt der Personenbezug?, CR 2008, S. 743 ff.

– Datenschutz zwischen Transparenz und Einwilligung, CR 2011, S. 169 ff.

Heckmann, Dirk, Der virtuelle Raum als Wohnung – Die sogenannte Online-Durchsuchung zwischen Privatsphäre und offenem Netz, in: Kluth, Winfried/Müller, Martin/Peilert, Andreas, Wirtschaft – Verwaltung – Recht, Festschrift für Rolf Stober, Köln 2008

– Polizeiliche Datenerhebung und -verarbeitung, VBlBW 1992, S. 164 ff.

– E-Commerce und @ctivity – Der virtuelle Raum als Ausübungs- und Gewährleistungsbereich grundrechtsgeschützten Verhaltens, in: Hromadka, Wolfgang (Hrsg.), Deutsch-Tschechisches Rechtsfestival, 2001, S. 77 ff.

– Persönlichkeitsschutz im Internet – Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderungen für Ehrschutz und Profilschutz, NJW 2012, S. 2631 ff.

Hein, Mathias, TCP/IP, 6. Aufl., Bonn 2002

Henrichs, Axel, Verdeckte personale Ermittlungen im Internet, Kriminalistik 2012, S. 632 ff.

– Ermittlungen im Internet, Kriminalistik 2011, S. 622 ff.

Henrichs, Axel/Wilhelm, Jörg, Polizeiliche Ermittlungen in sozialen Netzwerken, Kriminalistik 2010, S. 30 ff.

Hermann, Ronald/Lang, Gerhard/Schneider, Andreas, Polizeirelevante Grundrechte, Stuttgart 1998

Hermes, Georg, Unverletzlichkeit der Wohnung – Abschied vom Grundrechtsschutz für den Inhaber öffentlich zugänglicher Räume?, JZ 2005, S. 461 ff.

Herrmann, Christoph, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Frankfurt 2010

Herrmann, Klaus/Soiné, Michael, Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz, NJW 2011, S. 2922 ff.

Herzog, Marco, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, Frankfurt am Main 2000

Heß, Reinhold, Grundrechtskonkurrenzen, Berlin 2000

Hilgendorf, Eric/Hong, Seung-Hee, Cyberstalking, K&R 2003, S. 168 ff.

Hilgendorf, Eric/Valerius, Brian, Computer- und Internetstrafrecht, 2. Aufl., Berlin Heidelberg 2012

Hilgers, Hans, Zum Strafverfahrensrechtsänderungsgesetz 1999 (StVÄG 1999) – 1. Teil, NStZ 2000, S. 561 ff.

von Hippel, Reinhard/Weiß, Axel, Eingriffsqualität polizeilicher Observierungen, JR 1992, S. 316 ff.

Hirsch, Burkhard, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Zugleich Anmerkung zu BVerfG, NJW 2008, 822, NJOZ 2008, S. 1907 ff.

Hoeren, Thomas, Anonymität im Web – Grundfragen und aktuelle Entwicklungen, ZRP 2010, S. 251 ff.

– Grundzüge des Internetrechts, 2. Aufl., München 2002

– Zur Einführung: Informationsrecht, JuS 2002, S. 947 ff.

Hoeren, Thomas/Sieber, Ulrich (Hrsg.), Handbuch Multimedia-Recht, München, Stand: August 2010

Hofe, Gerhard, Abschied vom weiten Wohnungsbegriff des Art. 13 GG?, ZRP 1995, S. 169 ff.

Höfelmann, Elke, Das Grundrecht auf informationelle Selbstbestimmung anhand der Ausgestaltung des Datenschutzrechts und der Grundrechtsnormen der Landesverfassungen, Frankfurt am Main 1997

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

– Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009 ff.

Hohmann-Dennhardt, Christine, Informationeller Selbstschutz als Bestandteil des Persönlichkeitsrechts, RDV 2008, S. 1 ff.

Höhne, Focke, Der (Nicht-)Vollzug des Zugangserschwerungsgesetzes – Rechtliche Problemstellung und Ausblick, jurisPR-ITR 24/2010, Anm. 2

Hömig, Dieter (Hrsg.), Grundgesetz-Kommentar, 9. Aufl., Baden-Baden 2010

Hornick, Andreas, Staatlicher Zugriff auf elektronische Medien, StraFo 2008, S. 281 ff.

Hornung, Gerrit, Ein neues Grundrecht, CR 2008, S. 299 ff.

– Ermächtigungsgrundlage für die Online-Durchsuchung?, DuD 2007, S. 575 ff.

– Der Personenbezug biometrischer Daten, DuD 2004, S. 429 ff.

– Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, MMR 2004, S. 3 ff.

– Die Festplatte als „Wohnung“?, JZ 2007, S. 828 ff.

Hornung, Gerrit/Desoi, Monika, „Smart Cameras“ und automatische Verhaltensanalyse, K&R 2011, S. 153 ff.

Hsieh, Shuo-Chun, E-Mail-Überwachung zur Gefahrenabwehr, Stuttgart 2011

Hufen, Friedhelm, Staatsrecht II Grundrechte, 2. Aufl., München 2009

Husmann, Heike, Chatten im Internet Relay Chat (IRC), München 1998

Ihde, Rainer, Cookies – Datenschutz als Rahmenbedingung der Internetökonomie, CR 2000, S. 413 ff.

Iraschko-Luscher, Stephanie/Kiekenbeck, Pia, Datenschutz im Internet – Widerspruch oder Herausforderung?, RDV 2010, S. 261 ff.

Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. 7, 3. Aufl., Heidelberg 2009, Bd. 5, 2. Aufl., Heidelberg 2000

Jahn, Matthias, Der strafprozessuale Zugriff auf Telekommunikationsverbindungsdaten, JuS 2006, S. 491 ff.

Jahn, Matthias/Kudlich, Hans, Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, S. 57 ff.

Jandt, Silke/Roßnagel, Alexander, Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz?, MMR 2011, S. 637 ff.

Janowicz, Krzysztof, Sicherheit im Internet, Beijing 2002

Jarass, Hans D./Pieroth, Bodo, Grundgesetz-Kommentar, 12. Aufl., München 2012

– Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, S. 857 ff.

Joecks, Wolfgang/Miebach, Wulf (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 3, München 2012

Kant, Martina, Internet-Streifen, Bürgerrechte & Polizei/CILIP 71 (1/2002), S. 29 ff.

Karg, Moritz, IP-Adressen sind personenbezogene Verkehrsdaten, MMR-Aktuell 2011, Nr. 315811

Kaufmann, Carsten Noogie Thomas, Weblogs – rechtliche Analyse einer neuen Kommunikationsform, Hamburg 2009

Kleinknecht, Theodor/Müller, Hermann/Reitberger, L. (Begr.), Kommentar zur StPO, Köln, Stand: 2011

Kloepfer, Michael, Verfassungsrecht Bd. 2, München 2010

– Geben moderne Technologien und die europäische Integration Anlaß, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen?, NJW 1998, Beilage zu Heft 23, S. 21 ff.

Klutzny, Alexander, Online-Demonstrationen und virtuelle Sitzblockaden – Grundrechtsausübung oder Straftat?, RDV 2006, S. 50 ff.

Knemeyer, Franz-Ludwig, Polizei- und Ordnungsrecht, 11. Aufl., München 2007

Koch, Frank A., Schutz der Persönlichkeitsrechte im Internet: spezifische Gefährdungen, ITRB 2011, S. 158 ff.

Kochheim, Dieter, Verdeckte Ermittlungen im Internet, Stand: März 2012, abzurufen unter http://cyberfahnder.de

Köhntopp, Marit/Köhntopp, Kristian, Datenspuren im Internet, CR 2000, S. 248 ff.

König, Sabine, Kinderpornographie im Internet, Hamburg 2004

Koreng, Ansgar, Zensur im Internet, Baden-Baden 2010

Kraft, Dennis/Meister, Johannes, Rechtsprobleme virtueller Sit-ins, MMR 2003, S. 366 ff.

Kress, Sarah, Der „Große Lauschangriff" als Mittel internationaler Verbrechensbekämpfung, Hamburg 2009

Kretschmer, Joachim, Der große Lauschangriff auf die Wohnung als strafprozessuale Ermittlungsmaßnahme, Jura 1997, S. 581 ff.

Krey, Volker/Haubrich, Edgar, Zeugenschutz, Rasterfahndung, Lauschangriff, Verdeckte Ermittler, JR 1992, S. 309 ff.

Krist, Georg, Videoüberwachung auf öffentlichen Straßen und Plätzen, LKRZ 2011, S. 171 ff.

Krüger, Anja, Informationelle Selbstbestimmung und Kriminalaktenführung, DÖV 1990, S. 641 ff.

Krüpe-Gescher, Christiane, Die Überwachung der Telekommunikation nach den §§ 100a, 100b StPO in der Rechtspraxis, Berlin 2005

Kudlich, Hans, Strafprozessuale Probleme des Internet, JA 2000, S. 227 ff.

– Strafverfolgung im Internet – Bestandsaufnahme und aktuelle Probleme, GA 2011, S. 193 ff.

Kugelmann, Dieter, Polizei- und Ordnungsrecht, Berlin 2006

– Der polizeiliche Gefahrenbegriff in Gefahr? – Anforderungen an die Voraussetzungen polizeilicher Eingriffsbefugnisse, DÖV 2003, S. 781 ff.

Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios, Datenschutzrecht, Frankfurt am Main 2008

Kurose, James F./Ross, Keith W., Computernetzwerke, 4. Aufl., München 2008

Kutscha, Martin, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, S. 1042 ff.

– Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte, LKV 2008, S. 481 ff.

– Der Lauschangriff im Polizeirecht der Länder, NJW 1994, S. 85 ff.

– Verdeckte „Online-Durchsuchung" und Unverletzlichkeit des Wohnung, NJW 2007, S. 1169 ff.

Kyas, Othmar/a Campo, Markus, Internet professionell, 2. Aufl., Bonn 2001

Ladeur, Karl-Heinz, Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, DÖV 2009, S. 45 ff.

– Datenverarbeitung und Datenschutz bei neuartigen Programmführern in „virtuellen Videotheken" – Zur Zulässigkeit der Erstellung von Nutzerprofilen, MMR 2000, S. 715 ff.

– Innovationsoffene Regulierung des Internets, Baden-Baden 2003

– Informationelle Selbstbestimmung im Internet, NVwZ 2008, S. 521 ff.

– Persönlichkeitsschutz und „Comedy" – Das Beispiel der Fälle SAT 1/Stahnke und RTL 2/Schröder, NJW 2000, S. 1977 ff.

Lahrmann, Markus, Wehrlose Wächter, RdJB 1997, S. 419 ff.

Lammer, Dirk, Verdeckte Ermittlungen im Strafprozess, Berlin 1992

Lange, Nicole, Staatsanwaltliche Vorermittlungen – ohne rechtliche Grundlage?, DRiZ 2002, S. 264 ff.

– Vorermittlungen – die Behandlung des staatsanwaltlichen Vorermittlungsverfahrens unter besonderer Berücksichtigung von Abgeordneten, Politikern und Prominenten, Frankfurt am Main 1999

Larenz, Karl/Canaris, Claus-Wilhelm, Methodenlehre der Rechtswissenschaft, 3. Aufl., Berlin 1995

Laue, Christian, Strafrecht und Internet – Teil 1, jurisPR-StrafR 13/2009 Anm. 2

– Strafrecht und Internet – Teil 2, jurisPR-StrafR 15/2009 Anm. 2

Leisner, Walter, Das neue „Kommunikationsgrundrecht" – Nicht Alibi für mehr, sondern Mahnung zu weniger staatlicher Überwachung, NJW 2008, S. 2902 ff.

Lerch, Hana/Krause, Beate/Hotho, Andreas/Roßnagel, Andreas/Stumme, Gerd, Social Bookmarking-Systeme – die unerkannten Datensammler, MMR 2010, S. 454 ff.

Lisken, Hans/Denninger, Erhard (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., München 2007

Lisken, Hans/Denninger, Erhard/Rachor, Frederik (Hrsg.), Handbuch des Polizeirechts, 5. Aufl., München 2012

Lorenz, Dieter, Allgemeines Persönlichkeitsrecht und Gentechnologie, JZ 2005, S. 1121 ff.

Lorenz, Marc-Andor, Herausforderungen an das Recht der Informationsgesellschaft, JZ 1996, S. 716 ff.

Löwe-Rosenberg, Riess, Peter (Hrsg.), StPO, Bd. 2, 24. Aufl., Berlin 1989, 25. Aufl., Berlin 2004

Lübbe-Wolff, Gertrude, Satzungsrechtliche Beratungsrechte und Art. 13 GG, DVBl 1993, S. 762 ff.

Luch, Anika Dorthe, Das Medienpersönlichkeitsrecht – Schranke der „vierten Gewalt", Frankfurt am Main 2008

– Das neue „IT-Grundrecht", MMR 2011, S. 75 ff.

von Lucius, Julian, Netzneutralität in der Informationsgesellschaft, NVwZ 2011, S. 218 ff.

Maaßen, Stefan/Hühner, Sebastian, Neue Top-Level-Domains 2011, MMR 2011, S. 148 ff.

Makrutzki, Patric, Verdeckte Ermittlungen im Strafprozess, Berlin 2000

Malek, Klaus, Strafsachen im Internet, Heidelberg 2005

Mallmann, Otto, Das Melderecht nach der Novellierung des Melderechtsrahmengesetzes, NJW 1994, S. 1687 ff.

von Mangoldt, Hermann/Klein, Friedrich/Starck, Christian (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 6. Aufl., München 2010

Manssen, Gerrit, Staatsrecht II, 7. Aufl., München 2010

Marberth-Kubicki, Computer- und Internetstrafrecht, 2. Aufl., München 2010

Maunz, Theodor/Dürig, Günter (Begr.), Grundgesetz-Kommentar, Bd. 1 und 2, München, Stand: April 2012

Mecklenburg, Wilhelm, Internetfreiheit, ZUM 1997, S. 525 ff.

Meinel, Christoph/Sack, Harald, WWW, Berlin 2004

Meininghaus, Florian, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, Hamburg 2007

Meyer, Hans, Versuch über Demokratie in Deutschland, Berlin 2003

Meyerdierks, Per, Sind IP-Adressen personenbezogene Daten?, MMR 2009, S. 8 ff.

Meyer-Goßner, Lutz, Strafprozessordnung, 53. Aufl., München 2010

Meyer-Wieck, Hannes, Der Große Lauschangriff, Berlin 2005

Möller, Mirko, Rechtsfragen im Zusammenhang mit dem Postident-Verfahren, NJW 2005, S. 1605 ff.

Moos, Flemming, Datenschutz im Internet, in: Kröger, Detlef/Gimmy, Marc A., Handbuch zum Internetrecht, Berlin 2000

Möstl, Markus, Gefahr und Kompetenz, Jura 2005, S. 48 ff.

– Vorratsdatenspeicherung – wie geht es weiter?, ZRP 2011, S. 225 ff.

Mozek, Martin, Der „große Lauschangriff", Aachen 2001

Mühlberger, Sven J., Die Haftung des Internetanschlussinhabers bei Filesharing-Konstellationen nach den Grundsätzen der Störerhaftung, GRUR 2009, S. 1022 ff.

Müller, Martin, Der sogenannte „Große Lauschangriff", Marburg 2000

von Münch, Ingo/Kunig, Philip (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 6. Aufl., Stuttgart (u. a.) 2012

von Mutius, Albert, Anonymität als Element des allgemeinen Persönlichkeitsrechts, in: Bäumler, Helmut/von Mutius, Albert (Hrsg.), Anonymität im Internet, Wiesbaden 2003, S. 12 ff.

Neuhöfer, Daniel, Der Zugriff auf serverbasierte gespeicherte E-Mails beim Provider, Hamburg 2011

Nitz, Holger, Einsatzbedingte Straftaten verdeckter Ermittler, Hamburg 1997

Nolte, Norbert, Zum Recht auf Vergessen – Von digitalen Radiergummis und anderen Instrumenten, ZRP 2011, S. 236 ff.

Ohlenburg, Anna, Die neue EU-Datenschutzrichtlinie 2002/58/EG – Auswirkungen und Neuerungen für elektronische Kommunikation, MMR 2003, S. 82 ff.

– Der neue Telekommunikationsdatenschutz – Eine Darstellung von Teil 7 Abschnitt 2 TKG, MMR 2004, S. 431 ff.

Ostendorf, Heribert/Frahm, Lorenz Nicolai/Doege, Felix, Internetaufrufe zur Lynchjustiz und organisiertes Mobbing, NStZ 2012, S. 529 ff.

Ott, Stephan, Das Internet vergisst nicht – Rechtsschutz für Suchobjekte?, MMR 2009, S. 158 ff.

– Datenschutzrechtliche Zulässigkeit von Webtracking?, K&R 2009, S. 308 ff.

Pahlen-Brandt, Ingrid, Zur Personenbezogenheit von IP-Adressen, K&R 2008, S. 288 ff.

Pätzel, Claus, Das Internet als Fahndungshilfsmittel der Strafverfolgungsbehörden, NJW 1997, S. 3131 ff.

Perrey, Elke, Gefahrenabwehr und Internet, München 2002

Perschke, Stefan, Die Zulässigkeit nicht spezialgesetzlich geregelter Ermittlungsmethoden im Strafverfahren, Köln 1997

Peterson, Larry L./Davie, Bruce S., Computernetze, Deutsche Ausgabe der 4. amerikanischen Auflage, Heidelberg 2008

Petri, Thomas, Wertewandel im Datenschutz und die Grundrechte, DuD 2010, S. 25 ff.

– Das Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung“, DuD 2008, S. 443 ff.

Pfeiffer, Gerd, Strafprozessordnung, Kommentar, 5. Aufl., München 2005

Pieroth, Bodo/Schlink, Bernhard, Grundrechte Staatsrecht II, 26 Aufl., Heidelberg 2010

Pieroth, Bodo/Schlink, Bernhard/Kniesel, Michael, Polizei- und Ordnungsrecht, 6. Aufl., München 2010

Pils, Michael Johannes, Zum Wandel des Gefahrenbegriffs im Polizeirecht, DÖV 2008, S. 941 ff.

Pitschas, Rainer, Informationelle Selbstbestimmung zwischen digitaler Ökonomie und Internet, DuD 1998, S. 139 ff.

Placzek, Thomas, Allgemeines Persönlichkeitsrecht und privatrechtlicher Informations- und Datenschutz, Hamburg 2006

Poppenhäger, Holger, Informationelle Gewaltenteilung, Zulässigkeit und Grenzen der Nutzung personenbezogener Daten für statistische Zwecke und Zwecke des Verwaltungsvollzugs, NVwZ 1992, S. 149 ff.

Putzhammer, Barbara, Die Einwilligung in strafprozessuale Grundrechtsbeeinträchtigungen, München 2007

Rasmussen, Heike, Gesetzgeberische Maßnahmen zur Verhinderung der Erstellung ungewollter Nutzerprofile im Web, CR 2002, S. 36 ff.

Reppesgaard, Lars, Das Google-Imperium, Hamburg 2008

Riepl, Frank, Informationelle Selbstbestimmung im Strafverfahren, Tübingen 1998

Rogall, Klaus, Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht, Tübingen 1992

Roggan, Fredrik (Hrsg.), Online-Durchsuchungen, Berlin 2008

– Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur, NJW 2009, S. 257 ff.

– Große Lauschangriffe, in: Roggan, Fredrik/Kutscha, Martin (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., Berlin 2006

– Die Videoüberwachung von öffentlichen Plätzen, NVwZ 2001, S. 134 ff.

Rohde, Franz, Die Nachzensur in Art. 5 Abs. 1 Satz 3 GG, Kiel 1997

Röll, Marcus/Brink, Stefan, Kriminologische Erkenntnisse zum Nutzen von Videoüberwachung, LKRZ 2011, Teil 1 und 2, S. 330 ff., S. 373 ff.

Rosengarten, Carsten/Römer, Sebastian, Der „virtuelle verdeckte Ermittler“ in sozialen Netzwerken und Internetboards, NJW 2012, S. 1764 ff.

Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, München 2003

– Handbuch der Multimediadienste, Kommentar, München, Stand: April 2005

Roßnagel, Alexander/Schnabel, Christoph, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, S. 3534 ff.

Roßnagel, Alexander/Scholz, Philip, Datenschutz durch Anonymität und Pseudonymität, MMR 2000, S. 721 ff.

Ruder, Karl-Heinz/Schmitt, Steffen, Polizeirecht Baden-Württemberg, 7. Aufl., Baden-Baden 2011

Rudolphi, Hans-Joachim/Frisch, Wolfgang/Paeffgen, Hans-Ullrich/Rogall, Klaus/Schlüchter, Ellen/Wolter, Jürgen, Systematischer Kommentar zur Strafprozeßordnung und zum Gerichtsverfassungsgesetz, Band 3, München, Stand: Oktober 2009

Rux, Johannes, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, JZ 2007, S. 285 ff.

Sachs, Michael (Hrsg.), Grundgesetz-Kommentar, 6. Aufl., München 2011

Sachs, Michael/Krings, Thomas, Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", JuS 2008, S. 481 ff.

Säcker, Franz Jürgen (Hrsg.), Berliner Kommentar zum Telekommunikationsgesetz, 2. Aufl., Frankfurt am Main 2009

Santifaller, Michael, TCP/IP und ONC/NFS, 4. Aufl., Bonn 1998

Schaar, Peter, Datenschutz im Internet, München 2002

– Datenschutzrechtliche Einwilligung im Internet, MMR 2001, S. 644 ff.

– Datenschutzfreier Raum Internet?, CR 1996, S. 170 ff.

Schaar, Peter/Landwehr, Sebastian, Anmerkung zum Beschluss des BGH vom 31.1.2007 – StB 18/06 – zur verdeckten Online-Durchsuchung, K&R 2007, S. 202 ff.

Schenke, Wolf-Rüdiger, Polizei- und Ordnungsrecht, 6. Aufl., Heidelberg 2009

– Verfassungsrechtliche Grenzen des polizeilichen Gewahrsams und polizeilicher Informationseingriffe, DVBl 1996, S. 1393 ff.

Schertz, Christian, Der Schutz des Individuums in der modernen Mediengesellschaft, NJW 2013, S. 721 ff.

Schlegel, Stephan, Warum die Festplatte keine Wohnung ist – Art. 13 GG und die „Online-Durchsuchung", GA 2007, S. 648 ff.

Schmidt-Jortzig, Immo Joachim, Ermittlungskompetenzen des BKA, Frankfurt am Main 2009

Schmidt-Bleibtreu, Bruno/Hofmann, Hans/Hopfauf, Axel (Hrsg.), Grundgesetz-Kommentar, 12. Aufl., München 2011

Schmitz, Monika, Rechtliche Probleme des Einsatzes verdeckter Ermittler, Frankfurt am Main 1996

Schnabel, Christoph, Polizeiliche Videoüberwachung öffentlicher Räume nach § 8 III HbgPolDVG am Beispiel der Reeperbahn-Entscheidung des OVG Hamburg, NVwZ 2010, S. 1457 ff.

Schneider, Gerhard, Sperren und Filtern im Internet, MMR 2004, S. 18 ff.

Schneider, Hans, Verfassungsrechtliche Beurteilung des Volkszählungsgesetzes 1983, DÖV 1984, S. 161 ff.

Schoch, Friedrich, Das Recht auf informationelle Selbstbestimmung, Jura 2008, S. 352 ff.

– Die „Gefahr" im Polizei- und Ordnungsrecht, Jura 2003, S. 472 ff.

Scholz, Rupert/Pitschas, Rainer, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin 1984

Schöttle, Hendrik, Sperrungsverfügungen im Internet: Machbar und verhältnismäßig?, K&R 2007, S. 366 ff.

Schramm, Marc/Wegener, Christoph, Neue Anforderungen an eine anlasslose Speicherung von Vorratsdaten – Umsetzungsmöglichkeiten der Vorgaben des Bundesverfassungsgerichts, MMR 2011, S. 9 ff.

Schwenke, Matthias Christoph, Individualisierung und Datenschutz, Wiesbaden 2006

Schulz, Sönke E./Hoffmann, Christian, Grundrechtsrelevanz staatlicher Beobachtungen im Internet, CR 2010, S. 131 ff.

Schulz, Sönke E., Rechtsprobleme des Identitätsmanagements, DuD 2009, S. 601 ff.

Seidel, Gerd, Das Versammlungsrecht auf dem Prüfstand, DÖV 2002, S. 283 ff.

Seidel, Janine/Nink, Judith, Personensuchmaschinen, CR 2009, S. 666 ff.

Seifert, Fedor, Postmortaler Schutz des Persönlichkeitsrechts und Schadensersatz – Zugleich ein Streifzug durch die Geschichte des allgemeinen Persönlichkeitsrechts, NJW 1999, S. 1889 ff.

Sieber, Ulrich/Nolde, Malaika, Sperrverfügungen im Internet, Berlin 2008

Siegel, Thorsten, „Spiel ohne Grenzen" – Grundrechtliche Schranken der Videoüberwachung durch öffentliche Stellen und Private, VerwArch 2011, S. 159 ff.

Siegert, Marco, Das Internet – Grundlagenwissen für die Polizei, Berlin 2002

Siekmann, Helmut/Duttge, Gunnar, Staatsrecht Bd. 1 Grundrechte, 3. Aufl., Nürnberg 2000

Sievers, Malte, Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes, Baden-Baden 2003

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz-Kommentar, 6. Aufl., Baden-Baden 2006

– Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, S. 394 ff.

Simitis, Spiros/Fuckner, Gerhard, Informationelle Selbstbestimmung und „staatliches Geheimhaltungsinteresse", NJW 1990, S. 2713 ff.

Singelnstein, Tobias, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, S. 593 ff.

Sodan, Helge (Hrsg.), Grundgesetz-Kommentar, München 2009

Soiné, Michael, Fahndung via Internet – 1. Teil, NStZ 1997, S. 166 ff.

– Fahndung via Internet – 2. Teil, NStZ 1997, S. 321 ff.

– Verdeckte Ermittler als Instrument zur Bekämpfung der Kinderpornographie im Internet, NStZ 2003, S. 225 ff.

– Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder, NVwZ 2012, S. 1585 ff.

Söllner, Sebastian/Wecker, Sven-Erik, Bewegung der Massen durch Facebook, ZRP 2011, S. 179 ff.

Son, Jae-Young, Heimliche polizeiliche Eingriffe in das informationelle Selbstbestimmungsrecht, Berlin 2006

Spiegel, Gerald, Spuren im Netz, DuD 2003, S. 265 ff.

Spies, Axel, Netzneutralität – Wovon reden wir eigentlich?, MMR 2010, S. 585 ff.

Spindler, Gerald/Schuster, Fabian (Hrsg.), Recht der elektronischen Medien, Kommentar, 2. Aufl., München 2011

Sproß, Joachim, Das Hamburgische Sicherheits- und Polizeigesetz in einer verfassungsrechtlichen Würdigung, NVwZ 1992, S. 642 ff.

Stadler, Thomas, Sperrungsverfügungen gegen Access-Provider, MMR 2002, S. 343 ff.

– Zulässigkeit der heimlichen Installation von Überwachungssoftware – Trennung von Online-Durchsuchung und Quellen-Telekommunikationsüberwachung möglich?, MMR 2012, S. 18 ff.

Steidle, Roland/Pordesch, Ulrich, Im Netz von Google. Web-Tracking und Datenschutz, DuD 2008, S. 324 ff.

Stein, Erich, Taschenbuch Rechnernetze und Internet, 2. Aufl., München 2004

Steinle, Thomas, Internetkriminalität – Begriff, Ursachen und Wege der Bekämpfung, Die Polizei 2004, S. 296 ff.

Stern, Klaus/Becker, Florian (Hrsg.), Grundrechte-Kommentar, Köln 2010

Stern, Klaus, Das Staatsrecht der Bundesrepublik Deutschland, Bd. III/2, München 1994

Stögmüller, Thomas, Vertraulichkeit und Integrität informationstechnischer Systeme in Unternehmen, CR 2008, S. 435 ff.

Taeger, Jürgen, Kundenprofile im Internet, K&R 2003, S. 220 ff.

Tanenbaum, Andrew S., Computernetzwerke, 4. Aufl., München 2003

Tiedemann, Paul, Von den Schranken des allgemeinen Persönlichkeitsrechts, DÖV 2003, S. 74 ff.

Tinnefeld, Marie-Theres, Persönlichkeitsrecht und Modalitäten der Datenerhebung im Bundesdatenschutzgesetz, NJW 1993, S. 1117 ff.

Tinnefeld, Marie-Theres/Ehmann, Eugen/Gerling, Rainer W., Einführung in das Datenschutzrecht, 4. Aufl., München 2005

Tischer, Birgit, Das System der informationellen Befugnisse der Polizei, Frankfurt am Main 2004

Tröndle, Rüdiger, „Privacy Policies" und das Internet, CR 1999, S. 717 ff.

Valerius, Brian, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, Berlin 2004

– Ermittlungsmaßnahmen im Internet, JR 2007, S. 275 ff.

Vogelgesang, Klaus, Grundrecht auf informationelle Selbstbestimmung?, Baden-Baden 1987

Voigt, Paul, Datenschutz bei Google, MMR 2009, S. 377 ff.

Volkmann, Uwe, Verfassungsmäßigkeit der Vorschriften des Verfassungsschutzgesetzes von Nordrhein-Westfalen zur Online Durchsuchung und zur Internet-Aufklärung, DVBl 2008, S. 590 ff.

Voßkuhle, Andreas, Der Gefahrenbegriff im Polizei- und Ordnungsrecht, JuS 2007, S. 908 ff.

Wabnitz, Heinz-Bernd (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 3. Aufl., München 2007

Wagner, Sylke, Das Websurfen und der Datenschutz, Frankfurt am Main 2006

Wanckel, Endress, Persönlichkeitsschutz in der Informationsgesellschaft, Frankfurt am Main 1999

Warntjen, Maximilian, Die verfassungsrechtlichen Anforderungen an eine gesetzliche Regelung der Online-Durchsuchung, Jura 2007, S. 581 ff.

Warren, Samuel/Brandeis, Louis, The Right to Privacy, Havard Law Review 1890, S. 193 ff.

Wegener, Bernhard W./Muth, Sven, Das „neue Grundrecht" auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Jura 2010, S. 847 ff.

Weichert, Thilo, Datenschutz bei Suchmaschinen, MR-Int 2007, S. 188 ff.

– Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, S. 1463 ff.

Weisser, Niclas-Frederic, Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) – Rechtsprobleme, Rechtsform und Rechtsgrundlage, NVwZ 2011, S. 142 ff.

Welsing, Ruth, Das Recht auf informationelle Selbstbestimmung im Rahmen der Terrorabwehr. Darstellung anhand einer Untersuchung der präventiven Rasterfahndung, Hamburg 2009

Weßlau, Edda, Vorfeldermittlungen, Berlin 1989

Wick, Manfred, Gefahrenabwehr – Vorbeugende Verbrechensbekämpfung – Legalitätsprinzip, DRiZ 1992, S. 217 ff.

Wiedemann, Gregor, Regieren mit Datenschutz und Überwachung – Informationelle Selbstbestimmung zwischen Sicherheit und Freiheit, Marburg 2011

Wiegrefe, Carsten, Polizei im Internet, Bürgerrechte & Polizei/CILIP 55 (3/96), S. 67 ff.

Wilms, Jan/Roth, Jan, Die Anwendbarkeit des Rechts auf informationelle Selbstbestimmung auf juristische Personen i. S. von Art. 19 III GG, JuS 2004, S. 577 ff.

Woitke, Thomas, Web-Bugs – Nur lästiges Ungeziefer oder datenschutzrechtliche Bedrohung?, MMR 2003, S. 310 ff.

Wolf, Heinz/Stephan, Ulrich/Deger, Johannes, Polizeigesetz für Baden-Württemberg, 6. Aufl., Stuttgart 2009

Wolff, Heinrich Amadeus, Die Grenzverschiebung von polizeilicher und nachrichtendienstlicher Sicherheitsgewährleistung, DÖV 2009, S. 597 ff.

Wolter, Jürgen, Heimliche und automatisierte Informationseingriffe wider Datengrundrechtsschutz, GA 1988, S. 49 ff.

Wulff, Christian, Befugnisnormen zur vorbeugenden Verbrechensbekämpfung in den Landespolizeigesetzen, Aachen 2003

Würtenberger, Thomas/Heckmann, Dirk, Polizeirecht in Baden-Württemberg, 6. Aufl., Heidelberg 2005

Würtenberger, Thomas, Das Polizei- und Sicherheitsrecht vor den Herausforderungen des Terrorismus, in: Masing, Johannes/Jouanjan, Olivier, Terrorismusbekämpfung, Menschenrechtsschutz und Föderation, Tübingen 2008

Würtenberger, Thomas/Schenke, Ralf Peter, Der Schutz von Amts- und Berufsgeheimnissen im Recht der polizeilichen Informationserhebung, JZ 1999, S. 548 ff.

Würz, Karl, Polizeiaufgaben und Datenschutz in Baden-Württemberg, Stuttgart 1993

Zimmer, Heiko, Zugriff auf Internetzugangsdaten, Frankfurt am Main 2012

Zippelius, Reinhold, Juristische Methodenlehre, 10. Aufl., München 2006

Zippelius, Reinhold/Würtenberger, Thomas/Maunz, Theodor (Begr.), Deutsches Staatsrecht, 32. Aufl., München 2008

Zöller, Mark Alexander, Verdachtslose Recherchen und Ermittlungen im Internet, GA 2000, S. 563 ff.

– Möglichkeiten und Grenzen polizeilicher Videoüberwachung, NVwZ 2005, S. 1235 ff.

– Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, Heidelberg 2002

Zscherpe, Kerstin A., Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR 2004, S. 723 ff.