.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Möstl, Markus (2010):

Datenverfügbarkeit als Voraussetzung für innere Sicherheit. Ein Bericht aus Deutschland

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2), 61-69.

doi: 10.7396/2010_2_F

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Möstl, Markus (2010). Datenverfügbarkeit als Voraussetzung für innere Sicherheit. Ein Bericht aus Deutschland, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2), 61-69, Online: http://dx.doi.org/10.7396/2010_2_F.

Online publiziert: 3/2013

Ein Bericht aus Deutschland[1]

Datenverfügbarkeit als Voraussetzung für innere Sicherheit

MARKUS MÖSTL,
Universitätsprofessor am Lehrstuhl für Öffentliches Recht II, Universität Bayreuth.

Das Spannungsverhältnis von Freiheit und Sicherheit tritt derzeit nirgends deutlicher zu Tage als auf dem Felde der Datenverfügbarkeit, der Frage also, was Sicherheitsbehörden wissen dürfen und wann ihnen welche Ermittlungsmethoden zur Verfügung stehen. Der vorliegende Landesbericht aus Deutschland behandelt – unter besonderer Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts – vier aktuelle Problemkreise, die das Spannungsverhältnis von Freiheit und Sicherheit auf dem Felde der Datenverfügbarkeit exemplarisch beleuchten: Der erste Problemkreis betrifft die Frage nach angemessenen Eingriffsschwellen im präventiven Polizeirecht, vor allem soweit es um so genannte „Vorfeldbefugnisse" geht. Zum Zweiten werden Fragen des Schutzes des Kernbereichs privater Lebensgestaltung untersucht. Ein Augenmerk gilt drittens den durch die europarechtliche Vorratsdatenspeicherung aufgeworfenen Verfassungsfragen. Zu klären ist schließlich das Verhältnis von Polizei und Nachrichtendiensten, insbesondere hinsichtlich der Frage, inwieweit sich aus dem so genannten Trennungsgebot von Polizei und Nachrichtendiensten Grenzen für deren kooperatives Zusammenwirken ergeben.

1. EINLEITUNG

Ob mehr Sicherheitsgewährleistung weniger Freiheit bedeutet oder ob umgekehrt Freiheit ohne Sicherheit nicht denkbar ist, ist ein ewiger Streit[2] – ein Streit, der nicht einseitig auflösbar ist, denn beides ist richtig: Es sind dieselben Grundrechte, die den Staat – als Schutzpflichten – zu einer effektiven Sicherheitsgewährleistung verpflichten und ihn hierbei – als Abwehrrechte – zugleich in die Schranken weisen. Es ist dasselbe Rechtsstaatsprinzip, das sowohl auf effektive Rechtsdurchsetzung dringt als auch diese zu mäßigen sucht. Das Spannungsverhältnis von Freiheit und Sicherheit ist demnach in den Grundrechten und dem Rechtsstaatsprinzip selbst angelegt[3]; und es darf nicht gehofft werden, dass es einfache Großformeln der Lösung gäbe (etwa wie: „in dubio pro libertate"). Vielmehr helfen allein das mühsame Durchexerzieren des Verhältnismäßigkeitsprinzips und der sorgfältige Blick auf den einzelnen Fall, das Ringen um die Frage also, ob eine bestimmte freiheitsbeschränkende Maßnahme der Sicherheitsgewährleistung in der konkreten Situation oder Lage tatsächlich erforderlich und zumutbar ist.

Das Spannungsverhältnis von Freiheit und Sicherheit ist in den letzten Jahren nirgends deutlicher zu Tage getreten als auf dem Felde der Datenverfügbarkeit, der Frage also, was Sicherheitsbehörden wissen dürfen und wann ihnen welche Ermittlungsmethoden zur Verfügung stehen. Ein Blick auf die Gesetzgebung wie auf die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) macht dies gleichermaßen deutlich. In der Gesetzgebung ist eine

rasante Entwicklung des sicherheitsbehördlichen Informationsrechts zu verzeichnen. Das Recht der verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung (StPO) hat eine umfassende Novellierung erhalten.[4] Im Landes-Polizeirecht wurde der Bereich Datenverarbeitung seit der „Entdeckung" des Rechts auf informationelle Selbstbestimmung[5] zunehmend verrechtlicht, aber auch um vielerlei neuartige Befugnisse – von der Video-, Wohnraum- und Telekommunikationsüberwachung bis zur Online-Durchsuchung – angereichert.[6] Dem Bundeskriminalamt wurden im Gefolge der Föderalismusreform erstmals präventive Befugnisse der Terrorismusbekämpfung eingeräumt[7], und erneut standen vor allem die Ermittlungsbefugnisse im Zentrum der Diskussion der Novellierung des Bundeskriminalamtgesetzes (BKAG). In den Polizeigesetzen nehmen die neuartigen Datenerhebungs- und -verarbeitungsbefugnisse im Vergleich zu den klassischen Standardmaßnahmen mittlerweile den größten Regelungsraum ein und unterstreichen damit, dass modernes Polizeirecht vor allem Informationsrecht ist. Auch die Nachrichtendienste werden verstärkt für Zwecke der Kriminalitätsbekämpfung in Dienst genommen und mit der Polizei vernetzt.[8] Mit der Vorratsdatenspeicherung von Telekommunikationsdaten ist jüngst ein wiederum neuartiges Instrument der präventiven Sicherung von Informationsspuren hinzugekommen.[9]

Die Rechtsentwicklung gibt insgesamt beredtes Zeugnis davon ab, dass für die Kriminalitätsbekämpfung vor allem Wissen benötigt wird.

Dem staatlichen Drang nach Wissen freilich stehen die Freiheitsrechte entgegen, und so verwundert es nicht, dass das BVerfG die aufgezeigte Rechtsentwicklung rahmensetzend wie richtungsweisend zu begleiten hatte. In einer beeindruckenden Rechtsprechungsreihe der letzten Jahre – Großer Lauschangriff, niedersächsische Telefonüberwachung, Rasterfahndung, Online-Durchsuchung sind die entscheidenden Stationen[10] – hat sich in rascher Folge eine sich zunehmend konsolidierende, aber auch nach wie vor viele Fragen aufwerfende Doktrin zu den verdeckten Ermittlungsmaßnahmen entwickelt. Weitere Entscheidungen werden folgen; zur Vorratsdatenspeicherung sind einstweilige Anordnungen ergangen[11]; auch zum neuen BKAG ist bereits eine Verfassungsbeschwerde anhängig.[12] Die vom BVerfG entwickelten prozeduralen und materiellen Kriterien, die von ihm aufgestellten relativen und absoluten Schranken sind komplex und schwer überschaubar; die meist seitenlangen und immer unübersichtlicher werdenden Befugnisnormen auf dem Felde der Datenerhebung spiegeln diese Komplexität eindrucksvoll wider. Es ist hier nicht der Ort, all diese Einzelfragen umfassend würdigen zu können. Vielmehr will sich dieser Beitrag auf vier größere Problemkreise konzentrieren, die das Spannungsverhältnis von Freiheit und Sicherheit auf dem Felde der Datenverfügbarkeit exemplarisch beleuchten.

2. FRAGEN DER EINGRIFFSSCHWELLE – GEFAHR UND VORFELD

Der erste Problemkreis betrifft die Frage nach der angemessenen Eingriffsschwelle für Ermittlungsbefugnisse im präventiven Polizeirecht und damit das zentrale Konstruktionsmerkmal der einschlägigen Befugnisnormen.[13] Kern des Streits ist, ob die Polizei auch bei der Datenverarbeitung an ihre klassische Eingriffsschwelle der konkreten Gefahr gebunden sein soll oder mit der Informationserhebung bereits im Vor-

feld konkreter Gefahren ansetzen darf. Die Praxis hält Vorfeldbefugnisse für unverzichtbar, und sie haben auch Einzug in das Polizeirecht gehalten; unter dem Schlagwort der „vorbeugenden Bekämpfung von Straftaten“[14] haben sie ein programmatisches Leitbild erhalten. Eine breite Gegenströmung hält diese Entwicklung für prinzipiell problematisch, befürchtet ein Abgleiten in den „Präventionsstaat“, beklagt die „Erosion“ des Gefahrbegriffs als der klassischen rechtsstaatlichen Eingriffsschwelle.[15]

Auch das BVerfG hat noch zu keiner wirklich klaren Linie gefunden.

Im Urteil zur niedersächsischen Telefonüberwachung hat es Vorfeldbefugnisse auch bei intensiven Eingriffen nicht per se ausgeschlossen, andererseits aber die rechtsstaatlichen Risiken solcher Vorfeldbefugnisse betont und sie deswegen – gleichsam kompensatorisch – an sehr hohe Bestimmtheitsanforderungen geknüpft.[16] In Sachen Rasterfahndung dagegen – an sich einem weniger tiefen Eingriff – hat es die Schwelle der konkreten Gefahr für unverzichtbar gehalten, einen Einsatz im Vorfeld also ausgeschlossen, obwohl Rasterfahndungen, wenn überhaupt, gerade als Instrument der Vorfeldaufklärung Sinn machen dürften.[17] Im Urteil zur Online-Durchsuchung hingegen – obwohl wiederum einen weitaus tieferen Eingriff betreffend – hat es eine Eingriffsschwelle beschrieben, die, indem sie nur „tatsächliche Anhaltspunkte einer konkreten Gefahr“ und noch nicht in jedem Fall die „hinreichende Wahrscheinlichkeit, dass die Gefahr schon in näherer Zukunft eintritt“, verlangt, nahezu einhellig so interpretiert wurde, dass das BVerfG offenbar eine immerhin leichte Verlagerung ins Gefahrenvorfeld zulassen wollte.[18] Die Unsicherheit ist also groß, und die divergierende Gesetzgebungspraxis spiegelt diese Unsicherheit wider. Zwei Thesen können nach hier vertretener Ansicht einen Ausweg weisen.

These 1: Informationsbeschaffung und Gefahraufklärung im Gefahrenvorfeld sind nicht etwas per se Problematisches oder besonders Rechtfertigungsbedürftiges; sie bedeuten keine Erosion klassischer Gefahrenabwehr, sondern sind ihre logische Ergänzung.[19] Das Polizeirecht ist – richtig betrachtet – kein einheitlicher dogmatischer Block, für den insgesamt allein die klassische Gefahr-Störer-Dogmatik maßgebend sein könnte. Entwickelt wurde diese Dogmatik für Gefahrbeseitigungseingriffe, dh für Maßnahmen, durch die die Polizei in schadensträchtige Kausalverläufe eingreift und diese unterbricht. Die Unterbrechung des schadensträchtigen Kausalverlaufs – so die Grundidee der Gefahr-Störer-Dogmatik – soll der Polizei erst ab der Schwelle hinreichender Wahrscheinlichkeit (dh nicht im Gefahrenvorfeld) und nur gegenüber dem Störer möglich sein. Auf bloße Ermittlungseingriffe hingegen, durch die die Polizei gerade noch nicht in schadensträchtige Kausalverläufe eingreift, sondern zunächst nur Informationen über solche erhebt, lässt sich diese Gefahr-Störer-Dogmatik nicht ohne weiteres übertragen. Denn es kann zwar sein, dass Ermittlungsbefugnisse auch noch dann Sinn machen und gleichsam als erster Schritt der Gefahrenabwehr zum Einsatz kommen sollen, wenn bereits eine konkrete Gefahr festgestellt wurde. Geradezu typischerweise jedoch werden Ermittlungsmaßnahmen dem Zweck dienen, auf der Basis bestimmter Verdachtsmomente festzustellen, ob und ggf wo überhaupt eine konkrete Gefahr besteht (Gefahraufklärung). Gerade unter den Bedingungen moderner (häufig abgeschottet operierender) Kriminalitätsformen wird

es, soll effektive Gefahrenabwehr möglich bleiben, häufig unumgänglich sein, nicht zuzuwarten, bis konkrete Gefahren von sich aus zu Tage treten (weil es für ein Eingreifen dann bereits zu spät ist), sondern die Ermittlungen bereits im Gefahrenvorfeld ansetzen zu lassen, um Gefahren rechtzeitig erkennen zu können. Wenn polizeiliche Ermittlungsmaßnahmen aber geradezu typischerweise dem Zweck dienen, verdachtsgestützt aufzuklären, ob und wo genau konkrete Gefahren bestehen, so ist es logisch sinnlos, derartige Maßnahmen der Gefahraufklärung an die Eingriffsschwelle der konkreten Gefahr binden zu wollen oder sie deswegen als bedenkliche Abkehr von klassischen Eingriffsschwellen zu diskreditieren, weil sie nicht an die Gefahrenschwelle gebunden sind.

Gefahraufklärung im Gefahrenvorfeld ist keinerlei Abkehr von klassischer Gefahrenabwehr, sondern im Gegenteil ihre natürliche und notwendige Ergänzung.

Gerade weil die Gefahrenschwelle für kausalverlaufsrelevante Gefahrbeseitigungseingriffe aus rechtsstaatlichen Gründen stets eine hinreichende Schadenswahrscheinlichkeit, dh einen hinreichend fundierten Kenntnisstand, verlangt, der die Gefahrprognose zu tragen vermag, setzt sie geradezu zwingend voraus, dass im Vorfeld der Gefahrbeseitigung auch diejenigen Informationen erhoben werden dürfen, die für eine fundierte Gefahrprognose nötig sind.

These 2: Das polizeiliche Vorfeldrecht bedarf – zum Schutz der Freiheitsrechte – einer angemessenen rechtsstaatlichen Systembildung, der Entwicklung eines abgestuften Systems adäquater Eingriffsschwellen, die an die Stelle des – hier untauglichen – Gefahrbegriffs treten können.[20] Hier sind wir noch ganz am Anfang; hierauf sollte sich unser Augenmerk richten. Grundsätzlich zweifelhaft erscheint, ob der vom BVerfG im Urteil zur niedersächsischen Telefonüberwachung[21] beschrittene Ausweg, vor allem die rechtsstaatlichen Bestimmtheitsanforderungen an die detaillierte gesetzgeberische Umschreibung zulässiger Eingriffsanlässe nach oben zu schrauben, wirklich tragfähig ist; die informationellen Befugnisnormen leiden bereits jetzt an einer kaum mehr überschaubaren Länge und Unübersichtlichkeit; hier die Anforderungen noch weiter in die Höhe zu treiben, könnte dem rechtsstaatlichen Anliegen der Normenklarheit letztlich mehr schaden als nützen. Als anknüpfungsfähiger erweisen sich dagegen die Ausführungen im Online-Durchsuchungsurteil. Mit seiner Anforderung, dass bestimmte Tatsachen „im Einzelfall" „zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahmen gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden können"[22], formuliert das Gericht eine Eingriffsschwelle, die als „konkreter personenbezogener Gefahrverdacht" bezeichnet werden könnte und eine im Gefahrenvorfeld angesiedelte Gefahrverdachtsstufe umschreibt, die für besonders schwerwiegende Ermittlungseingriffe prädestiniert erscheint. Für weniger eingriffsintensive Ermittlungsmaßnahmen lässt sich der zu fordernde Gefahrverdachtsgrad adäquat abstufen – bis hinunter zum „abstrakten, rein lagebezogenen Gefahrverdacht", wie er zB für die Schleierfahndung zu fordern wäre. In der Entwicklung abgestufter Gefahrverdachtsgrade liegt der Schlüssel zur dog-

matischen Durchdringung des polizeilichen Vorfeldrechts.

3. FRAGEN DES SCHUTZES DES KERNBEREICHS PRIVATER LEBENSGESTALTUNG

Der zweite hier zu behandelnde Problemkreis betrifft den Schutz des Kernbereichs privater Lebensgestaltung, wie er durch die Menschenwürdegarantie in Art 1 Abs 1 Grundgesetz (GG) geboten ist. Im Urteil zum Lauschangriff[23] hat ihn das BVerfG erstmals voll entfaltet – mit weittragenden Konsequenzen für die nach Art 13 GG an sich zulässige Wohnraumüberwachung: Verbot der Überwachung in bestimmten Räumen und in Bezug auf Gespräche mit bestimmten Vertrauenspersonen; Pflicht zum Live-Mithören und ggf Abschalten, sobald der Kernbereich berührt ist.

Im Blick auf das Spannungsverhältnis von Freiheit und Sicherheit ist der Kernbereichsschutz interessant.

Und zwar deswegen, weil er, da die Menschenwürde unter dem Grundgesetz ja absolut geschützt und abwägungsfest ist, eine äußere und durch Sicherheitsinteressen nicht relativierbare Grenze staatlicher Ermittlungstätigkeit zu statuieren verspricht. Diese Erwartung wird auf den ersten Blick indes nicht voll eingelöst. Scheinbar paradoxerweise ist die Rechtsprechung des BVerfG zum Kernbereichsschutz nämlich dadurch geprägt, dass – trotz aller Unantastbarkeit der Menschenwürde – ein Eindringen in den Kernbereich nicht unter allen Umständen unterbleiben muss, sondern es in bestimmten Fällen praktisch unvermeidbarer Kernbereichseingriffe auch ausreichen kann, wenn erlangte Kernbereichsdaten nur unverzüglich gelöscht und nicht weiter verwertet werden. Wird dadurch der vermeintlich absolute Kernbereichsschutz aber nicht faktisch auf ein Optimierungsgebot reduziert? Die scheinbare Paradoxie löst sich auf, wenn man, wie zu Recht gesagt wurde, den Kernbereichsschutz nicht im Sinne einer schlechthin unberührbaren Sphäre verräumlicht, sondern als ein verfassungsgebotenes prozedurales Schutzkonzept begreift, das dem absoluten Achtungsanspruch der Menschenwürde insgesamt hinreichend gerecht wird.[24] Im Online-Durchsuchungsurteil hat das BVerfG näher präzisiert, wie dieses Schutzkonzept auszusehen hat, und von einem 2-stufigen Schutzkonzept gesprochen[25]: Auf der ersten Stufe hat der Gesetzgeber danach sicherzustellen, dass bereits die Erhebung von Kernbereichsdaten – soweit wie informations- und ermittlungstechnisch möglich – unterbleibt. Dies wird je nach Ermittlungsmaßnahme unterschiedlich weitreichend der Fall sein; während sich bei der Wohnraumüberwachung zB Prognosen anstellen und Kernbereichseingriffe oft vermeiden lassen, ist dies bei der Online-Durchsuchung praktisch unmöglich. Je weniger sich eine Erhebung von Kernbereichsdaten auf der ersten Stufe vermeiden lässt, umso wichtiger wird sodann die zweite Stufe, die nunmehr die Phase der Durchsicht und Auswertung betrifft. Auf ihr ist durch geeignete Verfahrensgestaltungen sicherzustellen, dass erhobene Kernbereichdaten unverzüglich gelöscht und nicht weiter verwertet werden. Die so umrissene Präzisierung durch das BVerfG hat viel zur Klärung beigetragen; dennoch bleiben im Detail viele Fragen offen.

4. FRAGEN DER VORRATSDATENSPEICHERUNG

Ein weiterer Problemkomplex betrifft die auf einer europäischen Richtlinie[26] beruhende Vorratsdatenspeicherung von Telekommunikationsdaten nach dem Telekom-

munikationsgesetz (TKG) einerseits und den polizei- bzw. strafprozessrechtlichen Regeln für den Abruf dieser Daten durch die Sicherheitsbehörden andererseits. Zwei Fragenkreise sind hier auseinanderzuhalten:

Der eine Fragenkreis betrifft die scheinbar technische, für die Beurteilung der Verfassungsmäßigkeit jedoch nichtsdestoweniger wichtige Frage nach der Verteilung der Eingriffsbeiträge und Rechtfertigungslasten zwischen TKG einerseits und Fachrecht (also StPO oder Polizeirecht) andererseits. Zu regeln ist zunächst die Pflicht der Telekommunikationsunternehmen, bestimmte Daten für bestimmte Zwecke vorzuhalten und ggf herauszugeben; dies ist eine wirtschaftsrechtliche, in der EU zu Recht auf die Binnenmarktkompetenzen[27] und nicht die dritte Säule gestützte und in Deutschland zu Recht im TKG und nicht im Sicherheits-Fachrecht geregelte Materie. Zu regeln ist sodann, unter welchen Voraussetzungen die Sicherheitsbehörden auf diese Daten zugreifen dürfen; dies ist eine Frage, die sinnvollerweise nur durch das jeweilige Fachrecht, also durch die Polizeigesetze für die Gefahrenabwehr und durch die StPO für die Strafverfolgung, geregelt werden kann und daher völlig zu Recht gerade nicht Gegenstand der EG-Richtlinie oder des TKG ist. Das BVerfG hat in seinen einstweiligen Anordnungen[28] beide Ebenen dadurch miteinander vermengt, dass es die telekommunikationsrechtliche Herausgabepflicht auf bestimmte Fälle der fachrechtlichen Zulässigkeit des Datenabrufs beschränkt hat. Im Sinne einer pragmatischen vorläufigen Regelung mag dies angehen. Im Hauptsacheverfahren wird man sich hingegen darauf zu besinnen haben, dass die Modalitäten des Abrufs in Verfassungsbeschwerden gegen das Fachrecht zu rügen sind, mit der Verfassungsmäßigkeit der Vorratsdatenspeicherung nach dem TKG hingegen nichts zu tun haben.

Der zweite Fragenkreis geht an die Substanz der Vorratsdatenspeicherung als solcher. Wird dadurch, dass völlig verdachtslos von jedermann Daten gespeichert und vorgehalten werden müssen, nicht die endgültige Abkehr von dem vorhin auch von mir betonten rechtsstaatlichen Erfordernis vollzogen, dass staatliche Ermittlungsbefugnisse an adäquate Eingriffsschwellen und -anlässe geknüpft sein müssen? Die Antwort lautet: nein. Entscheidend ist dabei, dass die jedermann treffende Vorhaltung von Daten durch Private für sich gerade noch keinen staatlichen Ermittlungseingriff bedeutet, sondern nur eine – im Übrigen nicht verdeckt, sondern offen stattfindende – vorsorgliche Sicherung des Vorhandenseins und der Zugänglichkeit von Spuren, auf die erst sodann – in einem zweiten Schritt – im Wege des staatlichen Ermittlungseingriffs (der seinerseits einen adäquaten Verdachtsgrad voraussetzt) zugegriffen werden kann. Ob eine solche präventive Spurensicherung wirklich erforderlich ist, muss im Lichte des Verhältnismäßigkeitsprinzips nüchtern diskutiert werden.[29] Nicht jedoch kann der Vorratsdatenspeicherung vorgehalten werden, sie breche aus dem System von Eingriffsschwellen aus, wie sie für staatliche Ermittlungsmaßnahmen gelten.

5. FRAGEN DES VERHÄLTNISSES VON POLIZEI UND NACHRICHTENDIENSTEN

Der letzte Problemkomplex hat das Verhältnis von Polizeien und Nachrichtendiensten zum Gegenstand.[30] Zu verzeichnen ist hier ein Trend, der plakativ als Vernachrichtendienstlichung der Polizei (die immer mehr Vorfeldbefugnisse erhält) und Verpolizeilichung der Nachrichtendienste (die immer mehr in die Kriminalitätsbekämpfung einbezogen werden) be-

zeichnet wurde[31]; komplettiert wird dieser Trend durch einen zunehmenden informationellen Verbund von Nachrichtendiensten und Polizei, die zB ein gemeinsames Terrorismusabwehrzentrum sowie eine gemeinsame Antiterrordatei betreiben.[32] Dass jegliche neue Befugnis für Polizei und Nachrichtendienste, und vor allem auch Befugnisse der Datenweitergabe zwischen Polizei und Nachrichtendiensten, der verfassungsrechtlichen Rechtfertigung bedürfen und vor dem Verhältnismäßigkeitsprinzip Bestand haben müssen, dh insbesondere auch an adäquate Voraussetzungen zu binden sind, liegt auf der Hand. Doch jenseits der Mühe, hier angemessene Lösungen im Detail zu finden, wird die Zusammenarbeit von Polizei und Nachrichtendiensten häufig weitaus grundsätzlicher – unter Berufung auf eine Großformel – in ein schiefes Licht gerückt: die Großformel vom Trennungsgebot von Polizei und Nachrichtendiensten nämlich; nur hierauf soll hier eingegangen werden.

Der Status des Trennungsgebots im deutschen Recht, insbesondere die Frage, ob es Verfassungsrang hat, ist umstritten; zurück geht es auf eine Anordnung der Alliierten; es ist für die deutsche Sicherheitsarchitektur zweifellos prägend geworden.[33] Für die hier interessierende Frage rein informationeller (dh nicht aktioneller) Befugnisse und des bloßen Informationsaustausches zwischen Polizei und Nachrichtendiensten ist es hingegen – so die hier vertretene These – völlig unergiebig.

Für die Nachrichtendienste heißt Trennungsgebot – richtig betrachtet – zum einen das Gebot organisatorischer Trennung, das zweifelsohne beachtet ist, zum anderen das sog Verbot „polizeilicher Befugnisse“. Gemeint ist damit, dass die Nachrichtendienste (in scharfer Abkehr von dem, was in Diktaturen üblich ist) zwar uU viel wissen, niemals aber selbst zur Tat schreiten und die Konsequenzen aus ihrem Wissen ziehen dürfen, indem sie unter Einsatz von Zwangsbefugnissen unmittelbar zu Maßnahmen der Gefahrenabwehr oder Strafverfolgung schreiten; dies ist allein der Polizei vorbehalten. Das Trennungsgebot beschränkt die Nachrichtendienste somit auf den rein informationellen Bereich; zum Handeln sind andere berufen. Schon hieraus wird deutlich, dass in dem bloßen Umstand der Informationsweitergabe keine Verletzung des Trennungsgebots liegen kann, weil diese ja im rein informationellen Bereich verbleibt und gerade keine Zwangsbefugnisse in Anspruch nimmt. Noch weitergehend muss das Recht zur Informationsweitergabe an andere jedoch sogar als die eigentliche Funktion eines „Nachrichten“-Dienstes und notwendige Kehrseite des Trennungsgebots angesehen werden, denn wenn die Nachrichtendienste weder selbst handeln noch ihr Wissen an die zum Handeln Berufenen weitergeben dürften, dann müsste man fragen, wozu sie überhaupt nützlich sein sollen.[34]

Ein funktionstüchtiger Informationsfluss zwischen Nachrichtendiensten und Polizei ist somit nicht Verletzung, sondern folgerichtige Konsequenz des Trennungsgebotes.

Auch für die Polizeien folgt aus dem Trennungsgebot wenig. Zwar mag es sein, dass die auch zum Handeln berufenen Polizeien aus rechtsstaatlichen Gründen über restriktivere Vorfeldbefugnisse verfügen müssen als die Nachrichtendienste. Ein völliges Verbot von Vorfeldbefugnissen kann hieraus jedoch nicht folgen, denn oben wurde gezeigt, dass Gefahrenaufklärung im Gefahrenvorfeld zwar der grundrechtlichen Begrenzung bedarf, nichtsdestoweniger aber als notwendiges Korrelat einer an die Gefahrenschwelle gebunde-

nen Gefahrbeseitigung erscheint, dh von der polizeilichen Aufgabe nicht hinweggedacht werden kann.

Erneut wird deutlich, dass nicht Großformeln (wie das Trennungsgebot), sondern allein die mühevolle Kleinarbeit des Verhältnismäßigkeitsprinzips einen angemessenen Ausgleich von Freiheit und Sicherheit zu bewirken vermögen.

6. AUSBLICK

Zum Schluss muss der Blick Richtung Europäische Union (EU) ausgeweitet werden: Was für Deutschland gezeigt wurde, gilt noch mehr für den Europäischen „Raum der Freiheit, der Sicherheit und des Rechts". Im durch Binnengrenzen nicht mehr behinderten einheitlichen kriminalgeografischen Raum Europa gewinnt die grenzüberschreitende Informationsvernetzung immer mehr an Bedeutung; auch europäisches Polizeirecht ist in erster Linie Informationsrecht[35]; und es verwundert nicht, dass sich die EU vermehrt den Grundsatz der Datenverfügbarkeit auf die Fahnen schreibt.[36] Dass grenz- und rechtsordnungsüberschreitende Datenverfügbarkeit eher noch größere rechtsstaatliche Probleme verursacht, als dies im Binnenraum der Mitgliedstaaten der Fall ist, liegt bei alledem auf der Hand. Auch die europäische Rechtsordnung wird sich der mühevollen Kleinarbeit des Verhältnismäßigkeitsprinzips nicht entziehen können, und den europäischen Grundrechten steht die Bewährungsprobe, auf dem Felde der Datenverfügbarkeit einen angemessenen Ausgleich von Freiheit und Sicherheit zu finden, noch bevor.

[1] Geringfügig modifizierte und um Nachweise ergänzte schriftliche Fassung eines Vortrags, den der Verfasser am 11. Juni 2009 als deutschen Landesbericht zum Themenblock „Das Spannungsverhältnis zwischen Freiheitsrechten und Sicherheit" auf der Dreiländertagung 2009 der verwaltungswissenschaftlichen Gesellschaften Deutschlands, Österreichs und der Schweiz in Schaffhausen gehalten hat. Das am 2. März 2010 ergangene Urteil des BVerfG zur Vorratsdatenspeicherung (1 BvR 256/08 u.a.) konnte nur noch in den Anmerkungen berücksichtigt werden.

[2] Vgl zB das Streitgespräch zwischen dem früheren Verfassungsrichter Hassemer und Bundesinnenminister Schäuble zum Thema „Wie viele Sicherheitsgesetze überlebt der Rechtsstaat" in der Frankfurter Allgemeinen Zeitung vom 11. März 2009, 33.

[3] Isensee (1992); Möstl (2002) 37–41.

[4] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007, BGBl I, 3198.

[5] Volkszählungsurteil des BVerfG vom 15. Dezember 1983, BVerfGE 65, 1.

[6] Möstl (2007) 581 f. Vgl zB Art 30 bis 49 des Bayerischen Polizeiaufgabengesetzes; zum polizeilichen Informationsrecht siehe Petri (2007).

[7] Terrorismusabwehrgesetz vom 25.12.2008, BGBl I S 3198.

[8] Nehm (2004); Wolff (2009).

[9] §§ 113a, 113b TKG in der Fassung des in Anmerkung 4 zitierten Gesetzes.

[10] BVerfGE 109, 279; 113, 348; 115, 320; 120, 274.

[11] BVerfG vom 11.03.2008 und vom 28.10.2008 – 1 BvR 256/08. Inzwischen ist auch die Hauptsacheentscheidung ergangen (Urteil vom 2. März 2010).

[12] Süddeutsche Zeitung vom 23.04.2009, 6.

[13] Möstl (2007); Poscher (2008); Trute (2009).

[14] So – zurückgehend auf § 1 Abs 1 Satz 2 des Vorentwurfs zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder – viele Landespolizeigesetze (zB § 1 Abs 1 Satz 2 PolG NW).

[15] Vgl die Nachweise bei Möstl (2007) 582, Anmerkung 10.

[16] BVerfGE 113, 348.

[17] Ebd. 114, 320.

[18] *Ebd. 120, 274.*
[19] *Möstl (2007) 584–586.*
[20] *Ebd. 587 f.*
[21] *BVerfGE 113, 348.*
[22] *BVerfGE 120, 274, 328 f.*
[23] *BVerfGE 109, 279.*
[24] *Poscher (2009).*
[25] *BVerfGE 120, 274, 338 ff.*
[26] *Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG; ABl Nr L 105/54.*
[27] *Gundel (2009). EuGH, Urteil vom 10.02.2009 – C 301/06.*
[28] *Siehe Anmerkung 11. Angreifbar insoweit auch die Hauptsacheentscheidung vom 2. März 2010 (vgl. Leitsatz 3 und Abs.-Nr. 264 ff.).*
[29] *Gundel (2009). Auch die Hauptsacheentscheidung des BVerfG vom 2. März 2010 hält die Vorratsdatenspeicherung nicht für schlechthin mit den Grundrechten unvereinbar.*
[30] *Nehm (2004); Wolff (2009).*
[31] *Möstl (2002) 408 m.w.N.*
[32] *Antiterrordateigesetz vom 22.12.2006, BGBl I S 3409.*
[33] *Nehm (2004) 3289 ff.*
[34] *Möstl (2002) 412.*
[35] *Pitschas (1993).*
[36] *Böse (2007).*

Quellenangaben

Böse, Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union (2007).
Gundel, Vorratsdatenspeicherung und Binnenmarktkompetenz: Die ungebrochene Anziehungskraft des Art 95 EGV, Europarecht (2009) 536.
Isensee, Das Grundrecht als Abwehrrecht und staatliche Schutzpflicht, in Isensee/Kirchhof (Hrsg), Handbuch des Staatsrechts (1992) § 111.
Möstl, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung (2002).
Möstl, Die neue dogmatische Gestalt des Polizeirechts, Deutsches Verwaltungsblatt (2007) 581.
Nehm, Das nachrichtendienstrechtliche Trennungsgebot und die neue Sicherheitsarchitektur, Neue Juristische Wochenschrift 2004, 3289.
Petri, Informationsverarbeitung im Polizei- und Strafverfahrensrecht, in Lisken/Denninger (Hrsg), Handbuch des Polizeirechts (2007).
Pitschas, Europäisches Polizeirecht als Informationsrecht, Zeitschrift für Rechtspolitik 1993, 124.
Poscher, Eingriffsschwellen im Recht der inneren Sicherheit, Die Verwaltung 2008, 345.
Poscher, Menschenwürde und Kernbereichsschutz, Juristenzeitung 2009, 269.
Trute, Grenzen des präventionsorientierten Polizeirechts in der Rechtsprechung des Bundesverfassungsgerichts, Die Verwaltung 2009, 85.
Wolff, Die Grenzverschiebung von polizeilicher und nachrichtendienstlicher Sicherheitsgewährleistung, Die öffentliche Verwaltung 2009, 597.