Dr. Heiko Stamer, Experte für IT-Sicherheit und Kryptografie, Mitglied der Fachgruppe „Angewandte Kryptologie“ der Gesellschaft für Informatik e. V.

Stellungnahme zum

Achten Gesetz zur Änderung des Brandenburgischen Polizeigesetzes

Gesetzentwurf der Landesregierung, Drucksache 5/4163

29. November 2011*

Im Dezember 2006 wurden vom Brandenburger Landtag verschiedene neue Befugnisse für den Eingriff in die Telekommunikation und eine anlassbezogene automatische Kennzeichenfahndung beschlossen. Die Einführung dieser Regelungen zur Gefahrenabwehr wurde dabei in den Begründungszusammenhang von „Bedrohungen aufgrund der Organisierten Kriminalität und des internationalen Terrorismus“[1] gestellt.

Mittlerweile hat sich gezeigt, dass insbesondere die automatische Kennzeichenerfassung *exzessiv* und *zweckfremd* zur Strafverfolgung bei Kfz-Diebstählen genutzt wird. Die Unterbrechung oder Verhinderung von Telekommunikationsverbindungen stellt wegen der fehlenden Zielgerichtetheit der Maßnahme einen *massiven* Eingriff in die Grundrechte von unvermeidbar betroffenen Dritten dar.

Zusammenfassend lässt sich feststellen, dass wegen der Problematik der Aufweichung des Einsatzbereichs, der hohen Missbrauchsgefahr und der mangelhaften Benachrichtigungspflichten diese Befugnisse meines Erachtens nicht mehr Bestandteil des Brandenbur-

*Tippfehler korrigiert am 15. Januar 2012

[1] Viertes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes, Gesetzentwurf der Landesregierung, Drucksache 4/3508

gischen Polizeigesetzes sein sollten. Ein Auslaufen der Regelungen zum 31. Dezember 2011 wird deshalb *dringend empfohlen.*

Einleitung

Immer weiter ausufernde staatliche Eingriffs- und Datenerhebungsbefugnisse gefährden die *informationelle Selbstbestimmung* der Bürgerinnen und Bürger in zunehmenden Maße. Mit jeder zusätzlichen staatlichen Befugnis erhöht sich gerade auch im Zuge der informationstechnischen Umsetzung bzw. Speicherung von damit in Zusammenhang stehenden Daten die zugrunde liegende Missbrauchsgefahr erheblich. Das im Bereich der Ingenieurs- und Naturwissenschaften bekannte Gesetz von Murphy[2] lässt sich insofern wie folgt auf diese Situation übertragen:

Alles, was missbraucht werden kann, wird auch missbraucht.

Deshalb ist der Gesetzgeber heutzutage besonders gefordert, neue und bestehende Eingriffs- und Datenerhebungsbefugnisse äußerst sorgfältig zu evaluieren und hinsichtlich ihrer Einschränkung von Grundrechten der Betroffenen sachgerecht abzuwägen. Die fortschreitende Automatisierung von Verwaltungsprozessen sowie die kontinuierliche Erhebung, Speicherung und Verarbeitung immenser Datenmengen mittels IT-Systemen verlangt zugleich einen zeitgemäßen und effektiven Datenschutz in allen Bereichen staatlichen Handelns.

Leider sieht die alltägliche IT-Praxis sowohl bei öffentlichen als auch bei nichtöffentlichen Stellen durchweg besorgniserregend aus: veraltete Betriebssysteme mit teilweise hunderten von Sicherheitslücken, unzureichender Schutz vor Viren und Schadsoftware, fehlende Verschlüsselung sensibler Daten, mangelhafte Dokumentation und Kontrolle von erteilten Berechtigungen, unzureichende Lösch- und Aussonderungskonzepte usw. Die eigentlich dringend notwendige strenge und regelmäßige Kontrolle durch die Aufsichtsbehörden wird erfahrungsgemäß aufgrund der mangelnden personellen und finanziellen Ausstattung weitgehend vernachlässigt; eventuell im Raum stehende (strafrechtliche) Sanktionen bleiben oft folgenlos. Es ist deshalb nur wenig verwunderlich, dass in der Presse immer häufiger vom Missbrauch personenbezogener Daten oder der sicherheitstechnischen Kompromittierung von wichtigen IT-Diensten zu lesen ist. Dabei sind die bekannt gewordenen Fälle sprichwörtlich nur die Spitze des Eisbergs.

Viele Angriffe auf IT-Systeme erfolgen nämlich durch so genannte Innentäter, die weitreichende Kenntnisse von ihren Zielobjekten haben: Beispielsweise kann

[2] weitläufig anerkannte Übersetzung: „Alles, was schiefgehen kann, wird auch schiefgehen."

der Missbrauch polizeilicher Informationssysteme zu privaten Zwecken als hinreichend belegt angesehen werden,[3] wobei mit an Sicherheit grenzender Wahrscheinlichkeit zu vermuten ist, dass hier das Dunkelfeld noch erheblich größer ist. Im Zuge solcher Missbrauchshandlungen wird seitens der Täter mit einer besonders hohen kriminellen Energie vorgegangen und penibel darauf geachtet, keine (elektronischen) Spuren in Protokollen oder Daten zu hinterlassen. Hinzu kommt, dass neben dem Missbrauch zu privaten Zwecken auch ein „dienstlicher Missbrauch“ vorliegen kann, indem bestehende rechtliche Voraussetzungen vorsätzlich unbeachtet bleiben und technisch-organisatorische Sicherungsmechanismen umgangen werden.

Abschließend sei darauf hingewiesen, dass seit geraumer Zeit die Rechtsprechung des Bundesverfassungsgerichts verschiedene gesetzliche Regelungen im Bereich der so genannten „Inneren Sicherheit“ beanstandet oder sogar verworfen hat. Hierbei ist insbesondere nicht zu verkennen, dass in den Begründungen der jeweiligen Entscheidungen *nur Empfehlungen* für eine mögliche, verfassungsgemäße Neuregelung derselben ausgesprochen werden. Der Gesetzgeber ist also keinesfalls zwangsläufig verpflichtet, eine Regelung entlang dieser äußersten Grenze auch auszulegen. Er kann insbesondere eine weniger eingriffsintensive Variante wählen oder im Zweifel sogar auf die Normierung der entsprechenden Befugnis zu Gunsten der betroffenen Grundrechte verzichten. Es ist nicht so, dass der Staat aus unbestimmten Schutzpflichten heraus verpflichtet wäre, fragwürdige Sicherheitsmaßnahmen nun unbedingt einzuführen.

Bewertung des Gesetzentwurfs der Regierung

Durch Artikel 2 des Gesetzentwurfs werden einige der in 2006 eingeführten Eingriffsbefugnisse entfristet, die sonst am 31. Dezember 2011 auslaufen würden.

Datenerhebung durch Eingriffe in die Telekommunikation

Der zur Entfristung vorgesehene § 33b Abs. 3 erlaubt der Polizei unter gewissen Voraussetzungen den Einsatz von technischen Mitteln (d. h. IMSI-Catcher, GSM/UMTS/WiFi-Jammer, Remote Forensic Software etc.), um einerseits spezifische Kennungen (z. B. IMEI/IMSI, IP/MAC-Adressen) für eine Maßnahme nach § 33b Abs. 1 (Überwachung und Aufzeichnung der Telekommunikation zur Gefahrenabwehr) oder den Standort eines Mobilfunkendgerätes zu ermitteln. Andererseits sollen technische Mittel erlaubt sein, um im Gefahrenfall die Telekommunikationsverbindungen von Störern oder Notstands-

[3] siehe Tätigkeitsberichte des Bundes- und der Landensdatenschutzbeauftragten

pflichtigen zu unterbrechen oder gar zu verhindern. Im vierten Absatz ist diesbezüglich noch angegeben, dass auch Verbindungen von Dritten unterbrochen oder verhindert werden dürfen, wenn dies unvermeidbar ist und zum Zwecke der Maßnahme nicht außer Verhältnis steht.

Sowohl der Einsatz *beliebiger* technischer Mittel als auch die zulässige *ungezielte* Unterbrechung und/oder Verhinderung von Telekommunikation stößt dabei auf große Vorbehalte: In den letzten Monaten haben die Skandale um den Einsatz des „Staatstrojaners“ (Remote Forensic Software) gezeigt, wie schnell das Vertrauen der Bevölkerung in verantwortungsvolles staatliches Handeln durch technisch unausgereifte und rechtlich fragwürdige Maßnahmen erschüttert werden kann. Die Formulierung der Regelung lässt aber insbesondere auch diese Technologie für die Ermittlung spezifischer Kennungen oder die Unterbrechung von Telekommunikationsverbindungen zu, obgleich damit zusätzlich in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingegriffen wird. Die *unscharfen* Verhältnismäßigkeitserwägungen des vierten Absatzes laden hingegen geradezu dazu ein, Telekommunikation mittels Jammer-Technologie in Zukunft breitflächig zu unterbrechen. In den Vereinigten Staaten gibt es seit kurzem ähnliche Bestrebungen im ÖPNV.[4] Dabei kann eine derartig ungezielte Verhinderung der Telekommunikation zu erheblichen wirtschaftlichen Schäden oder im Fall von Notrufen sogar zu tödlichen Konsequenzen führen.

Der fünfte Absatz von § 33b sieht zwar einen Richtervor- bzw. -nachbehalt vor, jedoch ist dieser in der Praxis faktisch *wirkungslos*.[5] Es hat sich gezeigt, dass die Anordnungstexte der Staatsanwaltschaften bzw. Polizeibehörden von den zuständigen Amtsrichtern weitgehend ungeprüft übernommen werden.[6] Unzulässige Grundrechtseinschränkungen können dann erst in langwierigen Beschwerdeverfahren von höheren Instanzen für rechtswidrig erklärt werden. Der Gesetzentwurf stellt diesbezüglich auch keine speziellen Anforderungen an die Prüfung der Anordnung.

Die Erlaubnis zur Zweckentfremdung der erhobenen Daten (spezifische Kennungen, festgestellter Standort) im achten Absatz ist ebenfalls kritisch zu sehen. Im Hinblick auf die unverhältnismäßige und weitreichende Funkzellenauswertung in Sachsen scheinen die einschränkenden Voraussetzungen dieses

[4] San Francisco Bay Area Rapid Transit (BART), Cell Phone Interruption Policy, Draft, Oct. 2011

[5] „Viele Durchsuchungen sind verfassungswidrig“, Interview mit Rudolf Mellinghoff (Richter am Bundesverfassungsgericht a. D.), taz, 28.10.2011

[6] Otto Backes, Christoph Gusy: Wer kontrolliert die Telefonüberwachung? – Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung. Peter Lang Verlag, Frankfurt am Main 2003, ISBN 978-3-631-51279-1

Absatzes bewusst sehr grob gewählt zu sein.

Die unverzügliche Löschung der Daten (Abs. 9 Satz 1), wenn sich nach Auswertung herausstellt, dass die Voraussetzungen für die Erhebung nicht vorlagen, ist ambivalent zu sehen: Einerseits verlangt effektiver Datenschutz, dass rechtswidrig erhobene Daten umgehend zu löschen sind. Andererseits wird damit den Betroffenen jegliche Möglichkeit der Auskunft und des nachträglichen Rechtsschutzes (Art. 19 Abs. 4 GG) genommen. Hier müsste eigentlich das Grundprinzip ‚Sperren statt Löschen' verbunden mit einer umfassenden Benachrichtigungspflicht gelten.

Fallbeispiele

Die folgenden Fallbeispiele sind wörtlich den entsprechenden Berichten[7] des Ministers des Innern an den Ausschuss für Inneres des Landtags entnommen. Durch *Hervorhebung* der relevanten Stellen wurde versucht, kritikwürdige Handlungen bei der Anwendung der Befugnisse deutlich zu machen.

> Durch den polizeilichen Einsatz technischer Mittel, wie z. B. den IMSI-Catcher, wurde in einem Fall der Standort eines Mobilfunkendgerätes nach § 33b Abs. 3 Nr. 2 bestimmt. Diese Maßnahme fand im Zuständigkeitsbereich des Polizeipräsidiums Frankfurt (Oder) statt.
>
> Anlass der Maßnahme war eine telefonische Bedrohung, wobei von einer Ernsthaftigkeit ausgegangen wurde. Die betreffende Person war zugleich Täter. Dieser konnte *an seiner Wohnanschrift* geortet und vorläufig festgenommen werden, Die Maßnahme wurde auf die Ermächtigung nach § 33b Abs. 3 Nr. 2 i. V. m. §§ 33b Abs. 1 und 33a Abs. 1 Nr. 1 BbgPolG gestützt, also zur Abwehr einer dringenden Gefahr für Leib oder Leben einer Person getroffen. Die Anordnungskompetenz lag beim Behördenleiter, wobei die nach § 33b Abs. 5 BbgPolG erforderliche richterliche Anordnung im Nachhinein eingeholt wurde.

Hier hätte im Zuge der Verhältnismäßigkeitsprüfung zuerst die Wohnanschrift des Betroffenen aufgesucht werden können, da offenbar die Identität des Störers bereits ermittelt war. Die Bestimmung des Standorts war also *überflüssig*.

> Durch den polizeilichen Einsatz technischer Mittel, wie z. B. den IMSI-Catcher, wurde in einem Fall der Standort eines Mobilfunkendgerätes

[7] Ausschussprotokoll 5/9 der 9. Sitzung (AI) 16.09.2010, Ausschussprotokoll 5/19-2 der 19. Sitzung (AI) 15.06.2011

nach § 33b Absatz 3 Nr. 2 bestimmt. Diese Maßnahme fand im Zuständigkeitsbereich des Bereiches I (ehemaliges Polizeipräsidium Frankfurt (Oder)) statt.

Anlass der Maßnahme war die Vermisstenmeldung durch eine Mutter, die ihre minderjährige Tochter, welche wegen einer psychischen Störung und einem Hang zum Alkohol, als gefährdet eingestuft wurde, suchte. Die Jugendliche kehrte weder nach Hause zurück, noch war sie in der Schule anwesend. Sie litt unter dem Borderline-Syndrom und befand sich deshalb in psychologischer Behandlung. Die Vermisste hatte erhebliche private Probleme. Der Einsatz technischer Mittel erschien zur genauen Standortlokalisierung notwendig. Die Maßnahme wurde auf die Ermächtigung nach § 33b Absatz 3 Nr. 2 i. V. m. §§ 33b Absatz 1 und 33a Absatz 1 Nr. 1 BbgPolG gestützt, also zur Abwehr einer dringenden Gefahr für Leib oder Leben einer Person getroffen. Der Einsatz wurde jedoch durch die Einsatzleitung auf der Anfahrt abgebrochen, *da die Vermisste zwischenzeitlich zu Hause erschien.*

In diesem Fall wurde anscheinend vorschnell gehandelt. Außerdem wäre mit Zustimmung der Erziehungsberechtigten eine Anfrage beim Diensteanbieter auch ohne polizeiliche Eingriffsbefugnisse (vgl. neuer sechster Absatz von § 33b) möglich gewesen.

Anlassbezogene automatische Kennzeichenfahndung

Die automatische Fahndung nach auffälligen Kraftfahrzeugen erfolgt in Brandenburg sowohl durch stationäre als auch mobile Systeme[8], die die Kennzeichen der passierenden Fahrzeuge mittels Foto-/Videotechnik erfassen und auswerten. Im Unterschied zu der Erhebung eines einzelnen Kraftfahrzeugkennzeichens durch Polizeistreifen können hier Daten *massenhaft und praktisch unbegrenzt* erhoben werden.[9] Durch den zugelassenen Abgleich mit Fahndungsbeständen (§ 36a Abs. 2) werden die dabei erhobenen Daten auch verarbeitet und im Übereinstimmungsfall ggf. an weitere Stellen übermittelt. Durch die Bezugnahme auf § 36 Abs. 1a können das auch europäische Stellen (vgl. Schengener Durchführungsübereinkommen) sein.

Obwohl es sich hier eigentlich um eine strikt *anlassbezogene* Maßnahme handeln soll, zeigt allein die stetig gestiegene Anzahl und der jeweilige Charakter der „Anlässe“, dass die Befugnis durch die Brandenburger Polizei nicht unbedingt auch maßvoll eingesetzt wird. Die Kennzeichenfahndung wird seit 2009 beispielsweise sehr häufig im Rahmen der Vorbereitung von Fußballspielen des

[8] Derzeit sind angeblich fünf stationäre und drei mobile Geräte im Einsatz.

[9] Pieroth/Schlink/Kniesel, Polizei- und Ordnungsrecht, Verlag C.H.Beck, 6. Auflage, 2010

FC Energie Cottbus (z. B. allein in 2010: 19. März, 26. April, 24. September, 13. Dezember) angewendet.[10] Dies unterstreicht die eingangs erwähnte *schleichende Aufweichung* der bei Einführung der Befugnisse gebrauchten Begründungszusammenhänge sehr anschaulich. Auch die teilweise hohe Trefferanzahl (z. B. 483 Treffer am 26. April 2010 bei einer Dauer von nur 4:30 h) beim Abgleich mit Fahndungsdatenbanken verwundert zumindest aus technischer Sicht. Ein Einsatz der automatischen Kennzeichenfahndung zur Verhinderung unmittelbar bevorstehender Straftaten hat indessen im Berichtszeitraum 2010 nicht stattgefunden.

Die entsprechende Regelung in § 36a sieht eine *verdeckte* Erhebung („ohne Wissen der Person“) vor, was einen besonders schweren Eingriff in die Grundrechte der Betroffenen darstellt. Besonders kritisch ist daher festzuhalten, dass 2007 bei einer Maßnahme im Vorfeld einer Versammlung sogar nur „Kennzeichenfragmente“[11] abgeglichen worden sind, d. h. quasi eine automatische Rasterfahndung von Versammlungsteilnehmern stattfand. In diesem Zusammenhang ist es perfide, dass bei Einführung des Gesetzes in der damaligen Begründung wie folgt argumentiert wurde:

> In diesem Zusammenhang ist darauf hinzuweisen, dass sich die Datenerhebung durch anlassbezogene automatische Kennzeichenfahndung zwar im Vergleich zu bisher möglichen und zulässigen Verfahrensweisen auf eine Mehrzahl von Betroffenen beziehen kann, diesen aber nur geringe Eingriffe in ihre Grundrechte abverlangt und darüber hinaus eine Vielzahl von andernfalls erforderlichen Kontrollen überflüssig macht.

Bewertung zu § 33b Abs. 3 und § 36a

Zusammenfassend lässt sich feststellen, dass wegen der oben beschriebenen Problematik der Aufweichung des Einsatzbereichs, der hohen Missbrauchsgefahr der Anlagen bzw. Systeme für dienstfremde Zwecke und der grundsätzlich unterbleibenden Benachrichtigung von unvermeidbar betroffenen Dritten, diese Befugnisse meines Erachtens nicht mehr Bestandteil des Brandenburgischen Polizeigesetzes sein sollten. Die geringen Anwendungsfallzahlen insbesondere von § 33b Abs. 3 Nr. 1 deuten auf eine *überflüssige* Eingriffsbefugnis hin. Ein Auslaufen der Regelungen zum 31. Dezember 2011 wird deshalb empfohlen.

[10] Ausschussprotokoll 5/9 der 9. Sitzung (AI) 16.09.2010, Ausschussprotokoll 5/19-2 der 19. Sitzung (AI) 15.06.2011

[11] Antwort (LReg) Drucksache 4/6818 09.10.2008

Übrige Auswirkungen des Gesetzentwurfs

Die übrigen Auswirkungen des Gesetzentwurfs sind marginal. Einzig die klarstellende Regelung in Bezug auf die Verbunddateien des Bundeskriminalamtes verdient eine kritische Anmerkung: Die Verfahrensverzeichnisse (Errichtungsanordnungen) des Bundeskriminalamtes[12] sind regelmäßig als Verschlusssache eingestuft und deshalb den Betroffenen weitgehend unzugänglich.

Weitere Unzulänglichkeiten der bestehenden Regelungen

Bei der Durchsicht sind mir folgende weitere Unzulänglichkeiten aufgefallen.

§ 33b Abs. 2

Der dritte Satz dieses Absatzes ist derzeit wie folgt gefasst:

> Wird erkennbar, dass in den Kernbereich privater Lebensgestaltung oder in ein durch ein Berufsgeheimnis nach §§ 53, 53a der Strafprozessordnung geschütztes Vertrauensverhältnis eingegriffen wird, ist die Datenerhebung zu unterbrechen, es sei denn, sie richtet sich gegen den Berufsgeheimnisträger selbst.

Die Einschränkung der Unterbrechung der Maßnahme durch den Schlussteil der Formulierung („es sei denn, sie richtet sich gegen den Berufsgeheimnisträger selbst“) erfasst – vermutlich unbeabsichtigt[13] – auch das erste Ziel (d. h. den „Kernbereich privater Lebensgestaltung“). Wenn sich die Maßnahme also gegen einen Berufsgeheimnisträger nach §§ 53, 53a StPO richtet, führt somit ein Eingriff in den Kernbereich privater Lebensgestaltung gerade nicht zu einer Unterbrechung. Eine solche Ausgestaltung dürfte jedoch den vom Bundesverfassungsgericht aufgestellten Voraussetzungen nicht genügen.

§ 33b Abs. 3

Im dritten Absatz wird auf die Voraussetzungen des zweiten und ersten Absatzes zurückgegriffen, wobei der erste Absatz wiederum auf die Voraussetzungen des § 33a Abs. 1 verweist. Die Komplexität solcher Abhängigkeiten ist beträchtlich und wird in polizeilichen Praxis zu Fehlinterpretationen führen.

---

[12] vgl. § 10 BKADV

[13] „Der Schutz des Kernbereichs privater Lebensgestaltung in Satz 6 wird in ähnlicher Weise wie bei der Wohnraumüberwachung gewährleistet und zwingt bei dessen drohender Verletzung zur Unterbrechung der Maßnahme.“ Begründung aus Drucksache 4/3508

Fragenkatalog

Im Folgenden gehe ich auf die von den Ausschussmitgliedern formulierten Fragen ein. Fragen, zu denen ich aus fachlicher Sicht nicht Stellung nehmen kann, sind hierbei ausgelassen.

1. Inwieweit entstünde eine Regelungslücke, wenn die Regelungen zum Jahresende ausliefen?

Es entstünde meines Erachtens hierdurch gerade keine „Regelungslücke“. Die Brandenburgische Polizei dürfte dann zur Gefahrenabwehr nur einerseits nicht mehr *technische Mittel* (z. B. IMSI-Catcher, GSM/UMTS/WiFi-Jammer, Remote Forensic Software) einsetzen, um

1. spezifische Kennungen, insbesondere Geräte- und Kartennummer von Mobilfunkendgeräten *beliebiger Personen* zu ermitteln, wenn dies für die Durchführung einer Maßnahme zur Erhebung personenbezogener Daten durch den verdeckten Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation *unerlässlich* ist,

2. den Standort eines Mobilfunkendgerätes zu ermitteln oder

3. Telekommunikationsverbindungen zu unterbrechen oder zu verhindern,

und müsste andererseits ihre ausufernde Praxis der *automatischen* Kennzeichenfahndung zukünftig unterlassen. Von einer „Regelungslücke“ kann also überhaupt nicht gesprochen werden.

Vielmehr bleibt der Einsatz *nicht-technischer* Mittel (Auskunftsersuchen an Diensteanbieter, Beschlagnahme von Mobilfunkendgeräten etc.) zur Gefahrenabwehr unberührt. Für die Strafverfolgung kann auf die entsprechenden Regelungen nach §§ 100g, 100i StPO zurückgegriffen werden. Hinsichtlich der Fahndung nach auffälligen Kfz-Kennzeichen stehen zuverlässige manuelle Prozeduren (Inaugenscheinnahme des Kennzeichens durch Beamte) zur Verfügung.

2. Wie beurteilen Sie die für die Entfristung vorgesehenen Regelungen in Bezug auf Eingriffstiefe und Eingriffsanlass?

Zur Entfristung vorgesehen sind die Regelungen des § 33b Abs. 3 und § 36a, die sonst am 31. Dezember 2011 außer Kraft treten würden. Beide weisen eine *erhebliche* Eingriffstiefe auf, insbesondere auch für davon unvermeidbar betroffene Dritte. Die Tatbestandsvoraussetzungen sind stellenweise sehr *komplex* formuliert und über das gesamte Gesetz hinweg betrachtet *inkonsistent*.

3. Wie bewerten Sie den Nutzen der Maßnahmen im Verhältnis zur Eingriffsintensität in die Rechte der betroffenen Bürger?

Der Nutzen rechtfertigt meines Erachtens nicht die schwerwiegenden Grundrechtseingriffe der betroffenen Bürger.

6. Wie schätzen Sie den erwarteten Erkenntnisgewinn der Behörden im Verhältnis zum Datenerhebungsaufwand ein?

Der erwartete Erkenntnisgewinn der Behörden ist aus meiner Erfahrung durchweg als *marginal* anzusehen, was jedoch nicht an der Qualität oder Quantität der erhobenen Informationen an sich liegt. Vielmehr sind die zuständigen Behörden bzw. Beamten mit der Vielzahl an erfassten Daten einfach technisch überfordert (vgl. beispielsweise die Zeitdauer und das Ergebnis bei der Forensik von Computerfestplatten aus Hausdurchsuchungen).

8. Wie bewerten Sie die Missbrauchsgefahr?

Ich sehe in den betreffenden polizeilichen Eingriffs- bzw. Erhebungsbefugnissen eine *erhebliche* Missbrauchsgefahr, die der vorliegende Gesetzentwurf auch nicht durch flankierende rechtliche oder technische Maßnahmen ausreichend begegnet.

Speziell hingewiesen sei hier auf die Unzulänglichkeit von Standard-Löschverfahren (mehrfaches Überschreiben) für moderne nicht-magnetische Speichermedien, die in vielen mobilen Geräten eingesetzt werden.

9. Die Einführung der Maßnahmen wurde 2006 mit der Bekämpfung des internationalen Terrorismus und der Bekämpfung der organisierten Kriminalität begründet – inwieweit dürfen die Maßnahmen auch für andere Zwecke verwendet werden?

Zumindest aus dem Blickwinkel eines *glaubwürdigen Verwaltungshandelns* dürften die entsprechenden Maßnahmen nur für die in der damaligen Begründung vorgesehenen Zwecke verwendet werden. Die Aufweichung der Anwendungsbereiche zerstört das Vertrauen in verlässliche Politik nachhaltig.

11. Wie bewerten Sie die Tatsache, dass die automatische Kennzeichenfahndung mittlerweile fast täglich eingesetzt wird? Wie bewerten Sie die Tatsache, dass sie zu ca. 94 % bei Kfz-Diebstählen (also im Rahmen der Strafverfolgung) eingesetzt wird? Wie bewerten Sie die Trefferquote von 2,62 %?

Meine Bewertung hinsichtlich des damaligen (Stichwort: Kennzeichenfragmente) und aktuellen Missbrauchs der automatischen Kennzeichenfahndung hatte ich weiter oben bereits deutlich gemacht. Der Einsatz der Maßnahme zur Ahndung von leichter bis mittlerer Kriminalität, also weit überwiegend primär zur Strafverfolgung, zeigt die zunehmende Erosion des Stellenwerts von Grundrechten im Rahmen staatlichen Handelns.

Als Negativbeispiel der automatischen Kennzeichenfahndung kann deren Einsatz in Bayern betrachtet werden: Dort ist ein Großteil der vorhandenen Anlagen stationär und im Dauerbetrieb an Bundesautobahnen eingesetzt. Die anlassunabhängige Fahndung nach gestohlenen Fahrzeugen ist dort zu einer flächendeckenden Standardmaßnahme geworden, obwohl sie bei Einführung ebenfalls nur für Fälle schwerster Kriminalität vorgesehen war.