Gutachterliche Stellungnahme

zu dem Gesetzentwurf der Landesregierung

Gesetz zur Änderung des Gesetzes zum Schutz personenbezogener Daten
(Datenschutzgesetz Nordrhein-Westfalen - DSG NRW)

- Landtags-Drucksache 16/6634 -

von Dr. iur. Ulf Buermeyer, LL.M. (Columbia)
Richter am Landgericht Berlin

ulf@buermeyer.de

Berlin, im Februar 2015

I. Vorschlag der Landesregierung

§ 29a DSG NRW lautet bisher:

> **§ 29a Mobile personenbezogene Datenverarbeitungssysteme**
> (1) [1]Informationstechnische Systeme zum Einsatz in automatisierten Verfahren, die an die Betroffenen ausgegeben werden und die über eine von der ausgebenden Stelle oder Dritten bereitgestellte Schnittstelle Daten automatisiert austauschen können (mobile Datenverarbeitungssysteme, z. B. Chipkarten), dürfen nur mit Einwilligung der betroffenen Person nach ihrer vorherigen umfassenden Aufklärung eingesetzt werden.
>
> (2) [1]Für die Betroffenen muss jederzeit erkennbar sein,
>
> 1. ob und durch wen Datenverarbeitungsvorgänge auf dem mobilen Datenverarbeitungssystem oder durch dieses veranlasst stattfinden,
>
> 2. welche personenbezogenen Daten der betroffenen Person verarbeitet werden und
>
> 3. welcher Verarbeitungsvorgang im Einzelnen abläuft oder angestoßen wird.
>
> [2]Den Betroffenen müssen die Informationen nach Nummer 2 und 3 auf ihren Wunsch auch schriftlich in Papierform mitgeteilt werden.
>
> (3) [1]Die Betroffenen sind bei der Ausgabe des mobilen Datenverarbeitungssystems über die ihnen nach § 5 zustehenden Rechte aufzuklären. [2]Sofern zur Wahrnehmung der Informationsrechte besondere Geräte oder Einrichtungen erforderlich sind, hat die ausgebende Stelle dafür Sorge zu tragen, dass diese in angemessenem Umfang zur Verfügung stehen.

Diesem Wortlaut soll ein neuer Absatz 4 angefügt werden:

> "(4) [1]Abweichend von Absatz 1 dürfen Leitstellen und Befehlsstellen der in Satz 4 genannten Einrichtungen und Organisationen zur Bestimmung des geografischen Standorts personenbezogene Daten von Einsatzkräften mittels elektronischer

Einrichtungen durch eine Funktion des Digitalfunks für Behörden und Organisationen mit Sicherheitsaufgaben (BOS-Digitalfunk) oder durch andere technische Mittel ohne Einwilligung der Betroffenen verarbeiten, soweit dies aus dienstlichen Gründen zur Sicherheit oder zur Koordinierung der Einsatzkräfte erforderlich ist. [2]Standortdaten dürfen ausschließlich zu den in Satz 1 festgelegten Zwecken verarbeitet werden. [3]Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks der Speicherung nicht mehr erforderlich sind. [4]Satz 1 bis 3 gelten für Einsatzkräfte der Berechtigten des § 4 Absatz 1 Nummern 1.1, 1.5, 1.6, 1.7 und 1.9 der BOS-Funkrichtlinie in der Fassung der Bekanntmachung vom 7. September 2009 (GMBl. 2009, S. 803), soweit es sich hierbei um kommunale Behörden oder um Landesbehörden handelt.

II. Verfassungsrechtlicher Hintergrund

Aus verfassungsrechtlicher Sicht bedarf die Verarbeitung personenbezogener Daten – und damit ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG) – der Rechtfertigung. Diese ist grundsätzlich sowohl durch eine wirksame, insbesondere tatsächlich autonom getroffene Einwilligung (vgl. § 4a Abs. 1 BDSG) als auch durch eine gesetzliche Ermächtigung zur Datenverarbeitung möglich.

Gesetzliche Eingriffe in die informationelle Selbstbestimmung müssen ihrerseits verhältnismäßig sein. Wesentliches Kriterium hierfür ist die Schwere des Eingriffs in die informationelle Selbstbestimmung: Je schwerer der Eingriff, umso strikter prüft das Bundesverfassungsgericht seine Verhältnismäßigkeit. In der Rechtsprechung haben sich dabei eine Reihe von Kriterien der Eingriffsschwere herausgebildet:

Von maßgebender Bedeutung für das Gewicht des Grundrechtseingriffs ist zunächst die ***Intensität der Beeinträchtigung***. Hierfür ist in den Blick zu nehmen, *welche Daten* erhoben werden und welche *Persönlichkeitsrelevanz* sie aufweisen,[1] also welchen Informationsgehalt und welche Aussagekraft sie haben.[2] Dabei ist auch die Persönlichkeitsrelevanz der Daten in Rechnung zu stellen, die erst durch eine weitergehende Verarbeitung und Verknüpfung der erfassten Daten gewonnen werden sollen.[3] Beispiele für besonders intensive Eingriffe sind etwa solche, mit denen *höchstpersönliche Informationen* erfasst werden oder *Bewegungs- oder Persönlichkeitsprofile* erstellt werden können,[4] etwa zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen.[5]

Weiter ist von Bedeutung für die Intensität des Eingriffs von Bedeutung, ob die Daten sogleich personenbezogen verarbeitet werden oder ob die Betroffenen zunächst ***anonym*** bleiben.[6]

Verschärft wird ein Eingriff in die informationelle Selbstbestimmung weiter, wenn und solange Eingriffe gegenüber den Betroffenen ***heimlich*** vorgenommen werden,[7] da dies die

---

1 BVerfGE 120, 378, 402; 125, 260, 318.

2 BVerfGE 125, 260, 319 (zu Art. 10 Abs. 1 GG); BVerfGE 130, 151, 188; laut BVerfGE 130, 151, 197 ist die begrenzte Aussagekraft bestimmter Daten von *„zentraler Bedeutung“* für die Abwägung.

3 BVerfGE 120, 378, 402.

4 BVerfGE 130, 151, 190; BVerfGE 126, 260, 319 stellt zu Art. 10 Abs. 1 GG auf *„tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten“* sowie *„bis in die Intimsphäre reichende inhaltliche Rückschlüsse“* ab.

5 BVerfGE 125, 260, 319 (zu Art. 10 Abs. 1 GG).

6 Zu Art. 10 Abs. 1 GG siehe BVerfGE 100, 313, 376; 109, 279, 353; 113, 348, 382; vgl. auch BVerfGE 67, 157, 178 f. zu (wenigstens regelmäßig) anonymen Telekommunikationsüberwachungsmaßnahmen nach dem G 10.

Wahrnehmung effektiven – namentlich rechtzeitigen – Rechtsschutzes vereitelt. Besonders gravierend sind Eingriffe außerdem, wenn sie in einer ***Situation vermeintlicher Vertraulichkeit*** vorgenommen werden.[8]

Das Gewicht eines Eingriffs durch eine gesetzliche Ermächtigung erhöht sich außerdem, wenn in einer ***Vielzahl von Fällen*** Daten erhoben werden und / oder eine ***Vielzahl von Personen*** betroffen ist[9] (sog. „Streubreite"),[10] so bei der automatischen Kfz-Kennzeichenerfassung,[11] während sich das Gewicht einer (auch häufigen) Maßnahme relativieren soll, wenn die Wahrscheinlichkeit des einzelnen, betroffen zu werden, eher gering ist.[12]

Eine Maßnahme der Datenerhebung ist umso gravierender, je vielfältiger die tatsächlichen und rechtlichen Möglichkeiten sind, die gewonnenen Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken zu verwenden. Dabei erhöht die ***Breite der Verwendungsmöglichkeiten*** die Eingriffstiefe schon bei der Erhebung, auch wenn die weiteren Verwendungen jeweils für sich eigene Eingriffe in den Schutzbereich darstellen.[13]

Maßgeblich ist auch, welche – über die Datenverarbeitung hinausgehenden – ***konkreten Nachteile*** den Betroffenen entweder tatsächlich drohen oder von ihnen nicht ohne Grund befürchtet werden;[14] ein Beispiel hierfür wäre etwa das Risiko, weiteren Ermittlungen ausgesetzt zu werden.[15] Unter dem Aspekt der Nachteile sind dabei nicht nur legale Nutzungen in Rechnung zu stellen, sondern auch die ***Missbrauchsmöglichkeiten***, die die Datenverarbeitung ermöglicht.[16]

---

7 BVerfGE 120, 378, 402 f.; vgl. zu Art. 10 Abs. 1 GG BVerfGE 113, 348, 383 f.; 125, 260, 320.

8 Vgl. zu Art. 10 Abs. 1 GG BVerfGE 113, 348, 383; 125, 260, 320.

9 BVerfGE 120, 378, 401; vgl. zu Art. 10 Abs. 1 GG BVerfGE 100, 313, 367; 113, 348, 382 sowie zu Art. 13 Abs. 1 GG BVerfGE 109, 279, 353.

10 BVerfGE 113, 348, 383; 125, 260, 318 (zu Art. 10 Abs. 1 GG) und BVerfGE 130, 151, 188.

11 BVerfGE 120, 378, 401.

12 So noch BVerfGE 67, 157, 178 f. zu Art. 10 Abs. 1 GG für die strategische Telekommunikationsüberwachung nach dem G 10.

13 So zunächst BVerfGE 113, 348, 384 f. zu Art. 10 Abs. 1 GG, vgl. auch BVerfGE 125, 260, 319 f. Tendenziell anders jüngst BVerfGE 130, 151, 190 f.: Folgeeingriffe in den Schutzbereich des Art. 10 Abs. 1 GG, die sich an die Abfrage von Bestandsdaten potentiell anschließen, sollen das Gewicht des letztgenannten Eingriffs nicht erhöhen, weil sie „nur nach Maßgabe eigener Rechtsgrundlagen zulässig" seien (zweifelhaft).

14 Vgl. zu Art. 10 Abs. 1 GG BVerfGE 100, 313, 376; 113, 348, 382 sowie zu Art. 13 Abs. 1 GG BVerfGE 109, 279, 353.

15 BVerfGE 125, 260, 320 (zu Art. 10 Abs. 1 GG).

16 BVerfGE 125, 260, 320 (zu Art. 10 Abs. 1 GG).

Eine Maßnahme ist umso gravierender, je weniger die Betroffenen hierzu ***durch ihr Verhalten Anlass*** gegeben haben.[17] Informationserhebungen gegenüber Personen, die den Eingriff durch ihr Verhalten nicht veranlasst haben, sind grundsätzlich von höherer Eingriffsintensität als anlassbezogene,[18] sodass beispielsweise Maßnahmen gegenüber unbeteiligten Dritten erheblich schwerer wiegen als gegenüber Beschuldigten einer Straftat.[19] Besonders gravierend sind Maßnahmen gegenüber Personen, die keinen Anlass für die Datenerhebung gegeben haben, wenn sie in großer Zahl ausgeführt werden, sodass ein ***Gefühl des Überwachtwerdens*** entsteht, die ***Unbefangenheit des Verhaltens beeinträchtigt*** wird und ***Einschüchterungseffekte*** eintreten können.[20]

Schließlich ist in den Blick zu nehmen, wie die gesetzlichen ***Eingriffsschwellen*** ausgestaltet sind, deren Überschreiten eine Datenverarbeitung legitimieren soll.[21]

Im folgenden wird der Gesetzentwurf im Lichte dieser verfassungsrechtlichen Anforderungen betrachtet.

17 BVerfGE 120, 378, 402; vgl. BVerfGE 100, 313, 380; 113, 348, 383; 125, 260, 318 zu Art. 10 Abs. 1 GG sowie zu Art. 13 Abs. 1 GG BVerfGE 109, 279, 353.

18 BVerfGE 120, 378, 402.

19 So für Art. 10 Abs. 1 GG BVerfGE 113, 348, 383 sowie zu Art. 13 Abs. 1 GG BVerfGE 109, 279, 353 f.

20 BVerfGE 120, 378, 402; vgl. zu Art. 10 Abs. 1 GG BVerfGE 126, 260, 320.

21 Vgl. zu Art. 10 Abs. 1 GG BVerfGE 100, 313, 376; 113, 348, 382.

III. Fragenkatalog

Dem Verfasser wurden zur Vorbereitung auf das Sachverständigengespräch die folgenden „Fragen zum Gesetzentwurf zur Änderung des Gesetzes zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen – DSG NRW)“ übermittelt. An dieser Gliederung orientiert sich auch die schriftliche Ausarbeitung.

1. Ist zum Zweck der Bestimmung des geografischen Standorts eine Änderung im Datenschutzgesetz NRW vonnöten oder könnte die Regelung auch an anderer Stelle erfolgen?

Bei der vorgeschlagenen Regelung handelt es sich um eine gesetzliche Ermächtigung zur Datenverarbeitung. Der Standort der Ermächtigung – also in welchem Landesgesetz eine solche Regelung getroffen wird – ist dabei aus verfassungsrechtlicher Perspektive grundsätzlich irrelevant, sofern kein so abwegiger Standort gewählt wird, dass die Geltung oder Bedeutung der Norm insgesamt unklar wird (Grundsatz der Normenklarheit). Die Regelung könnte demgemäß auch an anderer Stelle getroffen werden, etwa im Fachrecht der Polizei, der Feuerwehr und des Rettungsdienstes. Andererseits spricht die Tatsache, dass es sich der Sache nach in der Tat um eine Ausnahme von der Regelung des § 29a Abs. 1 DSG NRW handelt, unter dem Aspekt der Normenklarheit durchaus für den seitens der Landesregierung vorgeschlagenen Standort.

2. Der Gesetzesentwurf erlaubt neben der Ortung mittels Digitalfunk auch die Ortung mithilfe „anderer technischen Mittel“. Welche technischen Mittel könnten gemäß dem Gesetzesentwurf gegenwärtig oder in Zukunft zur Ortung verwendet werden und ist es sinnvoll die Bestimmung zur Ortung von Einsatzkräften der aufgeführten Behörden dahingehend zu öffnen? Betrifft das auch die Einsatzmeldungen und Rückmeldungen über SDS?

Die Regelung ist technisch entwicklungsoffen formuliert, was guter gesetzgeberischer Praxis entspricht, um allzu baldigen Novellierungsbedarf zu vermeiden. Aus verfassungsrechtlicher Sicht ist die technische Umsetzung einer Erhebung von Standortdaten im einzelnen als solche nicht relevant (vgl. den Katalog der maßgeblichen Faktoren oben unter II.). Wesentlich sind

vielmehr andere Faktoren, die unten noch im einzelnen behandelt werden, namentlich die Transparenz der Datenerhebung (heimliche ./. offene Erhebung) sowie die Frage, ob Standortdaten personenbezogen erhoben werden oder nicht. So wäre beispielsweise die Erhebung des Standorts eines Fahrzeugs regelmäßig weniger eingriffsintensiv als die Erhebung des Standorts einer Person, da sich von dem Fahrzeug jedenfalls nicht unmittelbar auf die Identitäten der eingesetzten Personen schließen lässt. Demnach würde es sich bei der Erhebung von Standortdaten von Fahrzeugen der Sache nach um eine Pseudonymisierung handeln, die unter dem Gesichtspunkt der Datensparsamkeit einer personenbezogenen Erhebung vorzuziehen ist.

3. Die Rettungsdienste sind unabhängig und sind dem Schutz personenbezogener Daten besonders verpflichtet, etwa auch von Menschen in der aufenthaltsrechtlichen Illegalität. Ist der Zugriff von Polizei und Verfassungsschutz auf Positionsdaten der unabhängigen Rettungsdienste rechtlich zulässig und wie ist die Rolle der Helfer zu bewerten, wenn diese durch ihr Funkgerät den Aufenthaltsort oder die Wohnungsadressen der Menschen an Sicherheitsbehörden preisgeben?

Eine solche Preisgabe wäre in der Tat (menschen-)rechtlich fragwürdig. Indes sieht der Gesetzentwurf mit seiner Zweckbindungsklausel hier eine sinnvolle Sicherung vor. Im Entwurfstext ist vorgesehen, dass Standortdaten ausschließlich verarbeitet werden dürfen,

> *„soweit dies aus dienstlichen Gründen* ***zur Sicherheit oder zur Koordinierung der Einsatzkräfte*** *erforderlich ist.“* (meine Hervorhebung)

Die Verwendung von Standortdaten zur strafrechtlichen oder aufenthaltsrechtlichen Verfolgung von Menschen, die die Hilfe des Rettungsdienstes in Anspruch nehmen, wäre nach dieser Formulierung eindeutig rechtswidrig. Denn eine solche Datenverarbeitung würde weder der Sicherheit der Einsatzkräfte noch deren Koordinierung dienen. Sofern die Behörden diese Begrenzung auch einhalten und die Daten insbesondere nicht weitergeben dürften die Interessen der Patientinnen und Patienten also gewahrt bleiben.

4. Welche milderen Alternativen könnte es zur vorgeschlagenen Regelung geben?

Der Gesetzestext lässt bisher nicht eindeutig erkennen, dass die Regelung tatsächlich strikt am Maßstab der Verhältnismäßigkeit ausgerichtet wäre. Dieser Maßstab erfordert, dass ein Grundrechtseingriff durch Gesetz geeignet, erforderlich und auch angemessen sein muss, um ein legitimes Ziel zu fördern. An der Legitimität der im Entwurf genannten Ziele – Sicherheit der Einsatzkräfte und deren Koordinierung – bestehen zwar keine Zweifel. Auch die Geeignetheit der Erhebung von Standortdaten zur Steuerung von Einsätzen und in Ausnahmefällen auch zu deren Sicherheit erscheint noch plausibel. Jedenfalls aus der bisherigen Gesetzesbegründung ergibt sich jedoch nicht, dass die Maßnahme auch stets erforderlich wäre, insbesondere keine verfassungsrechtlich milderen Eingriffe in die informationelle Selbstbestimmung der Einsatzkräfte möglich wären. Beispielsweise liegen die folgenden Überlegungen nahe, wie die Eingriffstiefe verringert werden könnte:

a) Zeitliche Grenzen der Positions-Überwachung

Nach dem bisherigen Gesetzeswortlaut ist unklar, wie über die Frage der Erhebung der Standortdaten entschieden werden soll. Entscheiden Leitstellenmitarbeiter spontan, dass sie aktuell Standortdaten benötigen, und aktivieren dann die Übertragung? Oder wird die Norm letztlich so angewendet werden, dass die Übermittlung gar *dauerhaft* aktiv ist? Der Wortlaut des Abs. 4 des Entwurfs schließt die letztere Interpretation zumindest nicht aus. Er sollte daher insoweit klargestellt werden, dass die Positionsüberwachung nur ausnahmsweise aktiviert werden kann, wenn aus besonderen Gründen – etwa wegen eines Großschadensereignisses – die Steuerung der Einsatzkräfte dies tatsächlich erfordert. Im „Normalbetrieb" funktioniert die Steuerung der BOS hingegen seit Jahrzehnten auch ohne Positions-Monitoring, sodass eine dauerhafte Überwachung der Standorte von Einsatzkräften gravierenden Zweifeln hinsichtlich ihrer Erforderlichkeit unterläge. Selbst die Begründung des Gesetzentwurfs verhält sich mit keinem Wort zur Frage der Erforderlichkeit, sondern spricht lediglich von einer *„hilfreiche[n] Technik"*[22]. Nützlichkeit alleine begründet indes keine verfassungsrechtliche Erforderlichkeit. Der Gesetzentwurf sollte daher klarstellen, dass die Standortdaten nicht im Regelbetrieb erhoben werden dürfen, sondern nur in besonders begründeten Ausnahmefällen.

b) Heimliche Erhebung von Positionsdaten

Ob die Standortübermittlung gerade aktiv ist oder nicht muss den Einsatzkräften nach dem Gesetzeswortlaut nicht ausdrücklich zur Kenntnis gegeben werden. § 29a Abs. 2 DSG NRW ließe

22 Ds 16/6634, Seite 1.

sich zwar so interpretieren (*„muss jederzeit erkennbar sein, 1. ob und durch wen Datenverarbeitungsvorgänge ... stattfinden“*). Allerdings dürften auf den betroffenen Systemen auch andere Datenverarbeitungsvorgänge stattfinden, sodass nach dem derzeitigen Entwurf jedenfalls nicht eindeutig gerade über die Tatsache der aktiven Standorterhebung informiert werden muss. Aus verfassungsrechtlicher Sicht handelt es sich damit um eine heimliche Datenerhebung, die einen wesentlich gravierenderen Eingriff darstellt als eine offene Erhebung. Insofern wäre zumindest zu fordern, dass konkret geregelt wird, dass gerade über die aktive Positions-Überwachung informiert wird. Praktisch könnte etwa eine Warnleuchte im Einsatzfahrzeug (oder, soweit es um persönliche Geräte von Personen geht, am jeweiligen Gerät) darauf hinweisen, dass die Leitstelle die Positions-Überwachung aktuell aktiviert hat. Es ist kein Grund erkennbar, warum die Überwachung des Standorts vor den betroffenen Einsatzkräften geheim gehalten werden müsste.

c) Zwangsweise Positionserhebung durch die Leitstellen

Der Gesetzentwurf setzt sich nicht mit der Frage auseinander, warum die betroffenen Einsatzkräfte nicht selbst Positionsmeldungen absetzen können. Im Bereich des analogen BOS-Funks wird dies seit Jahrzehnten so praktiziert, wenngleich üblicherweise nicht durch Angabe von Geokoordinaten, sondern von einsatzbezogenen Schlüsselbegriffen („am Ort“, „Einfahrt“ o.ä.). Aus datenschutzrechtlicher Perspektive wären freiwillige Positionsmeldungen offensichtlich weit weniger eingriffsintensiv, weil es sich wenigstens regelmäßig um freiwillige Datenübermittlungen handeln würde, sodass die betroffenen Einsatzkräfte in die Verarbeitung der Positionsdaten eingewilligt hätten. Insofern heißt es im Gesetzentwurf lediglich, dass *„eine Einholung der Einwilligung der Betroffenen nicht mit dienstlichen Gegebenheiten in Einklang zu bringen“* sei. Dies erschließt sich angesichts des Vorstehenden und der jahrzehntelangen Praxis der (analogen) Statusmeldungen nicht, insbesondere wenn man die Verwendungszwecke der Positionsdaten zugrundelegt, die im Gesetzentwurf genannt sind: Geht es tatsächlich darum, *„den betroffenen Einsatzkräften Hilfe und Unterstützung zukommen zu lassen“*[23], dann läge nichts näher, als diese selbst mitteilen zu lassen, wo sie sich befinden, denn ohne einen Hilferuf wird für die Leitstelle ohnehin kaum Anlass bestehen, *„Hilfe und Unterstützung“* zu schicken. Und soweit es um die Steuerung der Kräfte geht, wird jedenfalls im Regelfall nichts dagegen sprechen, dass die Leitstelle die Kräfte schlicht nach ihrem Standort fragt und die betroffenen Kräfte dann freiwillig ihren Standort übermitteln. Allein bei Großschadensereignissen wird dies angesichts der dann üblichen Überlastung der Funkkanäle regelmäßig anders zu beurteilen sein.

---

23 Ds. 16/6634, Seite 1.

Im Ergebnis dürfte in aller Regel eine freiwillige Übertragung der Standortdaten für die im Gesetzentwurf genannten Verwendungszwecke hinreichen, während die zwangsweise Erhebung durch die Leitstelle auf Ausnahmesituationen beschränkt bleiben sollte. Die gesetzliche Regelung sollte dieses Regel-Ausnahme-Verhältnis wiederspiegeln.

d) Problematik der Kreuzerhebungen

Der Gesetzeswortlaut lässt außerdem nach seinem derzeitigen Wortlaut „Kreuzerhebungen" zu, sodass etwa auch die Polizei den Standort von Rettungsdienst-Fahrzeugen erheben dürfte (jenseits der Frage, ob die aktuell eingesetzte oder geplante Technik dies auch unterstützt). Insofern ist unklar, ob dies tatsächlich gewollt ist; die Erforderlichkeit einer solchen Kreuzerhebung erschließt sich jedenfalls nicht ohne weiteres. Insofern sollte der Gesetzestext klargestellt werden, um eindeutig zu regeln, ob Kreuzerhebungen zulässig sein sollen. Falls nein sollte statt *„dürfen Leitstellen und Befehlsstellen ... personenbezogene Daten von Einsatzkräften ... verarbeiten"*[24] beispielsweise formuliert werden *„dürfen Leitstellen und Befehlsstellen ... personenbezogene Daten* ***der von ihnen gesteuerten*** *Einsatzkräfte ... verarbeiten"*.

Die Frage der Kreuzerhebungen erlangt besondere Brisanz angesichts des Verweises auf § 4 Absatz 1 Nummer 1.9 der BOS-Funkrichtlinie in Abs. 4 Satz 4 des Entwurfs: Demnach soll auch der Verfassungsschutz des Landes Nordrhein-Westfalen Standortdaten verarbeiten dürfen. Insoweit ist schon im Ansatz nicht zu erkennen, welchen (legitimen) Bedarf Geheimdienste an Standortdaten von anderen BOS-Kräften haben könnten; auch die Begründung des Gesetzentwurfs verhält sich nur zur Überwachung der Position eigener VS-Kräften bei Observationen. Verfassungsschutzbehörden verfügen grundsätzlich gerade nicht über eigene exekutive Kompetenzen, sondern geben im Bedarfsfalle Informationen über Gefahrenlagen an Polizeibehörden weiter, die dann in eigener Zuständigkeit die notwendigen Maßnahmen der Gefahrenabwehr einleiten. Demnach dürfte es hinreichen, wenn lediglich Polizeibehörden die Standortdaten ihrer Einsatzkräfte verarbeiten.

Dies gilt insbesondere im Hinblick auf die generell zweifelhafte Effektivität der Kontrolle der Arbeit der Verfassungsschutzbehörden: Datenmissbrauch etwa der Standorte von Rettungsdienstfahrzeugen durch unzulässige Zweckänderungen entgegen der Verwendungszweckregelung im Entwurfstext (siehe oben bei Frage 3) dürfte im Bereich der Geheimdienste wesentlich schwerer – wenn überhaupt – zu verhindern sein als im Bereich der Polizeibehörden. Die Befugnis des Verfassungsschutzes sollte daher ersatzlos entfallen, indem

---

[24] Ds. 16/6634, Seite 6.

die Nummer 1.9 aus der Verweisung in Abs. 4 Satz 4 des Entwurfs gestrichen wird, sofern nicht klargestellt wird, dass Kreuzerhebungen insgesamt unzulässig sind (vgl. den obigen Formulierungsvorschlag).

e) Personenbezogene Erhebung versus Pseudonymisierung / Anonymisierung

Schließlich wäre zu prüfen, ob die Standortdaten tatsächlich (wie im Gesetzentwurf ausdrücklich geregelt) „personenbezogen" erhoben werden müssen. Zu prüfen wäre hier, ob auch eine Erhebung nur personenbeziehbarer Daten in Betracht kommt, also von Pseudonymen wie etwa Dienstnummern, oder ob mit vollständig anonymisierten Daten gearbeitet werden kann. Dies würde die Eingriffstiefe wiederum ganz erheblich senken.

5. Angesichts der Tatsache, dass die Koordinierung der Einsatzkräfte bislang auch funktioniert hat, wie kann die im Gesetz geforderte notwendige Erforderlichkeit der Maßnahme begründet werden?

Das ist letztlich eine Tatsachenfrage, die sich der rein juristischen Bewertung entzieht. Die Begründung des Gesetzentwurfs lässt jedenfalls nicht erkennen, dass eine Erhebung von Standortdaten tatsächlich *notwendig* ist, sondern beschränkt sich im Kern darauf, deren *Nützlichkeit* festzustellen. Auf die Antwort zu Frage 4 wird ergänzend verwiesen.

IV. Schlussbemerkung

Hierbei handelt es sich um eine vorläufige rechtliche Einschätzung, die ich nach bestem Wissen und Gewissen erstellt habe. Meine endgültige Stellungnahme bleibt der mündlichen Anhörung vorbehalten.

Berlin, im Februar 2015

Dr. iur. Ulf Buermeyer, LL.M. (Columbia)
Richter am Landgericht Berlin