WESTFÄLISCHE WILHELMS-UNIVERSITÄT
Institut für Informations-, Telekommunikations- und Medienrecht (ITM)
- Zivilrechtliche Abteilung -
Prof. Dr. Franziska Boehm
Juniorprofessur für IT-Recht

Leonardo-Campus 9
D-48149 Münster
Tel.: 02 51/83-3 86 00
Fax: 02 51/83-3 86 01
Email:
boehmf@uni-muenster.de

07. Mai 2013

Stellungnahme zum „Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen und des Polizeiorganisationsgesetzes“

Öffentliche Anhörung des Innenausschusses am 8. Mai 2013, Landtag Nordrhein-Westfalen

Aufgrund der recht kurzen Zeitspanne zur Beantwortung des Fragenkatalogs wird nur auf die datenschutzrechtlichen Fragestellungen der §§ 20 a und b des Gesetzesentwurfs zum PolG NRW eingegangen.

A. Regelungsgehalt der §§ 20 a und 20 b, Abfrage von Telekommunikations- und Telemediendaten:

I. Zu den Voraussetzungen der Datenabfrage

Es ist festzustellen, dass die gleichen Eingriffsschwellen sowohl für die Abfrage von Bestandsdaten, der Internetprotokoll-Adresse, wie auch für Verkehrs- und Nutzungsdaten gelten. Über alle Datenarten darf die Polizei nur unter den in § 20 a Abs. 1 Satz 2 genannten Voraussetzungen Auskunft verlangt werden. Entweder muss die „**hohe Wahrscheinlichkeit eines Schades für Leben, Gesundheit oder Freiheit einer Person**“ bestehen oder die Abfrage muss „**zur Abwehr einer gemeinen Gefahr**“ erfolgen. Es ist demnach im ersten Fall keine gegenwärtige Gefahr notwendig, bei der „das schädigende Ereignis bereits begonnen hat oder unmittelbar mit an Sicherheit grenzender Wahrscheinlichkeit bevorsteht“[1], sondern eine etwas geminderte Wahrscheinlichkeitsstufe.

Im zweiten Fall bezieht sich der Begriff „gemeine Gefahr“ auf die Gefährdung von einer unbestimmten Zahl von nicht näher bestimmten Rechtsgütern bei Vorliegen eines „unüberschaubaren Gefahrenpotentials“[2] und findet sich auch in Art. 13 Abs. 4 und 7 GG. Der Begriff wird allerdings nicht näher im PolG NRW definiert und es wird auch kein Straftatenkatalog genannt, der hier für eine Klarstellung sorgen könnte, bei welchen Straftaten eine Abfrage möglich ist. Die Gesetzesbegründung verweist auf den Schutz von hochrangigen Rechtsgütern, vor allem von Suizidenten, Kindern, hilflosen Personen etc. und die Verhinderung angedrohter Straftaten. Welche damit gemeint sind, wird nicht aufgeführt. Eine Klarstellung wäre hier sinnvoll.

Zu begrüßen ist allerdings, dass es für die Abfrage einen Erforderlichkeitsvorbehalt („nur, soweit die Erreichung des Zwecks der Maßnahme auf andere Weise aussichtslos oder wesentlich erschwert wäre“) gibt. Die Frage 19, ob eine Beschränkung der Datenabfrage auf Einzelfälle erforderlich ist, ist mit Blick auf das Urteil des Bundesverfassungsgerichts

---

[1] Schoch in Schmid-Aßmann/Schoch, besonderes Verwaltungsrecht, 14. Auflage 2008,de Gruyter, S. 194, Rn. 100.
[2] Ibid, S. 195.

(BVerfG) zur Umsetzung der Vorratsdatenspeicherungsrichtlinie[3] vom 2. März 2010 zu beantworten. In Randnummer 231 des Urteils heißt es:

> „Die Abwägung zwischen dem Gewicht des in der Datenspeicherung und Datenverwendung liegenden Eingriffs und der Bedeutung einer wirksamen Gefahrenabwehr führt dazu, dass ein Abruf der vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer **gemeinen Gefahr** zugelassen werden darf (vgl. BVerfGE 122, 120 <141 ff.>). Die gesetzliche Ermächtigungsgrundlage **muss diesbezüglich zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die zu schützenden Rechtsgüter verlangen.** Dieses Erfordernis führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze nicht ausreichen, um den Zugriff auf die Daten zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die die Prognose einer **konkreten Gefahr** tragen. Es bedarf insoweit einer Sachlage, **bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden für die Schutzgüter der Norm durch bestimmte Personen verursacht wird.** [...]“

Geht man davon aus, dass das PolG NRW sich an den Formulierungen des Urteils (vgl. eine Gefahr für Leib, Leben oder Freiheit einer Person, oder zur Abwehr einer gemeinen Gefahr) anlehnt, kann geschlussfolgert werden, dass intendiert ist, auch dieselben Anforderungen gelten zu lassen, die das BVerfG in seinem Urteil aufstellt. Wäre dies der Fall, so sollte hinzugefügt werden, dass nur bei „einer Sachlage, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden für die Schutzgüter der Norm durch bestimmte Personen verursacht wird“ eine Abfrage von Telekommunikations- und Telemediendaten stattfinden soll. Um den verfassungsrechtlichen Anforderungen zu entsprechen, sollte die Beschränkung auf Einzelfälle daher im Gesetz festgehalten werden.

Im Vergleich zu anderen Bundesländern und im Vergleich zur Bundesgesetz (siehe Anhang) sind die Hürden zur Datenabfrage für alle Datenarten gleich geregelt und eher im oberen Bereich angesiedelt. Zu den Einzelheiten der Abfrage wird im Folgenden Stellung genommen.

II. Betroffene Daten

Zu begrüßen ist es, dass die einzelnen Datenarten aufgeführt werden, die abgefragt werden dürfen (§ 20 Abs. 1 Nr. 1-3 PolG NRW) und, dass solche Daten, die den Zugriff auf

[3] BVerfG, 1 BvR 256/08 vom 2.3.2010.

Endgeräte oder Speichereinrichtungen schützen (PIN, PUK, Passwörter etc.), nicht unter die Abfrageerlaubnis fallen. Insgesamt sind vier Datenarten genannt: Bestandsdaten i.S.d. §§ 95, 111 TKG, § 11 TMG, die IP-Adressen (§ 113 Abs. 1 S. 3 TKG), einzelne Verkehrsdaten i.S.d. § 96 TKG und bestimmte Nutzungsdaten i.S.d. § 15 TMG. Die Verwendung des Begriffs „Nutzungsdaten“ im Rahmen des TMG entspricht dem Begriff der Verkehrsdaten im Rahmen des TKG. Dass in diesem Zusammenhang der umständliche Begriff „personenbezogene Berechtigungskennung“ für die Bezeichnung der dynamischen IP-Adresse gewählt wurde, ist im Sinne der Normenklarheit nicht unbedingt zu begrüßen. Letztlich sollte auch der die Maßnahme ausführende Polizeibeamte beim Lesen des PolG verstehen, welche Maßnahmen unter die Abfrageerlaubnis des § 20 a Abs. 1 Nr. 2 a) fallen.

III. Betroffene Person

Aus den §§ 20 a und b geht nicht hervor, welche Personen oder Personenkategorien von der Datenabfrage bei den Dienstanbietern betroffen sind. In den anderen in diesem Abschnitt genannten Paragraphen wird hinsichtlich der Adressaten der Maßnahmen auf die §§ 4-6 PolG NRW zurückgegriffen, wenn für die Maßnahmen keine spezifischen Regelungen vorgesehen sind. Zu den besonderen Formen der Datenerhebung (§§ 17-20), die sich im selben Abschnitt (Abschnitt III) befinden, wird daher jeweils explizit auf die Vorschriften über die Verantwortlichkeiten Bezug genommen. Einige Beispiele sind die §§ 16a Abs. 1 Nr. 1, 17 Abs. 1 Nr. 1, 18 Abs. 1 und 19 Abs. 1 Nr. 1[4] PolG NRW.

Auch wenn in diesem Zusammenhang zu beachten ist, dass der Adressat der Maßnahme nach § 20a der Diensteanbieter ist und nicht derjenige Bürger, über den die Daten erhoben werden, sollten Regelungen darüber getroffen werden, von welchen Personen die Daten abgefragt werden dürfen. Dass dies nicht unmöglich ist, zeigt ein Vergleich mit den Polizeigesetzen anderer Länder. Beispielhaft sind hier die §§ 23a PolG BW und 34 b i.V.m.

---

[4] Beispielhaft hier:
§ 16a PolG NRW, Datenerhebung durch Observation: (1)Die Polizei kann personenbezogene Daten erheben durch eine durchgehend länger als 24 Stunden oder an mehr als an zwei Tagen vorgesehene oder tatsächlich durchgeführte und planmäßig angelegte Beobachtung (längerfristige Observation) 1. über die in den **§§ 4 und 5** genannten und unter den Voraussetzungen des **§ 6** über die dort genannten Personen, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist und
§ 17 PolG NRW, Datenerhebung durch den verdeckten Einsatz technischer Mittel: (1) Die Polizei kann personenbezogene Daten erheben durch den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen sowie zum Abhören und Aufzeichnen des gesprochenen Wortes Nr. 1 über die Personen, die in den **§§ 4 und 5** genannt werden, sowie unter den Voraussetzungen des **§ 6** über die dort genannten Personen, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist

34 a PAG Bayern genannt.[5]

Insgesamt fügt sich der § 20a PolG NRW damit weder in das restliche PolG NRW noch in die Regelungen der anderen Bundesländer zur Telekommunikationsdatenabfrage ein. Eine Vorschrift, die spezifiziert, wer die betroffenen Personen von Auskunftsersuchen der Polizei an die Diensteanbieter sind, könnte durch einen Verweis auf die §§ 4-6 PolG NRW eingefügt werden. Andere eventuell betroffene Personen, die nicht unter die in §§ 4-6 PolG NRW genannten Kategorien fallen, müssten dann explizit zusätzlich erwähnt werden. Hinzu

---

[5] **PolG BW, § 23a Besondere Bestimmungen über polizeiliche Maßnahmen mit Bezug zur Telekommunikation**
(1) Der Polizeivollzugsdienst kann ohne Wissen des Betroffenen Verkehrsdaten im Sinne des § 96 Absatz 1 des Telekommunikationsgesetzes über die in den **§§ 6 und 7** sowie unter **den Voraussetzungen des § 9 über die dort genannten Personen erheben**
(5) Auf Grund einer Anordnung nach Absatz 2 oder 3 hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, dem Polizeivollzugsdienst die **Maßnahme nach Absatz 1 zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen.** Von der Auskunftspflicht sind auch zukünftige Verkehrsdaten umfasst. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung in der jeweils geltenden Fassung. Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden.
PAG Bayern, Art. 34a Datenerhebung und Eingriffe in den Telekommunikationsbereich
(1) Die Polizei kann durch die Überwachung und Aufzeichnung der Telekommunikation personenbezogene Daten erheben
1.über die **für eine Gefahr Verantwortlichen**, soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist, oder
2.**über Personen, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen**, dass
a)sie für Personen nach Nr. 1 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen, ohne insoweit das Recht zur Verweigerung des Zeugnisses nach §§ 53, 53a StPO zu haben, oder weitergeben oder
b)die unter Nr. 1 genannten Personen ihre Kommunikationseinrichtungen benutzen werden.
Etc.
Art. 34b, Mitwirkungspflichten der Diensteanbieter
(1) Ist eine Datenerhebung nach Art. 34a Abs. 1 oder Abs. 3 Satz 1 Nr. 1 angeordnet, hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), nach Maßgabe der Regelungen des Telekommunikationsgesetzes und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen in der jeweils geltenden Fassung der Polizei die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen.
(2) Die Polizei kann **unter den Voraussetzungen des Art. 34a Abs. 1 Satz 1** oder Abs. 3 Satz 1 Diensteanbieter verpflichten,
1. ihr vorhandene Telekommunikationsverkehrsdaten der in Art. 34a Abs. 1 Satz 1 und Abs. 3 Satz 1 genannten Personen zu übermitteln,
2. Auskunft über deren zukünftige Telekommunikationsverkehrsdaten zu erteilen oder etc.

kommt, dass in § 20 a Abs. 2 lediglich der Begriff „Dritter“ erwähnt ist. Dieser ist jedoch nicht näher definiert und es stellt sich die Frage, wer (außer dem Störer oder der betroffenen Person) unter diesen Begriff fallen könnte.

IV. Benachrichtigungs- und Löschungspflichten

Grundsätzlich sind die Benachrichtigungs- und Löschungspflichten, geregelt in den §§ 20 a Abs. 2 und Abs. 4 PolG NRW, aus datenschutzrechtlicher Sicht zu begrüßen. Die Löschungspflicht entspricht dem Gebot der Datensparsamkeit. Daten sollen „unverzüglich“ nach der Unterrichtung der Personen gelöscht werden (§ 20 a Abs. (4), S. 3). Hier findet sich ein Verweis auf § 17 Abs. (5) PolG NRW, der vorschreibt auf „die Möglichkeit nachträglichen Rechtsschutzes“ hinzuweisen. In diesem Zusammenhang sollte beachtet werden, dass eventuelle Datenabfragen später nicht nur bei der Einlegung eines Rechtsmittels überprüfbar sein müssen (die Rechtsmittelfrist ist also abzuwarten), sondern auch bei einem möglichen Verfahren unter Einbeziehung des Landesdatenschutzbeauftragten. Fraglich ist also, wie der Begriff „unverzüglich“ auszulegen ist. Da die Rechtmäßigkeit der Maßnahme nach der Benachrichtigung der betroffenen Person nachweisbar sein muss, sollte darauf geachtet werden, dass eine Dokumentation zur Überprüfung der Maßnahme möglich ist. Fälle, in denen Rechtsmittel eingelegt werden oder der Datenschutzbeauftragte angerufen wird und eine Überprüfung der Daten aufgrund einer verfrühten Löschung nicht mehr abrufbar sind, könnten so vermieden werden.

In diesem Zusammenhang soll auch erwähnt werden, dass sich die Erhebung, Speicherung und Löschung von Täter- oder Opferdaten, Verantwortlichen oder Nichtverantwortlichen nach den gleichen Grundsätzen richtet (§ 20 a Abs. 4 S. 3 PolG NRW) und nicht zwischen den verschiedenen Datenarten unterschieden wird. Hier sollten auch Entwicklungen auf europäischer Ebene im Polizeibereich (Entwurf einer Richtlinie für den Datenschutz im Polizeibereich, Europol und Eurojust Beschluss 2009[6]) miteinbezogen werden, die zwischen personenbezogenen Daten verschiedener Kategorien betroffener Personen unterscheiden. An dieser Stelle spielt auch wieder die o.g. Kritik an der Unbestimmtheit des Adressatenkreises eine Rolle. Wenn nicht klar ist, welche Personen von den Maßnahmen betroffen sind, können auch nicht die verschiedenen Datenkategorien unterschieden werden.

[6] Artikel 5 des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr KOM(2012)10 endgültig; Artikel 14 des Europol-Beschlusses 2009/371/JI; Artikel 15 des Eurojust-Beschlusses 2009/426/JI.

V. Fehlender Richtervorbehalt

Ein Richtervorbehalt ermöglicht eine Überprüfung des Abfrageantrags durch eine neutrale und unabhängige Stelle. Im Falle von schweren Grundrechtseingriffen sollen Richtervorbehalte fehlenden oder zu spät kommenden Rechtschutz kompensieren.[7] Es soll also effektiver Rechtsschutz garantiert werden. Im Telekommunikationsbereich formuliert das BVerfG diese Voraussetzung im Urteil zur Vorratsdatenspeicherung wie folgt:

> „Nach der Rechtsprechung des Bundesverfassungsgerichts kann bei Ermittlungsmaßnahmen, die einen schwerwiegenden Grundrechtseingriff bewirken, verfassungsrechtlich eine vorbeugende Kontrolle durch eine unabhängige Instanz geboten sein. Dies gilt insbesondere, wenn der **Grundrechtseingriff heimlich** erfolgt **und für den Betroffenen unmittelbar nicht wahrnehmbar ist** (vgl. BVerfGE 120, 274 <331>). **Für die Abfrage und Übermittlung von Telekommunikationsverkehrsdaten kann dies der Fall sein**. **Angesichts des Gewichts des hierin liegenden Eingriffs reduziert sich der Spielraum des Gesetzgebers dahingehend, dass solche Maßnahmen grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen sind**. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren“[…].[8]

Es ist also zu fragen, welche Intensität der Grundrechtseingriff der vorgesehenen Maßnahmen hat. Alle Maßnahmen in den §§ 20 a und b erfolgen heimlich und sind für den Betroffen nicht wahrnehmbar. Dies entspricht dem Sinn und Zweck der Maßnahme. Im Folgenden werden kurz die verschiedenen Grundrechtseingriffe angesprochen:

a. Auskunft über Bestandsdaten i.S. d. §§ 95, 111 TKG und 14 TMG:

Bei den Bestandsdaten handelt es sich um freiwillige Auskünfte, die bei Abschluss des Vertrages mit dem Telekommunikations- oder Telemedienanbieter getätigt werden. Obwohl hier das Recht auf informationelle Selbstbestimmung zum Tragen kommt[9], besteht wohl kein verfassungsrechtliches Gebot hier einen Richtervorbehalt vorzusehen, da es sich nicht um

---

[7] Gusy, „Überwachung der Telekommunikation unter Richtervorbehalt – Effektiver Grundrechtsschutz oder Alibi“, ZRP 2003, S. 275 mit weiteren Nachweisen.

[8] BVerfG, 1 BvR 256/08 vom 2.3.2010, Rn. 248.

[9] BVerfGE v. 24.01.2012, Az.: 1 BvR 1299/05. Rn. 121 ff.; Kugelmann, Stellungnahme zur Anhörung vor dem Innenausschuss des Deutschen Bundestages zu dem Entwurf eines Gesetzes und zur Neuregelung der Bestandsdatenauskunft, BT Drs. 17/12034, S. 10.

besonders sensible oder besonders geschützte Daten handelt.

b. Auskunft über die dynamische IP-Adresse

Generelle Aussagen für die Eingriffsintensität der Abfrage von dynamischen IP-Adressen zu treffen gestaltet sich schwierig.[10] Das Bundesverfassungsgericht geht in seinem Urteil zur Vorratsdatenspeicherung zwar von einem Eingriff in Art. 10 GG aus, nicht aber von der Notwendigkeit eines Richtervorbehalts. Der Eingriff erfolge nur punktuell und die Verwendung der vorsorglich gespeicherten Daten allein führe lediglich zu der Auskunft, „welcher Anschlussinhaber unter einer bereits bekannten, etwa anderweitig ermittelten IP-Adresse im Internet angemeldet war".[11] Dennoch ist die Eingriffsintensität bei der Abfrage der IP-Adresse höher als bei einfachen Bestandsdaten, da auch Rückschlüsse auf die Inhalte der aufgerufenen Webseite gezogen werden können. Um dieser gesteigerten Eingriffsintensität Rechnung zu tragen, wäre die Überprüfung durch eine unabhängige Stelle ratsam.

c. Auskunft über Verkehrsdaten, i.S.d. § 96 TKG und Nutzungsdaten i.S.d. § 15 TMG

Die Auskunft über Verkehrsdaten stellt einen Eingriff in Art. 10 Abs. 1 GG dar. Der § 100 g StPO, der die Abfrage von Verkehrsdaten auf Bundesebene regelt, genauso wie alle anderen Bundesländer (siehe Tabelle im Anhang) sehen hier einen Richtervorbehalt vor. Die Verkehrs- bzw. Nutzungsdaten geben Ausschluss darüber, wer mit wem zu welcher Zeit und wie lange telefoniert hat. Die Abfrage dieser Daten greift daher intensiver in Grundrechte ein, als die Abfrage von Bestandsdaten. Dieser erhöhten Eingriffsintensität wird aber nicht durch einen Richtervorbehalt Rechnung getragen. Auch wenn die Eingriffshürden für die Abfrage von allen Daten relativ hoch angesetzt sind, wäre eine unterschiedliche Gewichtung der Abfragemöglichkeiten für die unterschiedlichen Datenarten durch die Einführung eines Richtervorbehalts anzuraten.

d. Einsatz von IMSI Catchern

Die Fragestellung, ob die Ermittlung des Standorts von Mobiltelefonen durch Einsatz eines IMSI-Catchers in das Grundrecht aus Art. 10 GG eingreift, war Gegenstand des Urteils des

[10] VGl. hier mit einer ausführlichen Würdigung: *Bäcker*, Stellungnahme zur Anhörung vor dem Innenausschuss des Deutschen Bundestages zu dem Entwurf eines Gesetzes und zur Neuregelung der Bestandsdatenauskunft, BT Drs. 17/12034, S. 10 ff.
[11] BVerfG, 1 BvR 256/08 vom 2.3.2010, Rn. 256.

BVerfG zur Vorratsdatenspeicherung sowie zur Verfassungsmäßigkeit der Ermittlung von Mobilfunkdaten durch IMSI-Catcher (Beschluss vom 22.8.2006 – 2 BvR 1345/03). In beiden Urteilen kam das BVerfG zu dem Schluss, dass der Einsatz von IMSI-Catchern nicht in den Schutzbereich der Telekommunikationsfreiheit (Fernmeldegeheimnis) aus Art. 10 Abs. 1 GG eingreife, da das Fernmeldegeheimnis nur die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs schütze[12]. Geschützt seien in erster Linie die Vertraulichkeit der ausgetauschten Informationen und damit der Kommunikationsinhalt gegen unbefugte Kenntniserlangung durch Dritte.[13] Die Feststellung einer Geräte- oder Kartennummer stehe allerdings nicht in unmittelbarem Zusammenhang mit einem tatsächlich stattfindenden oder zumindest versuchten Kommunikationsvorgang zwischen Menschen, vielmehr kommunizieren lediglich technische Geräte miteinander.[14] Das Grundrecht auf informationelle Selbstbestimmung ist zwar berührt[15], das BVerfG geht jedoch von einer „geringen Eingriffsintensität“ aus.[16] Die bundesrechtliche Regelung in § 100i StPO, die den Einsatz von IMSI-Catchern regelt, sieht hier dennoch einen Richtervorbehalt vor.

Auch wenn es nicht in allen o.g. Einzelfällen verfassungsrechtlich geboten scheint, einen Richtervorbehalt vorzusehen, ergibt ein Vergleich mit den Regelungen der anderen Bundesländer ein eindeutiges Bild: NRW wäre, wenn das PolG NRW in seiner jetzigen Form verabschiedet würde, das einzige Land ohne jeglichen Richtervorbehalt. Insbesondere in Bezug auf die Abfrage von IP-Adressen und den Einsatz von IMSI Catchern wäre dies ein bedenkliches Signal. Auch in Fällen, in denen nicht nur *eine* Maßnahme angeordnet werden soll, sondern ein Kumulation von den in §§ 20 a und b genannten Maßnahmen stattfinden soll, erscheint eine Überprüfung durch eine unabhängige Stelle geboten. Der Grundrechtseingriff wird dann intensiviert und die Eingriffsintensität höher, wenn alle Daten auf einmal abgefragt werden. Auch wenn die einzelne Maßnahme nicht unter einen

---

[12] BVerfGE 67, 157, 172; 106, 28, 35 f.; bestätigt durch Beschluss vom 22.8.2006 – 2 BvR 1345/03, Rn. 51, vgl. http://www.bundesverfassungsgericht.de/entscheidungen/rk20060822_2bvr134503.html

[13] BVerfGE 100, 313, 358; 107, 299, 312; bestätigt durch Beschluss vom 22.8.2006 – 2 BvR 1345/03, RNn. 52, vgl. http://www.bundesverfassungsgericht.de/entscheidungen/rk20060822_2bvr134503.html

[14] BVerfG Beschluss vom 22.08.2007 – 2 BvR 1345/03, RN 57; Weitere Nachweise im Beschluss des BVerfG: Günther, NStZ 2005, S. 485 Fn 1, 491; Jordan, Kriminalistik 2005, S. 514 <515 f.>; Demko, NStZ 2004, S. 57 <61>; Eisenberg/Singelnstein, NStZ 2005, S. 62 <66>; Bernsmann, NStZ 2002, S. 103; Günther, Kriminalistik 2004, S. 11 <14>; Weßlau, ZStW Bd. 113 <2001>, S. 681 <690>; Kudlich, JuS 2001, S. 1165 <1168>, vgl. http://www.bundesverfassungsgericht.de/entscheidungen/rk20060822_2bvr134503.html

[15] BVerfG, Beschluss vom 22.8.2006 – 2 BvR 1345/03, Rn. 67.

[16] BVerfG, Beschluss vom 22.8.2006 – 2 BvR 1345/03, Rn. 77.

Richtervorbehalt fällt, wäre daher bei einer Kumulation der Maßnahmen oder durch eine Abfrage von Daten, die einen längeren Zeitraum betreffen, ein Richtervorbehalt dringend zu empfehlen.

B. Thesenartige Zusammenfassung:

- Zu den Voraussetzungen der Abfrage:
  Die Abfrageerlaubnis sollte auf Einzelfälle beschränkt werden.
- Zu den betroffenen Personen:
  Es müssen Regelungen darüber getroffen werden, von welchen Personen die Daten abgefragt werden dürfen. Dies kann durch einen Verweis auf §§ 4-6 PolG NRW geschehen. Es sollte auch spezifiziert werden, wer „Dritte“ i.S.d. §§ 20 a und b PolG NRW sind.
- Zu den Benachrichtigungs- und Löschungspflichten:
  Hier ist die Bedeutung des Begriffs „unverzüglich“ unklar. Es sollte darauf geachtet werden, dass die abgefragten Daten zur Überprüfung der Maßnahme vorliegen.
- Zum fehlenden Richtervorbehalt:
  Hier sollte für jede Datenart einzeln überprüft werden, ob ein Richtervorbehalt von Nöten ist.

Anhang: Tabelle mit Übersicht und Vergleich über die Regelungen anderer Bundesländer und dem Bundesgesetz

Anhang zur Stellungnahme PolG NRW, Prof. Dr. Franziska Boehm: Übersicht über die Regelungen anderer Bundesländer und des BundesPolG

	NRW	Bayern	Niedersachsen	Rheinland-Pfalz
Erfasste Daten	**Bestandsdaten** iSd §§ 95, 111 TKG, § 11 TMG; **Folgende Verkehrsdaten** iSd § 96 TKG Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennung, bei Verwendung von Kundenkarten die Kartennummer, bei mobilen TK-Endgeräten auch die Standortdaten **Folgende Nutzungsdaten** iSd § 15 TMG Merkmale zur Identifikation des Nutzers, Angaben über den Beginn und das Ende sowie den Umfang der jeweiligen Nutzung nach Datum und Uhrzeit.	○ vorhandene Telekommunikationsverkehrsdaten ○ zukünftige Telekommunikationsverkehrsdaten ○ für die Ermittlung des Standortes eines Mobilfunkendgerätes erforderliche spezifischen Kennungen (§ 34b Abs. 2 i.V.m. § 34a Abs. 1, 3)	○ Telekommunikationsverbindungsdaten i.S.d. § 96 TKG (§ 33c i.V.m. § 33 Abs. 1 Nds.SOG i.V.m. § 100g StPO) ○ **Inhalte der TK** einschließlich der innerhalb des TK-Netzes in Datenspeichern abgelegten Inhalte. ○ **TK-Verbindungsdaten**, **Standortkennung** einer aktiv geschalteten Mobilfunkeinrichtung	○ Auskünfte über die TK, § 31 Abs.1 POG RLP; Umfasst Inhalte der TK und Verkehrsdaten, § 31 Abs. 2 ○ Auskünfte über Nutzungsdaten nach § 15 TMG, § 31b Abs. ○ Ermittlung von spezifischen **Kennungen** (insb. Geräte- und Kartennummer) ○ **Standort**
Voraussetzungen der Datenabfrage	Hohe Wahrscheinlichkeit eines Schadens für Leben Gesundheit oder Freiheit oder Abwehr einer gemeinen Gefahr	Dringende Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Dringende Gefahr für Leib, Leben oder Freiheit einer Person	○ Gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person	Gegenwärtigen Gefahr für Leib oder Leben einer Person oder Gegenwärtige Gefahr für solche Güter der Allgemeinheit, deren Bedrohung die Grundla-

	Und nur, soweit die Erreichung des Zwecks der Maßnahme auf andere Weise aussichtslos oder wesentlich erschwert wäre	oder Abwehr einer dringenden Gefahr für Sachen, soweit eine gemeine Gefahr besteht		gen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, und nur, soweit zwingend erforderlich
Richtervorbehalt	**Nein**	**Ja** (§ 34c Abs. 1 iVm § 34 Abs. 4 PAG)	**Ja** (§33c S. 2 i.V.m. § 33a Abs. 4 SOG)	**Ja** (§§ 31 Abs. 4, 31a Abs. 3, 31b iVm 31 Abs. 4 POG)
Nachholung der richterlichen Anordnung bei Gefahr im Verzug möglich	kein Richtervorbehalt	**Ja**, behördliche Anordnung muss unverzüglich durch den Richter bestätigt werden (§ 34c Abs. 1 iVm § 34 Abs. 4 PAG)	**Ja**, behördliche Anordnung muss innerhalb von drei Tagen durch den Richter bestätigt werden (§33c S.2 i.V.m. 33a Abs. 5 SOG)	**Ja**, behördliche Anordnung muss unverzüglich durch den Richter bestätigt werden. (§§ 31 Abs. 5, 31a Abs. 3, 31b iVm 31 Abs. 5 POG)
Wegfall des Richtervorbehalts bei der Standortermittlung einer gefährdeten Person		**Ja** (§ 34c Abs. 2 PAG) Maßnahme dient der Ermittlung des Aufenthaltsortes der gefährdeten Person		**Nur bei Gefahr im Verzug** (§ 31a Abs. 3 POG) Datenerhebung erfolgt zur Ermittlung des Aufenthaltsortes einer vermissten, suizidgefährdeten oder sonstigen hilflosen Person

Einteilung der Betroffenen in Verantwortliche und Nichtverantwortliche	**Nein,** Dritte werden genannt	**Ja** ○ Verantwortliche, bzw. Personen, welche Nachrichten von oder für diese entgegennehmen / weiterverbreiten (§ 34b Abs. 2 S. 1 Nr. 1 i.V.m. § 34a Abs. 1 S. 1 PAG) ○ Gefährdete Personen (§ 34b Abs. 2 S. 1 Nr. 1 i.V.m. § 34c Abs. 2 PAG; § 34a Abs. 3 S. 1,)	**Ja** ○ Verantwortlicher (§ 33a Abs. 1 Nr. 1 SOG) ○ Nichtverantwortliche (§ 33a Abs. 1 Nr. 2) (§ 33c S.1: In § 33a Abs. 1 genannte Personen)	**Ja** ○ Verantwortlicher, § 31b Abs. 1 Nr.1 i.V.m. §§ 4, 5 ○ Nichtverantwortlicher, § 31b Abs. 1 Nr. 1 i.V.m. § 7 ○ Zudem: Personen, die Mitteilungen für oder von Verantwortlichen nach §§ 4, 5 entgegennehmen oder weitergeben, § 31b Abs. 1 Nr. 2

	Baden-Württemberg	**Brandenburg**	**Thüringen**	**Saarland**
Erfasste Daten	○ Verkehrsdaten i.S.d. § 96 Abs. 1 TKG, § 23a Abs. 1 BW PolG, ○ Vertrags- / Bestandsdaten i.S.d. §95 TKG, § 23a Abs. 9 BW PolG ○ Daten gem. § 111 TKG	○ Vorhandene Verkehrsdaten, ○ Standortdaten ○ Zukünftige Verkehrsdaten Jeweils gem. § 33b Abs. 6 BbgPolG	○ Verkehrsdaten gem. §§ 96 Abs. 1 und 113a TKG, § 34a PAG	○ Verkehrsdaten nach dem TKG ○ Standortdaten ○ Jeweils § 28b Abs. 2 a.E.
Voraussetzungen der Datenabfrage	konkrete Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand oder die Sicherheit des Bundes oder	Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand oder die Sicherheit des Bundes oder des Landes	dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person	gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder vorbeugenden Bekämpfung der in § 100c der Strafpro-

	eines Landes oder gemeine Gefahr		oder für Sachen, soweit eine gemeine Gefahr besteht	zessordnung genannten Straftaten, § 28b Abs. 2
Richtervorbehalt	**Ja** (Anordnung durch AG), § 23a Abs. 2	**Ja,** § 33b Abs. 6 S. 4	**Ja,** § 34a Abs. 5 S. 1PAG	**Ja**, § 28b Abs. 5 S. 1
Nachholung der richterlichen Anordnung bei Gefahr im Verzug möglich	Ja, § 23a Abs. 2 S. 7 i.V.m. § 23 Abs. 3 S.8	Ja, bei unverzüglicher richterlicher Bestätigung, § 33b Abs. 6 S. 4	Ja, § 34a Abs. 5 S. 2 PAG (gem. S. 3 gerichtliche Bestätigung innerhalb von 3 Tagen erforderlich)	Ja, § 28b Abs.4 S. 4; unverzügliche Nachholung erforderlich
Wegfall des Richtervorbehalts bei der Standortermittlung einer gefährdeten Person	Ja, § 23a Abs. 3, hinsichtlich vermissten, suizidgefährdeten oder hilflosen Personen	Ja, wenn Gefahr im Verzug, § 33b Abs. 6 S. 4, letzter Hs.		
Einteilung der Betroffenen in Verantwortliche und Nichtverantwortliche	○ Verantwortliche gem. §§ 6, 7 ○ Unbeteiligte unter bes. Voraussetzungen des § 9	Ja, Einteilung in Verantwortlichen und Notstandspflichtigen gem. § 33b Abs. 6 S. 1 i.V.m. § Abs. 2	○ Verantwortliche gem. § 34a Abs. 3 S.1 Nr.1 ○ Mutmaßlich Beteiligte einer Straftat, Nr. 2 ○ Andere Personen nur, wenn unvermeidliche Folge von Erhebungen bei o.g. Personen	○ Verantwortliche gem. § 28b Abs. 1 i.V.m. §§ 4, 5 ○ Nichtverantwortliche gem. § 6 ○ Personen, die mutmaßlich Straftaten begehen werden, § 28b Abs. 1 S.1 Nr.2

	Sachsen-Anhalt	Hessen	M-V (Entwurf der LReg)	BundesPolG
Erfasste Daten	Verkehrsdaten i.S.d. § 3 Nr. 30 TKG; § 17a SOG LSA	Verkehrsdaten i.S.d. §§ 96, 113a TKG	Nur Bestands- und Vertragsdaten gem. § 95, 111 TKG (Bisher nur Überwachung und Aufzeichnung geregelt, § 34a SOG M-V)	Vertrags- und Bestandsdaten gem. §§ 95, 111 TKG; § 22a BPolG
Voraussetzungen der Datenabfrage	Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person	gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person	Gefahr im Einzelfall	Erforderlichkeit zur Ermittlung eines Sachverhaltes oder Aufenthaltsortes einer Person, wenn diese Daten zur Erfüllung einer der BPol obliegenden Aufgabe erforderlich
Richtervorbehalt	Ja, § 17a SOG LSA	Ja, § 15a Abs. 5 S. 1	Nein, allerdings sind auch keine Verkehrsdaten erfasst (s.o.)	Nein, allerdings sind auch keine Verkehrsdaten erfasst
Nachholung der richterlichen Anordnung bei Gefahr im Verzug möglich	Ja	Ja	/	
Wegfall des Richtervorbehalts bei der Standortermittlung einer gefährdeten Person	/	/	/	
Einteilung der Betroffenen in Verantwortliche und Nichtverantwortliche	○ Gefahrverursacher ○ Personen die für o.g. Mitteilungen entgegennehmen oder weitergeben ○ Jeder Person, soweit unerlässlich		Nein, allerdings sind keine Verkehrsdaten erfasst (s.o.)	Nein, allerdings sind auch keine Verkehrsdaten erfasst

Anmerkungen:

- Die Tabelle erhebt keinen Anspruch auf Vollständigkeit.
- Nicht aufgeführte Bundesländer haben (noch) keine Regelungen zur Abfrage von Bestands- Verbindungs- oder Nutzungsdaten in den Polizeigesetzen getroffen, in Mecklenburg-Vorpommern ist eine entsprechender Entwurf von der Landesregierung beschlossen worden, ein Landtagsbeschluss steht aber noch aus.
- § 20a PolG NRW enthält keine Aussagen darüber, über wen die fraglichen Daten erhoben werden dürfen.
- Es wird damit von dem Grundsatz des Gefahrenabwehrrechts, dass sich konkrete Maßnahmen in erster Linie gegen den Verantwortlichen und nur unter besonderen Voraussetzungen des Einzelfalls gegen Nichtverantwortliche (Notstandspflichtige) richten dürfen, abgewichen, obwohl die Abfrage von Verkehrs- und Nutzungsdaten einen erheblichen Eingriff in das Fernmeldegeheimnis darstellt.
- Diesem Grundsatz entsprechend ist es sowohl in NRW für andere Formen der Datenerhebung (vgl. §§ 17-20 PolG NRW) als auch in den anderen Bundesländern hinsichtlich der Abfrage von TK-Daten in der Regel (Ausnahme wohl Hessen s.o., sowie Mecklenburg-Vorpommern, welches aber nur Bestandsdaten erfasst die nicht unter das Fernmeldegeheimnis fallen) üblich, besondere Voraussetzungen hinsichtlich der betroffenen Person, insbesondere für Nichtverantwortliche, zu statuieren.
  Die Eingriffsschwelle liegt damit hinsichtlich Nichtverantwortlichen deutlich unter derjenigen der meisten anderen Befugnisse.
- In den anderen Bundesländern sind i.d.R. nur Verkehrs- nicht hingegen Nutzungsdaten von den Befugnissen umfasst
- **Im Gegensatz zu allen anderen Landespolizeigesetzen ist die Abfrage nicht unter Richtervorbehalt gestellt**.
- Insgesamt erhalten die Behörden in NRW damit (unter den etwas strengeren Voraussetzungen, unter denen eingegriffen werden darf) weitreichendere Befugnisse als in den anderen Bundesländern, da sie an weniger formelle Voraussetzungen und keine (präventive) gerichtliche Kontrolle geknüpft sind. Die Kenntnisnahme oder Überprüfbarkeit derartig eingriffsintensiver Maßnahmen durch externe Stellen (Gerichte oder den Betroffenen selbst) ist daher alleine von der Einhaltung der Unterrichtungspflicht nach § 20a Abs. 4 durch die handelnde Behörde abhängig.

Prof. Dr. Franziska Boehm, Juniorprofessur für IT-Recht, WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER, Institut für Informations-, Telekommunikations- und Medienrecht (ITM) - Zivilrechtliche Abteilung -, 07. Mai 2013