Prof. Dr. Viola Schmid, LL.M. (Harvard)

cylaw
tu-darmstadt

2. SIRA Conference Series:
Innere Sicherheit – auf Vorrat gespeichert?

„Die Vorratsdatenspeicherungsentscheidung des BVerfG – Eckpfeiler für eine Charta des (internationalen) (IT-)Sicherheitsrechts?“

Universität der Bundeswehr München, 26. – 27. Mai 2011

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA
Sicherheit im öffentlichen Raum

Outline

cylaw
tu-darmstadt

A. „?“
B. „Recht“
C. „Sicherheit“
D. „(IT-)Sicherheit“
E. „Nationales (IT)-Sicherheitsrecht“

I. „SPI“-Modell (Staat - Private - IT-Sicherheit) als Gesamtsicht
II. Rationes decidendi des BVerfG
1. „Antiprofilierungsratio“
2. „Differenzierungsratio“(SPI-Modell)
3. „Kernbereichsratio
4. „Kombinationsratio“
5. IT-Sicherheit als Verfassungsprinzip

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

Outline

cylaw
tu-darmstadt

a) Qualität der IT-Sicherheit: „besonders hohe[r] Standard“
b) Realisierung der Qualitätsanforderungen
(1) Getrennte Speicherung der Daten
(2) Anspruchsvolle Verschlüsselung
(3) Gesichertes Zugriffsregime unter Nutzung etwa des 4-Augen-Prinzips
(4) Revisionssichere Protokollierung
(5) Einhaltung des Zweckbindungsgrundsatzes (bestimmte Zwecke; mit Erreichen der Zwecke Löschungsverpflichtung)
(6) Effektivität der Durchsetzung der IT-Standards bei der Übermittlung: Pedigree (Kennzeichnung)
(7) Differenzierung: „Push“- und „Pull-Betrieb“

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

Outline

cylaw
tu-darmstadt

F. „Internationales (IT-) Sicherheitsrecht“ im 3-Ebenen-Modell

I. Staatliche und private (Rechtsdurchsetzungs-)Interessen

1. Völkerrecht

a) Sicherheitsrecht (staatliche Interessen)

b) Urheberrecht (private Interessen)

2. Europarecht

a) Sicherheitsrecht (staatliche Interessen)

b) Urheberrecht (private Interessen)

3. Deutsches Recht

a) Sicherheitsrecht (staatliche Interessen)

b) Urheberrecht (private Interessen)

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

Outline

cylaw
tu-darmstadt

II. Identitätsvorbehalt nach deutschem Verfassungsrecht in der Rechtsprechung des BVerfG

1. Lissabon-Entscheidung

2. Welche „rationes“ gehören zum „unantastbaren Kerngehalt der Verfassungsidentität des Grundgesetzes“?

G. „Eckpfeiler?“

I. Konflikt der „Kombinationsratio“ des BVerG mit der „Trennungsratio“ des EuGH in seiner „VDS (1)“-Entscheidung

1. „Trennungsratio“

a) EuGH „VDS (1)“: Keine Kompetenz der EG wenn Datennutzung mitgeregelt wird.

b) Ril 2006/24/EG überlässt Regelung des Zugangs den Mitgliedstaaten

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

Outline

cylaw
tu-darmstadt

2. EuGH „VDS (1)“ und BVerfG „VDS“ im Wortlaut

II. Vorläufiges Fazit zur Rechtslage vor dem 01.12.2009 im Hinblick auf den EG-Vertrag

III. Caveat: Ist die „Trennungsratio“ des EuGH mit dem Vertrag von Lissabon Rechtsgeschichte?

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

A. „?“

cylaw
tu-darmstadt

Cyberlaw: „Das Recht der Verteilung von Chancen und Risiken, Rechten und Pflichten im Cyberspace“.

Subdisziplin: „Informationstechnologisches Sicherheitsrecht“ – das Recht des

- „Ob“ und des
- „Wie“

der Informationstechnologie in der Sicherheitspolitk (Gefahrenabwehr, Verfolgungsvorsorge, Strafverfolgung).

„?“: Notwendigkeit

- inter- und multidisziplinärer Forschung,
- dynamisch-technikorientierter Auslegung von Recht,
- einer „Blankett-Strategie“.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

B. „Recht“

cylaw
tu-darmstadt

Traditionell: Legislative, Exekutive, Judikative.

„Informationstechnologisches Sicherheitsrecht“: BVerfG als „Reserve-gesetzgeber“ → „**Karlsruher Republik**“

- „Akustische Wohnraumüberwachung“,
- „Polizeirechtliche Telekommunikationsüberwachung“,
- „Rasterfahndung“,
- „Kennzeichenscanning“,
- „Online-Durchsuchung“,
- „Videosurveillance-Denkmal“,
- „Geschwindigkeitsüberwachung“,
- „Kontostammdaten“.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

C. „Sicherheit“

cylaw
tu-darmstadt

Artikel 67 AEU:

(1) Die Union bildet einen Raum der **Freiheit**, der **Sicherheit** und des **Rechts**, in dem die **Grundrechte** und die verschiedenen **Rechtsordnungen** und **-traditionen** der **Mitgliedstaaten geachtet werden**.

(2) […]

„Sicherheit gilt es nicht zu definieren, sondern als Prozess zu optimieren.“

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

D. „(IT-)Sicherheit“

cylaw
tu-darmstadt

Thesen:

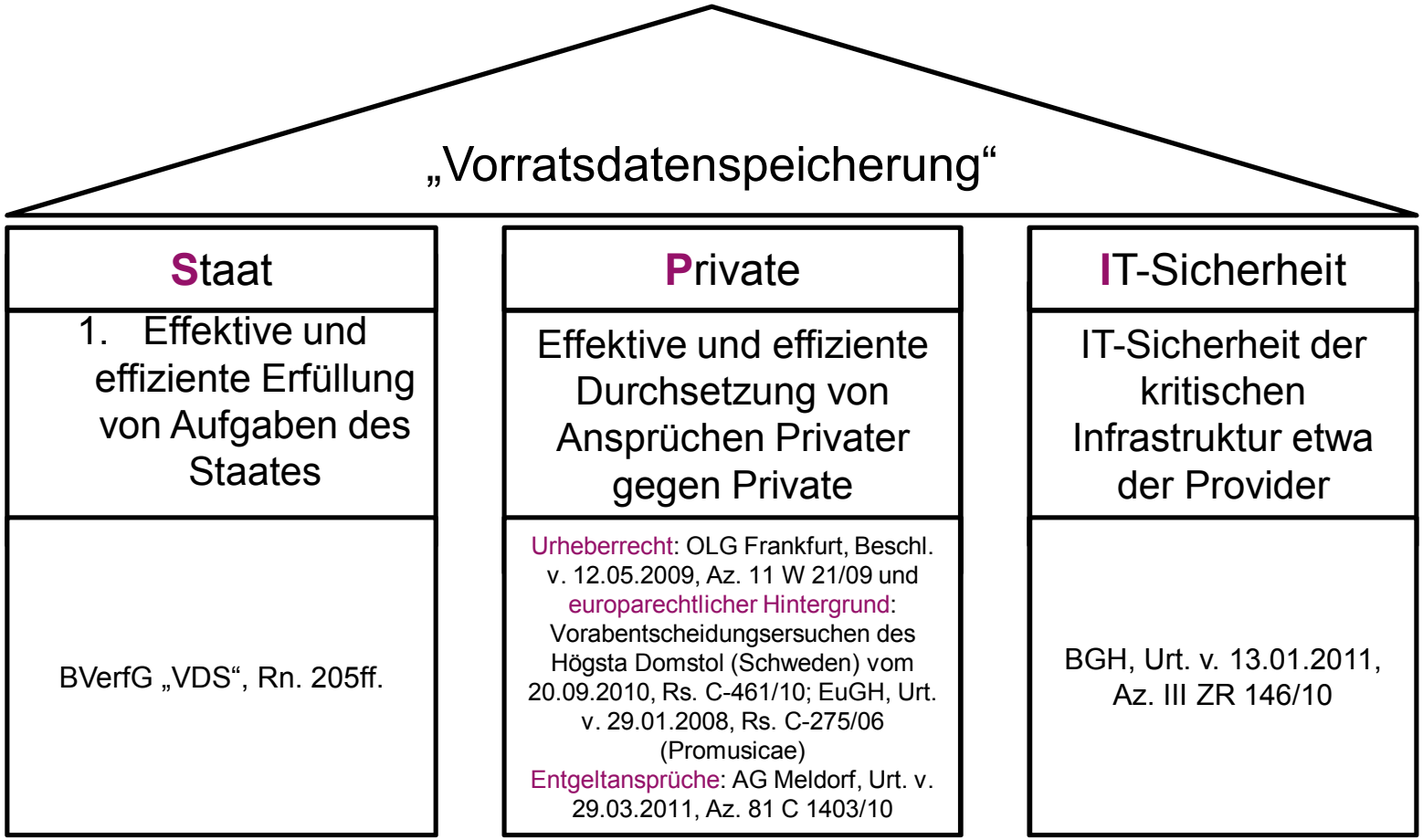
- Keine Sicherheitspolitik ohne Informationstechnologie,
- Keine sicherheitspolitischen „Erfolge“ ohne sichere Informationstechnologie „(IT-) Sicherheit“ ,
- Neue externe und interne Bedrohungsszenarien im/in Ubiquitous Computing, Ambient Assisted Living (AAL), Connected Worlds, Internet of Things, Computer Assisted Living (CAL).
- Klammer „(IT-)“ symbolisiert Verknüpfung von IT-Sicherheit und Sicherheit.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

E. „Nationales (IT-)Sicherheitsrecht“
I. „SPI“-Modell (Staat - Private - IT-Sicherheit) als Gesamtsicht

cylaw
tu-darmstadt



GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

E. I. „SPI“-Modell (Staat - Private - IT-Sicherheit) als Gesamtsicht

cylaw
tu-darmstadt

Staat	Private	IT-Sicherheit
Effektive und effiziente Erfüllung von Aufgaben des Staates	Effektive und effiziente Durchsetzung von Ansprüchen Privater gegen Private	IT-Sicherheit der kritischen Infrastruktur etwa der Provider
etwa § 100 g StPO, § 15 a Abs. 2 HSOG	etwa § 101 Abs. 1, 2, 9 UrhG und § 97 TKG	§§ 100, 109 TKG

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

E. II. Rationes decidendi des BVerfG
1. „Antiprofilierungsratio“

cylaw
tu-darmstadt

Ständige Rechtsprechung seit BVerfGE 65, 1 (43) (Volkszählung):

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, **wer was wann und bei welcher Gelegenheit über sie weiß**.“

Aufrechterhalten in BVerfG „Vorratsdatenspeicherung“ (im Folgenden: BVerfG „VDS“)

< 241>: „Eine vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten über sechs Monate ist unter anderem deshalb ein so schwerwiegender Eingriff, weil sie ein Gefühl des ständigen Überwachtwerdens hervorrufen kann; sie erlaubt in unvorhersehbarer Weise tiefe Einblicke in das Privatleben, ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich ist. Der Einzelne weiß nicht, was welche staatliche Behörde **über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können**.“

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

E. II. 2. „Differenzierungsratio“

cylaw
tu-darmstadt

- Vorratsdatenspeicherung: Es handelt sich im Hinblick auf § 3 Abs. 3 – 5 BDSG um eine unpräzise Qualifizierung der involvierten Informationstechnologien, weil es sich um die **E**rhebung, **S**peicherung, **Ü**bermittlung und **N**utzung von Daten („**ESÜN**“) handelt.
- BVerfG „VDS“ differenziert zwischen Speicherung und Übermittlung und lässt im Rahmen der Übermittlung nur Push-Betrieb zu.

BVerfG „VDS“:

<250> Zur Wirksamkeit der Kontrolle gehört es auch, dass die Daten aufgrund der Anordnung von den Telekommunikationsunternehmen als speicherungsverpflichteten Dritten herausgefiltert und übermittelt werden, das heißt den Behörden also **nicht ein Direktzugriff** auf die Daten eröffnet wird. Auf diese Weise wird die Verwendung der Daten auf das **Zusammenwirken verschiedener Akteure** verwiesen und damit in **sich gegenseitig kontrollierende Entscheidungsstrukturen** eingebunden.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

E. II. 3. „Kernbereichsratio“

cylaw
tu-darmstadt

„Enge[r] Kreis auf besondere Vertraulichkeit angewiesener Telekommunikationsverbindungen“

BVerfG „VDS“:

<238> Verfassungsrechtlich geboten ist […], zumindest für einen **engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikations-verbindungen** ein grundsätzliches Übermittlungsverbot vorzusehen. Zu denken ist hier etwa an **Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern** ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen (vgl. § 99 Abs. 2 TKG).

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

E. II. 4. „Kombinationsratio“

cylaw
tu-darmstadt

Wer die Erhebung, Speicherung und Übermittlung regelt (Art. 73 Abs. 1 Nr. 7 GG „Telekommunikationsrechtliche Kompetenz“), muss klare Kriterien zur Nutzung zugrunde legen („Sachkompetenz“).

BVerfG „VDS“:

<264> 5. Die […] den Verhältnismäßigkeitsanforderungen genügenden normenklaren Begrenzung der Datenverwendung ist ein untrennbarer Bestandteil der Anordnung der Speicherungsverpflichtung und obliegt deshalb dem die Verpflichtung auferlegenden Bundesgesetzgeber. […]

<213> Allerdings entspricht es der ständigen Rechtsprechung des Bundesverfassungsgerichts, dass dem Staat eine Sammlung von personenbezogenen Daten auf Vorrat **zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich strikt untersagt ist** (vgl. BVerfGE 65, 1 <46>; 100, 313 <360>; 115, 320 <350>; 118, 168 <187>).

<266> Demgegenüber ist es unzulässig, **unabhängig von solchen Zweckbestimmungen einen Datenpool auf Vorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt.**

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

E. II. 5. IT-Sicherheit als Verfassungsprinzip

cylaw tu-darmstadt

a) Qualität der IT-Sicherheit: „besonders hohe[r] Standard“

BVerfG „VDS“:

<221> Eine Speicherung der Telekommunikationsverkehrsdaten im Umfang des § 113a TKG bedarf der gesetzlichen Gewährleistung eines **besonders hohen Standards der Datensicherheit**.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

E. II. 5. IT-Sicherheit als Verfassungsprinzip

cylaw
tu-darmstadt

b) Realisierung der Qualitätsanforderungen

(1) Getrennte Speicherung der Daten
(2) Anspruchsvolle Verschlüsselung
(3) Gesichertes Zugriffsregime unter Nutzung etwa des 4-Augen-Prinzips
(4) Revisionssichere Protokollierung
(5) Einhaltung des Zweckbindungsgrundsatzes (bestimmte Zwecke; mit Erreichen der Zwecke Löschungsverpflichtung)
(6) Effektivität der Durchsetzung der IT-Standards bei der Übermittlung: Pedigree (Kennzeichnung)
(7) Differenzierung: „Push"- und „Pull-Betrieb"

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

E. II. 5. IT-Sicherheit als Verfassungsprinzip

cylaw
tu-darmstadt

b) Realisierung der Qualitätsanforderungen

BVerfG „VDS“ :

<223> [Sachverständigenvortrag in der mündlichen Verhandlung und in schriftlichen Stellungnahmen (Ergänzung der Verfasserin):] […] ein weites Spektrum von Instrumenten zur Erhöhung der Datensicherheit aufgezeigt. **Genannt wurden etwa** eine **getrennte Speicherung** der nach § 113a TKG zu speichernden Daten auf auch **physisch getrennten und vom Internet entkoppelten Rechnern, eine asymmetrische kryptografische Verschlüsselung unter getrennter Verwahrung der Schlüssel, die Vorgabe des Vier-Augen-Prinzips** für den Zugriff auf die Daten verbunden **mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln, die revisionssichere Protokollierung des Zugriffs auf die Daten und deren Löschung** sowie der Einsatz von automatisierten Fehlerkorrektur- und Plausibilitätsverfahren. Ergänzend […] **Schaffung von Informationspflichten bei Datenschutzverletzungen, die Einführung einer verschuldensunabhängigen Haftung oder eine Stärkung der Ausgleichsansprüche für immaterielle Schäden** […].

<250> Zur Wirksamkeit der Kontrolle gehört es auch, dass die Daten aufgrund der Anordnung von den Telekommunikationsunternehmen als speicherungsverpflichteten Dritten herausgefiltert und übermittelt werden, das heißt den Behörden **also nicht ein Direktzugriff auf die Daten** eröffnet wird. Auf diese Weise wird die Verwendung der Daten auf das Zusammenwirken verschiedener Akteure verwiesen und damit in sich gegenseitig kontrollierende Entscheidungsstrukturen eingebunden.

F. „Internationales (IT-)Sicherheitsrecht“ im 3-Ebenen-Modell
I. Staatliche und private (Rechtsdurchsetzungs-) Interessen
1. Völkerrecht

cylaw tu-darmstadt

a) Sicherheitsrecht (staatliche Interessen)

BVerfG „VDS“ zur Convention on Cybercrime:

<87> § 100g StPO hat darüber hinaus für das Übereinkommen des Europarats über Computerkriminalität (BGBl II S. 1242; im Folgenden: Übereinkommen über Computerkriminalität) Bedeutung (vgl. BTDrucks 16/5846, S. 27 f. und 50). Das Übereinkommen verpflichtet nicht nur zur Schaffung materiellen Strafrechts zur Bekämpfung der Computerkriminalität, sondern auch zu bestimmten strafverfahrensrechtlichen Regelungen. **Insbesondere sind nach Art. 16 des Übereinkommens die zuständigen Behörden zu ermächtigen, die umgehende Sicherung von Verkehrsdaten anzuordnen.** Personen, in deren Kontrolle sich solche Daten befinden, müssen verpflichtet werden können, diese kurzfristig und unversehrt zu sichern, um den zuständigen Behörden zu ermöglichen, deren Weitergabe zu erwirken (sogenanntes Quick Freezing). Eine entsprechende Regelung hielt der Gesetzgeber allerdings für entbehrlich, weil die einzufrierenden Daten aufgrund der umfassenden Speicherung nach § 113a TKG ohnehin aufbewahrt werden müssten (vgl. BTDrucks 16/5846, S. 53).

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

F. I. 1. Völkerrecht

cylaw
tu-darmstadt

b) Urheberrecht (private Interessen)

EuGH „Promusicae“ zum TRIPS-Übereinkommen:
<60> Die von Promusicae geltend gemachten Art. 41, 42 und 47 des TRIPS-Übereinkommens, wonach das Gemeinschaftsrecht in einem Bereich, für den das Übereinkommen gilt, wie das bei den im Rahmen des vorliegenden Vorabentscheidungsersuchens genannten Bestimmungen der Fall ist, so weit wie möglich nach diesen Vorschriften auszulegen ist (vgl. in diesem Sinne Urteile vom 14. Dezember 2000, Dior u. a., C-300/98 und C-392/98, Slg. 2000, I-11307, Randnr. 47, und vom 11. September 2007, Merck Genéricos – Produtos Farmacêuticos, C-431/05, Slg. 2007, I-0000, Randnr. 35), verlangen zwar den effektiven Schutz des geistigen Eigentums und einen gerichtlichen Rechtsschutz, um dieses durchzusetzen; **doch sie enthalten keine Bestimmungen, wonach die oben genannten Richtlinien dahin auszulegen wären, dass die Mitgliedstaaten zwingend die Pflicht zur Weitergabe personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorsehen müssten**.

F. I. 2. Europarecht

cylaw
tu-darmstadt

a) Sicherheitsrecht (staatliche Interessen)

- Richtline 2006/24/EG*,
- Evaluationsbericht zur Richtline über die Vorratsdatenspeicherung (Richtlinie 2004/24/EG),
- European Commission: Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010, (COM) 609 final,
- Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union", Brussels, 14.1.2011,
- Stockholm Programme,
- Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme,
- Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.

* Weitere Hinweise in der „VDS"-Entscheidung des EuGH, Urt. v. 10.02.2009, Rs. C-301/06.

cylaw
tu-darmstadt

b) Urheberrecht (private Interessen)

- Enforcementrecht zum Urheberrecht Richtlinie 2004/48/EG*
- Anhängig (Vorabentscheidungsersuchen des Högsta Domstol (Schweden) vom 20.09.2010, Rs. C-461/10)

* Weitere Hinweise in der „Promusicae“-Entscheidung des EuGH, Urt. v. 29.01.2008, Rs. C- 275/06.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

F. I. 3. Deutsches Recht

cylaw
tu-darmstadt

a) Sicherheitsrecht (staatliche Interessen)

§ 15 a Abs. 2 HSOG Datenerhebung durch Telekommunikationsüberwachung

(2) Unter den Voraussetzungen des Abs. 1 können die Polizeibehörden auch Auskunft über Verkehrsdaten nach § 96 Abs. 1, § 113a des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Gesetz vom 29. April 2009 (BGBl. I S. 994), in einem zurückliegenden oder einem zukünftigen Zeitraum sowie über Inhalte verlangen, die innerhalb des Telekommunikationsnetzes in Speichereinrichtungen abgelegt sind. Erfolgt die Erhebung von Verkehrsdaten nicht beim Telekommunikationsdiensteanbieter, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

F. I. 3. Deutsches Recht

cylaw
tu-darmstadt

a) Sicherheitsrecht (staatliche Interessen)

§ 113b TKG alte Fassung „Verwendung der nach § 113a gespeicherten Daten“

Der nach § 113a Verpflichtete darf die allein auf Grund der Speicherungsverpflichtung nach § 113a gespeicherten Daten

1. zur Verfolgung von Straftaten,

2. zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder

3. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes

an die zuständigen Stellen auf deren Verlangen übermitteln, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist; für andere Zwecke mit Ausnahme einer Auskunftserteilung nach § 113 darf er die Daten nicht verwenden. § 113 Abs. 1 Satz 4 gilt entsprechend.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

F. I. 3. Deutsches Recht

cylaw
tu-darmstadt

a) Sicherheitsrecht (staatliche Interessen)

§ 20 m BKAG Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten

(1) […]

(2) Unter den Voraussetzungen des Absatzes 1 Satz 1 kann das Bundeskriminalamt von denjenigen, die geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln, Auskunft über Nutzungsdaten (§ 15 Abs. 1 des Telemediengesetzes) verlangen. Die Auskunft kann auch über zukünftige Nutzungsdaten angeordnet werden. Die Daten sind unverzüglich sowie auf dem vom Bundeskriminalamt bestimmten Weg durch den Diensteanbieter zu übermitteln.

(3) […]

F. I. 3. Deutsches Recht

cylaw
tu-darmstadt

a) Sicherheitsrecht (staatliche Interessen)

§ 100g StPO Auskunft über Telekommunikationsverbindungen

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer

1. eine Straftat von auch im Einzelfall **erheblicher Bedeutung**, insbesondere **eine in § 100a Abs. 2 bezeichnete Straftat**, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder

2. eine Straftat **mittels Telekommunikation** begangen hat, so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (**§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes**) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.

(2) […]

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

F. I. 3. Deutsches Recht

cylaw
tu-darmstadt

b) Urheberrecht (private Interessen)

§ 101 UrhG Anspruch auf Auskunft

(1) Wer in gewerblichem Ausmaß das Urheberrecht oder ein anderes nach diesem Gesetz geschütztes Recht widerrechtlich verletzt, kann von dem Verletzten auf unverzügliche Auskunft über die Herkunft und den Vertriebsweg der rechtsverletzenden Vervielfältigungsstücke oder sonstigen Erzeugnisse in Anspruch genommen werden. […]

(2) In Fällen offensichtlicher Rechtsverletzung oder in Fällen, in denen der Verletzte gegen den Verletzer Klage erhoben hat, besteht der Anspruch unbeschadet von Absatz 1 auch gegen eine Person, die in gewerblichem Ausmaß

1. rechtsverletzende Vervielfältigungsstücke in ihrem Besitz hatte,
2. rechtsverletzende Dienstleistungen in Anspruch nahm,
3. für rechtsverletzende Tätigkeiten genutzte Dienstleistungen erbrachte oder
4. nach den Angaben einer in Nummer 1, 2 oder Nummer 3 genannten Person an der Herstellung, Erzeugung oder am Vertrieb solcher Vervielfältigungsstücke, sonstigen Erzeugnisse oder Dienstleistungen beteiligt war,

[…]

(9) Kann die Auskunft nur unter Verwendung von Verkehrsdaten (§ 3 Nr. 30 des Telekommunikationsgesetzes) erteilt werden, ist für ihre Erteilung eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der Verkehrsdaten erforderlich, die von dem Verletzten zu beantragen ist. […]

F. II. Identitätsvorbehalt nach deutschem Verfassungsrecht in der Rechtsprechung des BVerfG

cylaw
tu-darmstadt

1. Lissabon-Entscheidung:

<240> [...] **Darüber hinaus prüft das Bundesverfassungsgericht, ob der unantastbare Kerngehalt der Verfassungsidentität des Grundgesetzes nach Art. 23 Abs. 1 Satz 3 in Verbindung mit Art. 79 Abs. 3 GG gewahrt ist** (vgl. BVerfGE 113, 273 <296>). Die Ausübung dieser verfassungsrechtlich radizierten Prüfungskompetenz folgt dem Grundsatz der Europarechtsfreundlichkeit des Grundgesetzes, […]. Insoweit gehen die verfassungs- und die unionsrechtliche Gewährleistung der nationalen Verfassungsidentität im europäischen Rechtsraum Hand in Hand. Die Identitätskontrolle ermöglicht die Prüfung, ob infolge des Handelns europäischer Organe die in Art. 79 Abs. 3 GG für unantastbar erklärten Grundsätze der Art. 1 und Art. 20 GG verletzt werden. Damit wird sichergestellt, dass der Anwendungsvorrang des Unionsrechts nur kraft und im Rahmen der fortbestehenden verfassungsrechtlichen Ermächtigung gilt.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

F. II. Identitätsvorbehalt nach deutschem Verfassungsrecht in der Rechtsprechung des BVerfG

cylaw
tu-darmstadt

2. Welche „rationes“ gehören zum „unantastbaren Kerngehalt der Verfassungsidentität des Grundgesetzes“?

BVerfG „VDS“:

<218> […] **Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert** werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland (vgl. zum grundgesetzlichen Identitätsvorbehalt BVerfG, Urteil des Zweiten Senats vom 30. Juni 2009 - 2 BvE 2/08 u.a. -, juris, Rn. 240), **für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss. Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.**

→ jedenfalls die **„Antiprofilierungsratio“**

→ vielleicht auch die **„Kombinationsratio“**

G. „Eckpfeiler?“
I. Konflikt der „Kombinationsratio“ des BVerfG mit der „Trennungsratio“ des EuGH in seiner „VDS (1)“-Entscheidung

cylaw tu-darmstadt

1. „Trennungsratio“:

a) EuGH „VDS (1)“: Keine Kompetenz der EG wenn Datennutzung mitgeregelt wird

Art. 95 EG alte Fassung (nunmehr Art. 114 AEU)
(1)Soweit in diesem Vertrag nichts anderes bestimmt ist, gilt abweichend von Artikel 94 für die Verwirklichung der Ziele des Artikels 14 die nachstehende Regelung. Der Rat erläßt gemäß dem Verfahren des Artikels 251 und nach Anhörung des Wirtschafts- und Sozialausschusses die Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben.
(2) […]

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

G. „Eckpfeiler?“
I. Konflikt der „Kombinationsratio“ des BVerfG mit der „Trennungsratio“ des EuGH in seiner „VDS“- Entscheidung

cylaw tu-darmstadt

b) Ril 2006/24/EG überlässt Regelung des Zugangs den Mitgliedstaaten

Erwägungsgründe zur Ril 2006/24/EG

(25) **Diese Richtlinie berührt nicht das Recht der Mitgliedstaaten, Rechtsvorschriften über den Zugang zu und die Nutzung von Daten durch von ihnen benannte nationale Behörden zu erlassen**. Fragen des Zugangs zu Daten, die gemäß dieser Richtlinie von nationalen Behörden für solche Tätigkeiten auf Vorrat gespeichert werden, die in Artikel 3 Absatz 2 erster Gedankenstrich der Richtlinie 95/46/EG aufgeführt sind, fallen nicht in den Anwendungsbereich des Gemeinschaftsrechts. Sie können aber durch nationales Recht oder Maßnahmen nach Titel VI des Vertrags über die Europäische Union geregelt werden. Derartige Rechtsvorschriften oder Maßnahmen müssen die Grundrechte, wie sie sich aus den gemeinsamen Verfassungstraditionen der Mitgliedstaaten ergeben und durch die EMRK gewährleistet sind, in vollem Umfang wahren. Nach Artikel 8 der EMRK in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte müssen Eingriffe von Behörden in das Recht auf Privatsphäre den Anforderungen der Notwendigkeit und Verhältnismäßigkeit genügen und deshalb festgelegten, eindeutigen und rechtmäßigen Zwecken dienen, wobei sie in einer Weise erfolgen müssen, die dem Zweck des Eingriffs entspricht, dafür erheblich ist und nicht darüber hinausgeht.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

G. „Eckpfeiler?“
I. Konflikt der „Kombinationsratio“ des BVerfG mit der „Trennungsratio“ des EuGH in der „VDS (1)“- Entscheidung

cylaw
tu-darmstadt

b) Ril 2006/24/EG überlässt Regelung des Zugangs den Mitgliedstaaten

Ril 2006/24/EG - Artikel 4
Zugang zu Daten
Die Mitgliedstaaten erlassen Maßnahmen, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden. Jeder Mitgliedstaat legt in seinem innerstaatlichen Recht unter Berücksichtigung der einschlägigen Bestimmungen des Rechts der Europäischen Union oder des Völkerrechts, insbesondere der EMRK in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte, das Verfahren und die Bedingungen fest, die für den Zugang zu auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.

G. „Eckpfeiler?“
I. Konflikt der „Kombinationsratio“ des BVerfG mit der „Trennungsratio“ des EuGH in seiner „VDS (1)“-Entscheidung

cylaw tu-darmstadt

2. EuGH „VDS (1)“ und BVerfG „VDS“ im Wortlaut

BVerfG „VDS“:

<266> Demgegenüber ist es unzulässig, **unabhängig von solchen Zweckbestimmungen einen Datenpool auf Vorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt.**

EuGH „VDS (1)“:

<83> Die Richtlinie 2006/24 regelt somit Tätigkeiten, die unabhängig von der Durchführung jeder eventuellen Maßnahme polizeilicher oder justizieller Zusammenarbeit in Strafsachen sind. **Sie harmonisiert weder die Frage des Zugangs zu den Daten durch die zuständigen nationalen Strafverfolgungsbehörden noch die Frage der Verwendung und des Austauschs dieser Daten zwischen diesen Behörden**. Diese Fragen, die grundsätzlich in den von Titel VI des EU-Vertrags erfassten Bereich fallen, **werden von den Bestimmungen** dieser Richtlinie **nicht erfasst**, wie insbesondere in ihrem 25. Erwägungsgrund und in ihrem Art. 4 ausgeführt wird.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

G. II. Vorläufiges Fazit zur Rechtslage vor dem 01.12.2009 im Hinblick auf den EG-Vertrag

cylaw
tu-darmstadt

- **Widerspruch der Trennungsratio des EuGH zu der Kombinationsratio des BVerfG.**
- **Widerspruch der Kombinationsratio des BVerfG zu der Trennungsratio des EuGH.**

BVerfG „VDS“:
<218> […] **für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss. Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.**

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

G. III. Caveat: Ist eine „Trennungsratio“ des EuGH mit dem Vertrag von Lissabon Rechtsgeschichte?

cylaw
tu-darmstadt

Artikel 82 Abs. 1 AEU

(1) Die justizielle Zusammenarbeit in Strafsachen in der Union beruht auf dem Grundsatz der gegenseitigen Anerkennung gerichtlicher Urteile und Entscheidungen und umfasst die Angleichung der Rechtsvorschriften der Mitgliedstaaten in den in Absatz 2 und in Artikel 83 genannten Bereichen.

Das Europäische Parlament und der Rat **erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Maßnahmen,** um

a) Regeln und Verfahren festzulegen, mit denen die Anerkennung aller Arten von Urteilen und gerichtlichen Entscheidungen in der gesamten Union sichergestellt wird;

b) Kompetenzkonflikte zwischen den Mitgliedstaaten zu verhindern und beizulegen;

c) die Weiterbildung von Richtern und Staatsanwälten sowie Justizbediensteten zu fördern;

d) **die Zusammenarbeit zwischen den Justizbehörden oder entsprechenden Behörden der Mitgliedstaaten im Rahmen der Strafverfolgung sowie des Vollzugs und der Vollstreckung von Entscheidungen zu erleichtern.**

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

G. III. Caveat: Ist eine „Trennungsratio“ des EuGH mit dem Vertrag von Lissabon Rechtsgeschichte?

cylaw
tu-darmstadt

Artikel 82 Abs. 2 AEU

(2) **Soweit dies zur Erleichterung der gegenseitigen Anerkennung gerichtlicher Urteile und Entscheidungen und der polizeilichen und justiziellen Zusammenarbeit in Strafsachen mit grenzüberschreitender Dimension erforderlich ist, können das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren durch Richtlinien Mindestvorschriften festlegen.** Bei diesen Mindestvorschriften werden die Unterschiede zwischen den Rechtsordnungen und -traditionen der Mitgliedstaaten berücksichtigt.

Die Vorschriften betreffen Folgendes:

a) die Zulässigkeit von Beweismitteln auf gegenseitiger Basis zwischen den Mitgliedstaaten;

b) die Rechte des Einzelnen im Strafverfahren;

c) die Rechte der Opfer von Straftaten;

d) sonstige spezifische Aspekte des Strafverfahrens, die zuvor vom Rat durch Beschluss bestimmt worden sind; dieser Beschluss wird vom Rat einstimmig nach Zustimmung des Europäischen Parlaments erlassen. Der Erlass von Mindestvorschriften nach diesem Absatz hindert die Mitgliedstaaten nicht daran, ein höheres Schutzniveau für den Einzelnen beizubehalten oder einzuführen.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

G. III. Caveat: Ist eine „Trennungsratio“ des EuGH mit dem Vertrag von Lissabon Rechtsgeschichte?

cylaw
tu-darmstadt

Artikel 87 Abs. 1, 2 AEU

(1) Die Union entwickelt eine polizeiliche Zusammenarbeit zwischen allen zuständigen Behörden der Mitgliedstaaten, einschließlich der Polizei, des Zolls und anderer auf die Verhütung oder die Aufdeckung von Straftaten sowie entsprechende Ermittlungen spezialisierter Strafverfolgungsbehörden.

(2) Für die Zwecke des Absatzes 1 können **das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren Maßnahmen erlassen**, die Folgendes betreffen:

a) Einholen, Speichern, Verarbeiten, Analysieren und Austauschen sachdienlicher Informationen;

b) Unterstützung bei der Aus- und Weiterbildung von Personal sowie Zusammenarbeit in Bezug auf den Austausch von Personal, die Ausrüstungsgegenstände und die kriminaltechnische Forschung;

c) gemeinsame Ermittlungstechniken zur Aufdeckung schwerwiegender Formen der organisierten Kriminalität.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA Sicherheit im öffentlichen Raum

cylaw
tu-darmstadt

Für die Diskussion: Ihre Kritik ist Input für mich

Prof. Dr. Viola Schmid, LL.M. (Harvard)
schmid@jus.tu-darmstadt.de

Technische Universität Darmstadt
Fachgebiet Öffentliches Recht
S1|03 306
Hochschulstr. 1
64289 Darmstadt
Tel.: +49 6151 16-6464
Fax: +49 6151 16-3984

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SIRA
Sicherheit im öffentlichen Raum