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

Informations- und Datenschutzrecht I

Modul 1

DATUM	MODUL	TITEL
25.10.2005	1	**Strategie und Grundlagen der Vorlesung**

A. Strategie der Vorlesung

Ziel der Vorlesung ist die Vorstellung der Strukturen des Cyberlaw. Cyberlaw ist ein Ober begriff für das Recht, das den Cyberspace so „organisiert", dass er zu einer lebenswerten „Cyberworld" wird. Cyberlaw ist multidisziplinär und ist sowohl im Zivil- als auch im Straf- und Öffentlichen Recht verankert. Darüber hinaus ist das Cyberlaw (inter-)national und verlangt deswegen neben der Kenntnis der deutschen Normen- und Gerichtshierarchie auch völker- und europarechtliche Kenntnisse. Die Vorlesung kann nur einen kleinen Ausschnitt dieses Rechtsgebiets vorstellen. Strategie ist es deswegen, mit eklektischem „Mut zur Lücke" anhand weniger Einzelfälle (etwa Rasterfahndung) in die juristische Methode und Argumentation einzuführen. Vorlesungsbegleitend wird eine Übung angeboten, in der anhand von Fallbeispielen (aus der Praxis) der in der Vorlesung behandelte Stoff vertieft und in Vorbereitung auf die Vorlesungsklausur eingeübt werden soll.

I. Internet Sprechstunde ?

Fragen und Kritik können an Frau Prof. Schmid persönlich unter info@Prof-Schmid.de gerichtet werden. E-Mails bitte nur unter Angabe der Vorlesung.

II. Literatur

Die Lehrbücher und Kommentare werden in der juristischen Teilbibliothek in einem Regal nahe dem Eingang zusammengestellt. Verwendet werden sollte jeweils die aktuellste Fassung, da das Cyberlaw ein Rechtsgebiet „im Entstehen" ist und deswegen vielen Veränderungen unterworfen wird.

1 Lehrbücher

- Boehme-Neßler, Volker, Cyberlaw, 2001
- Gola, Peter/ Klug, Christoph, Grundzüge des Datenschutzrechts, 2003
- Hoeren, Thomas, Internetrecht, 2005 (kostenloser Download unter: http://www.uni-muenster.de/Jura.itm/hoeren/)
- Holznagel, Bernd, Grundzüge des Telekommunikationsrecht, 2001 (Neuauflage angekündigt für Oktober 2004)
- Kloepfer, Michael, Informationsrecht, 2002
- Koehler, Markus/Arndt, Hans-Wolfgang, Recht des Internets, 4. Aufl., 2003
- Roßnagel, Alexander Handbuch Datenschutzrecht, 2002
- Schaar, Peter, Datenschutz im Internet, 2002

- Tinnefeld, Marie-Therese, Einführung in das Datenschutzrecht, 4. Aufl. 2004

2 Kommentare

- Roßnagel, Alexander, Recht der Multimediadienste, Loseblattsammlung
- Simitis, Spiros, Kommentar zum Bundesdatenschutzgesetz, 2003
- Schaffland, Hans-Jürgen/Wiltfang, Noeme, Bundesdatenschutzgesetz Kommentar, Loseblattsammlung

3 Gesetzestexte

Obligatorisch: TUD-Cyberlaw Gesetzestext, zu beziehen über das Fachgebiet Öffentliches Recht

- Telemediarecht: TeleMediaR, Beck-Texte, 2005
- Sodan, Helge, Öffentliches, Privates und Europäisches Wirtschaftsrecht, 7. Aufl., 2004

4 Zeitschriften

- CR, Computer und Recht (CRi, Computer und Recht international)
- DuD, Datenschutz und Datensicherheit
- ITRB, IT-Rechtsberater
- K&R, Kommunikation und Recht
- MMR, Multimedia und Recht
- TKMR, Zeitschrift für Telekommunikations- und Medienrecht

III. Rechtsquellen

1 Virtuell

a) Normen

- Europarecht: http://www.europa.eu.int/eur-lex/de/index.html
- Seiten der Bundesministerien und Seite der Bundesregierung http://www.bundesregierung.de/Gesetze/-,7214/Gesetze-A-Z.htm
- Hessenrecht: http://www.hessenrecht.hessen.de/gvbl/start.htm

b) Rechtsprechung

- EuGH: http://curia.eu.int/de/content/juris/index.htm
- BVerfG: http://www.bverfg.de/

- BGH: http://www.bundesgerichtshof.de/

c) Mailinglist

Das ITM (Institut für Informations- Telekommunikation- und Medienrecht) der Universität Münster bietet eine Auswahl juristisch–technischer Mailinglisten an (http://www.uni-muenster.de/Jura.itm/hoeren/material/Mailinglisten.htm).

2 Realworld: Normen

- Bundesgesetzblatt (Teilbibliothek)
- Hessisches Gesetzblatt (Teilbibliothek)
- Amtsblatt der Europäischen Union (Teilbibliothek)

IV. Zitieretikette

Grundsätzlich gilt für das Zitieren von Gesetzen:

Art. (oder §) Abs. 1 S. 1 [gegebenenfalls: HS. (Halbsatz), Nr. und Lit.] Abkürzung des Gesetzestexts (etwa GG). Bsp.: § 10 Abs. 2 S. 1 Nr. 5 Lit. a MDStV II oder § 10 Abs. 1 Nr. 1 MDStV II (Beachte: Der Satz wird nur erwähnt, wenn der Absatz mehr als einen Satz enthält. Gleiches gilt für das Verhältnis, Absatz zu Artikel/§).

V. Konzept der „Flexible, sensible and sensitive Solution“

Die Inhalte der Vorlesungen können aktuellen Gegebenheiten und/oder den Fortschritten der Studenten angepasst werden.

B. Begriff: Was ist Cyberlaw?

I. Definition Cyberlaw

Das Cyberlaw ist eine Querschnittsmaterie aus Zivil-, Straf- und Öffentlichem Recht.

Cyberlaw in einer öffentlich-rechtlichen Betrachtung ist ein Oberbegriff für Medien-, Telekommunikations-, Computer-, Internet-, Informations-, Datensicherheits- und Datenschutzrechte, die sich mit den Themen des Cyberspace und der Cyberworld befassen.

II. Abgrenzung zu zivil- und strafrechtlichen Betrachtungen

1 Zivil- und Öffentliches Recht

Das Zivilrecht regelt die Rechtsbeziehungen zwischen Privatpersonen oder juristischen Personen. Demgegenüber handelt es sich um Öffentliches Recht, wenn es um rechtliche Beziehungen zum Staat geht. Die Abgrenzung zwischen Zivil- und Öffentlichem Recht ist in den einfachen Fällen einfach und in den schwierigen Fällen nur mit einer Entscheidung des Gesetzgebers und/oder der Rechtswissenschaft bzw. der Rechtsanwender „lösbar“:

- Beispiel für einen einfachen Fall („clear case“):

  B ersteigert bei Ebay von S eine Digitalkamera: Da B und S Privatpersonen sind, ist ihre Rechtsbziehung zivilrechtlich. Durch den geschlossenen Kaufvertrag ist B verpflichtet, dem Kaufpreis zu zahlen, und S ist verpflichtet, B das Eigentum an der Digitalkamera zu übertragen.

Das Zivilrecht regelt also etwa die Vertragsbeziehungen Privater (B und S) im Cyberspace. Schwieriger („hard case“) ist die Einordnung folgenden

- Beispiels:

  Die Polizeibehörden in Hamburg, Bremen, Schleswig-Holstein, Mecklenburg-Vorpommern, Bayern, ... beschließen, dass alle Polizeibeamten mit Digitalkameras zur Beweissicherung vor Ort ausgestattet werden sollen. Damit Sie einen preiswerten Anbieter finden, machen Sie im Internet eine gebündelte Ausschreibung. Um der Jugendkriminalität, die auch auf fehlende Ausbildungschancen zurückzuführen ist, vorzubeugen, wird ein soziales Leistungskriterium in die Vergabebedingungen eingeführt. Derjenige Anbieter soll den Zuschlag bekommen, der mehr Ausbildungsplätze zur Verfügung stellt. Der Digitalkamerahersteller D 1 bekommt den Zuschlag unter anderem deshalb. D 2, der im Vergabeverfahren unterlegene Konkurrent, fühlt sich benachteiligt. Sind Beschaffungsgeschäfte (Kameras) von Behörden öffentlich-rechtlich oder zivilrechtlich zu beurteilen? Welche Rechtsnatur hat das Vergaberecht (wenn Behörden Auftraggeber sind)?[1] Verändert die Einführung sozialer Vergabekriterien, die der Verbesserung öffentlicher Sicherheit dienen sollen, die Zuordnung zum Zivil- oder Öffentlichen Recht?

Neben diesen Beispielen, bei denen die Zuordnung eines Sachverhalts zum Zivilrecht die Zuordnung zum Öffentlichen Recht ausschließt (und umgekehrt), gibt es auch ein Verhältnis der Komplementarität der Rechtsordnungen zueinander. So ist das Öffentliche Recht für die Infrastruktur privater Rechtsbeziehungen „zuständig“. Ein Beispiel ist das Signaturrecht, das Öf-

[1] Der Gesetzgeber hat sich für eine Zuordnung zum Kartellrecht (§ 97 (Abs. 4) GWB) entschieden.

fentliches Recht ist, und auch den E-Commerce – und nicht „nur“ das E-Government - fördern soll.

TESTFRAGE: Wozu braucht man die Unterscheidung von Zivil- und Öffentlichem Recht?

2 Straf- und Öffentliches Recht

Einfacher als die Unterscheidung zwischen Zivil- und Öffentlichem Recht ist die Unterscheidung zwischen Öffentlichem Recht und Strafrecht. Typisch sind nämlich die Sanktionen, die das Straf- und Ordnungswidrigkeitenrecht verhängen: Freiheits- und Geldstrafen, Einziehung und Geldbußen. Charakteristisch für das Strafrecht ist seine Ex-Post-Betrachtung: erst nachdem eine die Rechtsgüter gefährdende oder verletzende Handlung begangen oder eine die Rechtsgüter bewahrende Handlung unterlassen wurde, bestraft das Strafgericht den Täter. Das öffentliche Recht kennt demgegenüber nicht nur repressive, sondern auch präventive Instrumente wie ein Verbot mit Erlaubnisvorbehalt.

- Zulassung der Veranstaltung von Rundfunk

§ 20 Abs. 1 Rundfunkstaatsvertrag [Zulassung]

(1) Private Veranstalter bedürfen zur Veranstaltung von Rundfunk einer Zulassung nach Landesrecht. (…)

Rechtstechnisch stellt die Zulassungspflicht ein präventives Verbot mit Erlaubnisvorbehalt dar. D.h. bei Vorliegen der gesetzlichen Voraussetzungen ist eine Zulassung zu erteilen.

Das Strafrecht sanktioniert nicht nur Verbrechen und Vergehen in der Realworld, sondern auch Vergehen und Verbrechen, die durch den oder im Cyberspace begangen werden. Das Nebeneinander von Realworld/strafrechtlichem Traditional Law und zwischen Cyberworld/strafrechtlichem Cyberlaw kennt zwei Konstellationen.

a) "Umgehungsszenario"

Grundsätzlich sollen "Inhalte", die eine Rechtsordnung nicht toleriert, nicht deshalb verbreitet werden dürfen, weil die Technik des Cyberspace dies ermöglicht.

§ 11 Abs. 3 StGB

Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen in denjenigen Vorschriften gleich, die auf diesen Absatz verweisen.

In einer puristisch-rechtlichen Betrachtung ist es deshalb einleuchtend, dass etwa die volksverhetzende "Auschwitzlüge" (§ 130 StGB) oder unzulässige (kinder-)pornographische Inhalte (§ 184 StGB) nicht mit der Technik des Cyberspace verbreitet werden dürfen. Wie schwie-

rig die Durchsetzung solcher rechtlichen Regelungs- und Steuerungsintentionen ist, wird in einem weiteren Modul der Vorlesung aufgezeigt werden. Es wird ebenfalls zu diskutieren sein, welche Veränderungen der rechtlichen Methodik (Rechtsrealismus) und der verfassungsrechtliche Beurteilung zu Steuerungsverlusten führen können.

b) Spezifisches strafrechtliches Cyberlaw

Der Cyberspace und die Potenzierung der Datenorganisationskompetenz birgt neue, spezifische Risiken für die Datenschutzrechte der Grundrechtsträger. So gab es Werksspionage und Geheimnisverrat auch früher: die Schnelligkeit und Verfügbarkeit technischer Tools zur Datenorganisation führt zu einer neuen Qualität der Rechtsgutsgefährdung. Ausdruck dieser Gefährdungen wie ihrer Sanktionierung sind Delikte wie das Ausspähen von Daten (§ 202a StGB), der Computerbetrug (§ 263a StGB), die Datenveränderung (§ 303a StGB) und die Computersabotage (§ 303b StGB). Diese Beispiele belegen die Ambivalenzthese, die im Laufe der Vorlesung weiter exemplifiziert werden wird.

3 Veränderung der traditionellen Einteilung der Rechtsdisziplinen durch das Völker- und Europarecht

Wenn bereits für das deutsche Rechtssystem seit Jahrzehnten vor allem um die Abgrenzung von Zivil- zu Öffentlichem Recht in den "hard cases" gerungen wurde, so erfolgt im Rahmen der Europäisierung des deutschen Rechts ein weiterer Perspektivenwechsel: Der europäische Gesetzgeber ist an der Förderung des Binnenmarkts

Art. 14 Abs. 2 EG [Binnenmarkt]

Der Binnenmarkt umfasst einen Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gemäß den Bestimmungen dieses Vertrages gewährleistet ist.

und der Verfolgung von Aufgaben "interessiert".

Art 2 EG [Gemeinschaftsaufgabe]

Aufgabe der Gemeinschaft ist es, durch die Errichtung eines Gemeinsamen Marktes und einer Wirtschafts- und Währungsunion sowie durch die Durchführung der in den Artikeln 3 und 4 genannten gemeinsamen Politiken und Maßnahmen in der ganzen Gemeinschaft eine harmonische, ausgewogene und nachhaltige Entwicklung des Wirtschaftslebens, ein hohes Beschäftigungsniveau und ein hohes Maß an sozialem Schutz, die Gleichstellung von Männern und Frauen, ein beständiges, nichtinflationäres Wachstum, einen hohen Grad von Wettbewerbsfähigkeit und Konvergenz der Wirtschaftsleistungen, ein hohes Maß an Umweltschutz und Verbesserung der Umweltqualität, die Hebung der Lebenshaltung und der Lebensqualität, den wirtschaftlichen und sozialen Zusammenhalt und die Solidarität zwischen den Mitgliedstaaten zu fördern.

Ob diese Ziele in den einzelnen Mitgliedstaaten durch den Erlass von Öffentlichem oder Zivilrecht verfolgt werden, interessiert das Europarecht erst dann, wenn dies nicht effektiv erfolgt. Das Europarecht verlangt nach der Rechtsprechung des Europäischen Gerichtshofs grundsätzlich, dass der "effet utile" erreicht wird.
Die Vorlesung hat sich für einen pragmatischen Ansatz entschieden - sie konzentriert sich auf den öffentlich-rechtlichen Bereich und erweitert dort, wo aktuelle Tendenzen oder schwerwiegende Rechtsgutsgefährdungen dies nahe legen, die Perspektive etwa in das Strafrecht. Aus dem Strafrecht wird deshalb die völkerrechtliche Convention on Cybercrime (CCC) des Europarates vorgestellt behandelt werden, die ein internationales Vorgehen gegen die Online-Kriminalität zum Gegenstand hat.

III. Informations- und Datenschutzrecht

Im Rahmen der Vorlesung erfolgt eine Konzentration auf einen Teilbereich des Cyberlaw, nämlich das Informations- und Datenschutzrecht (IuD).
Das Informations- und Datenschutzrecht kann als Recht zu, auf und an der Information bezeichnet werden. Nicht nur die Rechte auf Information (etwa Akteneinsichtsrechte oder Ansprüche nach dem Informationsfreiheitsgesetz, die in späteren Modulen vorgestellt werden), sondern auch das Recht an der Information (Datenschutz; Schutz von Betriebs- und Geschäftsgeheimnissen) reflektieren die Interessen der "Akteure" auf dem Informationsmarkt und an dem Produkt "Information". Konsequenterweise müsste die Bezeichnung dieses Rechtsgebiets "Informations(schutz)recht" lauten. Gebräuchlich ist für den Schutz von Rechten an der Information die Bezeichnung "Datenschutzrecht" - ohne dass freilich überzeugend erklärt wird, inwieweit sich der Begriff des "Datums" von dem der "Information" unterscheidet. Jedenfalls bringt die Verknüpfung beider Begriffe mit dem „und" die Multipolarität dieser Informationswelt zum Ausdruck.
Das Informations- und Datenschutzrecht enthält Aussagen über den Informationstransport (Telekommunikationsrecht), den -zugang (Informationsfreiheitsgesetze), die -verweigerung (Geheimnisrecht), die –überflutung (Spam), den -inhalt (Medienrecht) und über die Eigentums- und Nutzungsrechte (Datenschutz, Urheberrecht). Das Recht auf die Information wird durch das Recht an der Information beschränkt. Damit dieses Recht an der Information (etwa das Recht auf Datenschutz; auf Schutz von Geschäfts- und Betriebsgeheimnissen und auf Schutz für das Werk des Urhebers) effektiv geschützt werden kann, bedarf es einer bestimmten Qualität der Organisation von Daten. Unter "**Organisation"** von Daten werden hier verschiedene Prozesse verstanden:

<table>
<tr><td colspan="3">TUD-Terminologie: „Datenorganisation“</td></tr>
<tr><td colspan="3">§ 3 Abs. 2 BDSG: Erhebung, Verarbeitung oder Nutzung</td></tr>
<tr><td>Erhebung
§ 3 Abs. 3 BDSG
➢ Beschaffung</td><td>Verarbeitung
§ 3 Abs. 4 BDSG
➢ Speicherung
➢ Veränderung
➢ Übermittlung
➢ Sperrung
➢ Löschung</td><td>Nutzung
§ 3 Abs. 5 BDSG
➢ Verwendung , soweit nicht Verarbeitung (Auffangtatbestand)</td></tr>
<tr><td colspan="3">von personenbezogenen Daten</td></tr>
</table>

Das Verhältnis von Datensicherheit zu Datenschutz ist akzessorisch - "kein Datenschutz ohne Datensicherheit" Diese Akzessorietät hat auch zur Folge, dass die Datensicherheit als Instrument des Datenschutzes verfassungsrechtlich geschützt ist. Einfachgesetzlich ist die Datensicherheit etwa in § 9 Bundesdatenschutzgesetz (BDSG) (und der Anlage) geschützt.

§ 9 BDSG [Technische und organisatorische Maßnahmen]

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

BDSG Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. (…) (Zutrittskontrolle),
2. (…) Zugangskontrolle),
3. (…) (Zugriffskontrolle),
4. (…) (Weitergabekontrolle),
5. (…) (Eingabekontrolle),
6. (…) (Auftragskontrolle),
7. (…)(Verfügbarkeitskontrolle),

(…)

Weil nicht nur der Begriff der "Information" sondern auch der Begriff und die rechtliche Würdigung des personenbezogenen Datums vieldeutig sind, hat sich vor allem in der technikwissenschaftlichen Praxis der Begriff "IT-Sicherheit" verbreitet. In einer teleologischen Betrachtung lassen sich folgende sechs Kriterien der Daten- bzw. IT-Sicherheit ermitteln, [2] wobei die Terminologie in der Literatur nicht unumstritten ist.[3]

- (1) Identität: Eine Darstellung, die einen autorisierten Benutzer eindeutig identifiziert und der Name des Benutzers oder ein Pseudonym sein kann,
- (2) Authentizität: Die Daten müssen von der angegebenen Quelle stammen und die Identität muss korrekt sein,
- (3) Integrität: die Daten sollen nicht verändert werden können und vollständig sein,
- (4) Vertraulichkeit (TUD-Terminologie: „Intimität"): die Daten, der Datenverarbeitungsvorgang und die -anlagen sollen vor dem Zugriff Unbefugter geschützt werden,
- (5) Verfügbarkeit: der Zugriff auf die Daten soll gewährleistet sein und
- (6) Verbindlichkeit: (als Resultat der Kriterien 1-5).

C. Methode der Fallbearbeitung

Ausgangspunkt der Vorlesung sind verschiedene Szenarien.

I. Fallszenarium

Fall 1: Rasterfahndung nach dem 11. September

Es ist wohl nicht übertrieben, wenn man behauptet: „Der 11. September 2001 hat die Welt verändert." Um den Gefahren zu begegnen, verlangt die Behörde X von einer Universität mit hohem Ausländeranteil Daten über Ausländer arabischer Herkunft. Student Y fühlt sich in seinen Rechten verletzt.

II. Schema (Analyse)

Die Analyse mit Hilfe des folgenden Schemas soll die Verortung der Interessen verdeutlichen. Bei diesem Schema handelt es sich noch nicht um eine rechtliche Falllösung, sondern um eine Methode der Strukturierung des Sachverhalts und der Interessen der "Akteure".

---

[2] Zu den Begriffen vgl. IT-Grundschutzhandbuch, Glossar, BSI 2003; kostenloser Download: http://www.bsi.de/gshb/deutsch/download/index.htm , Common Criteria, Teil 1, Glossar, kostenloser Download: http://www.bsi.de/cc/downcc21.htm.

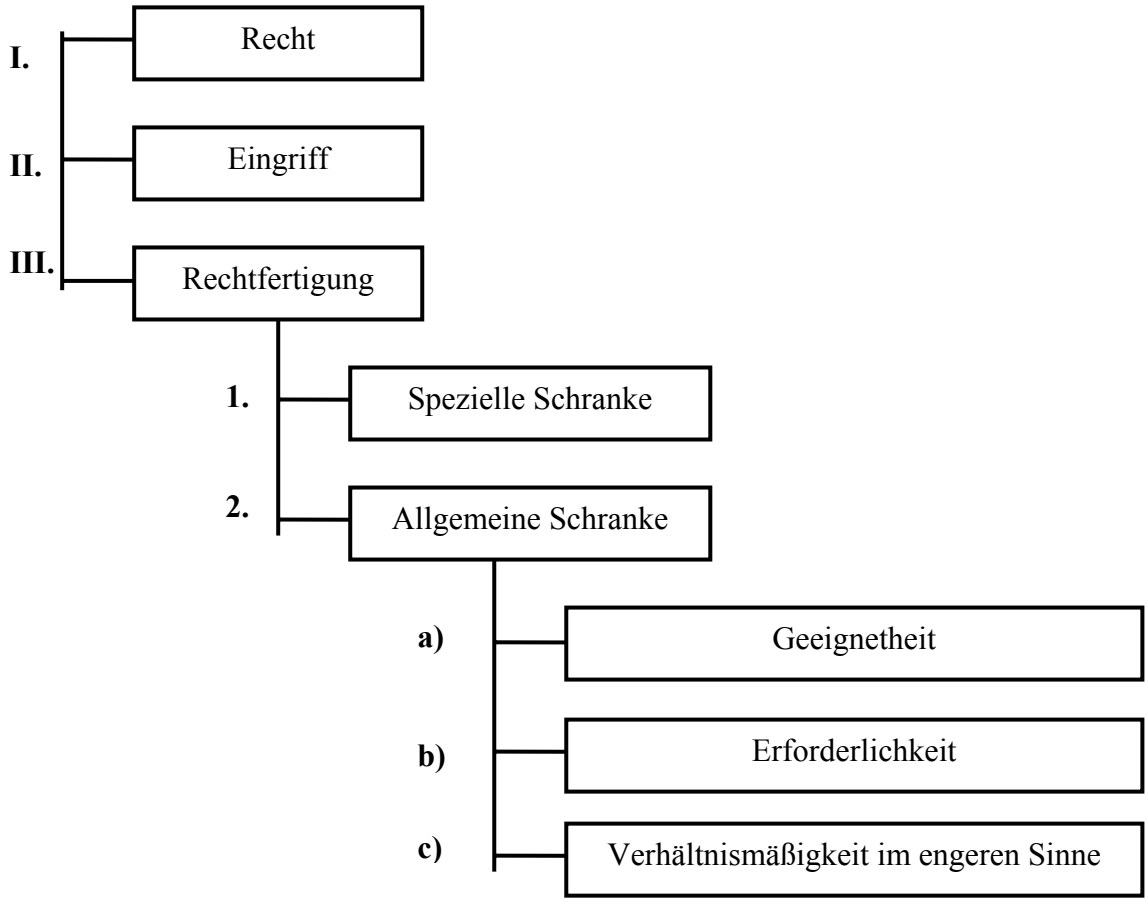
[3] 32. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, 2003, 18.5.2 (S. 152).

		Abkürzung	Analyse
1	**Personal-Aktiv**	**P-Akt**	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an Informationen interessiert ist.
2 a)	**Personal-passiv** Datenschutz	**P-Pas D**	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an der Reservierung und Sicherung von Informationen interessiert ist.
2 b)	**Personal-passiv** Informationskosten	**P-Pas I**	Hierunter fallen die Kosten für die Erhebung, Speicherung, Aufbereitung und Übermittlung von Informationen. Ein Beispiel, das die Rechtsprechung bereits beschäftigt hat, ist § 90 TKG a.F.[4].
3	**Objekt**		Auf Informationen welchen Inhalts soll zugegriffen werden?
4	**Kausal/Zweck**	**KauZ**	Zu welchem Zweck soll auf diese Informationen zugegriffen werden (etwa: Kampf gegen den Terrorismus; Wahrung der Urheberrechte)?
5	**Qualität der Informationstechnik**	**QualInf**	Hierunter sind die unterschiedlichen Formen der "Organisation" von Daten zu verstehen. Beispielhaft wie in § 3 Abs. 3 - 5 BDSG (Erheben, Verarbeiten, Nutzen) aufgezählt.
6	**Verfahren**		Welches Verfahren verlangt das Recht für die Organisation und den Umgang mit diesen Daten (etwa: die Einwilligung des Betroffenen, § 4a BDSG; die Einschaltung eines Gremiums, §§ 14, 15 Artikel 10-Gesetz - G 10)?
7	**Rechtfertigung/ Verhältnismäßigkeit**	**Rfg**	Hier findet die aus dem deutschen Verfassungsrecht bekannte Verhältnismäßigkeitsprüfung statt, die das Interesse von Personal Aktiv (Rechtfertigungsrechtsgut) mit dem Interesse des Personal Passiv Datenschutz (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und dem Interesse des Personal Passiv Informationskosten (Art. 12, 14, 2 Abs. 1 GG) (als Eingriffsrechtsgütern) abwägt.

[4] OVG Münster Beschl. v. 17.05.2002, TKMR 2002, 400. Zur Pflicht zur Führung von Kundendateien in sicherheitsbehördlichem Interesse bei Prepaid-Produkten. Das TKG (Telekommunikationsgesetz) wurde am 26.06.2004 novelliert. Zu weiteren Details siehe Vorlesung Informations- und Datenschutzrecht II (Wintersemester).

III. Prüfungsschema (Falllösung)

Prüfungsschema



Dieses Prüfungsschema wird in der Vorlesung verwendet zur europarechtlichen und verfassungsrechtlichen Grundrechtsprüfung und zur Prüfung der europäischen Grundfreiheiten.

Die "Spezielle Schranke" muss noch definiert werden: sie bezeichnet diejenige Schrankenbestimmung, die unmittelbar in etwa einem Grundrecht genannt wird.

Etwa, in

Art. 5 Abs. 2 GG
Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre.

Im Prüfungspunkt „Verhältnismäßigkeit“ ist im Detail folgendes zu prüfen:

Geeignetheit	Eingriff muss geeignet sein um den Schutz des Rechtsguts, das die Eingriffsrechtfertigung bildet (Rechtfertigungsrechtsgut), zu bewirken – Tauglichkeit des Mittels für den Zweck.

Erforderlichkeit	Es darf keine Maßnahme geben, die für den Schutz des Rechtfertigungsrechtsguts genauso geeignet und weniger eingreifend ist.
Verhältnismäßigkeit im engeren Sinne	Eingriff in das Eingriffsrechtsgut darf nicht außer Verhältnis zum Schutz des Rechtfertigungsrechtsguts stehen – Grundrechtseingriff darf in seiner Intensität nicht außer Verhältnis zum angestrebten Ziel stehen.

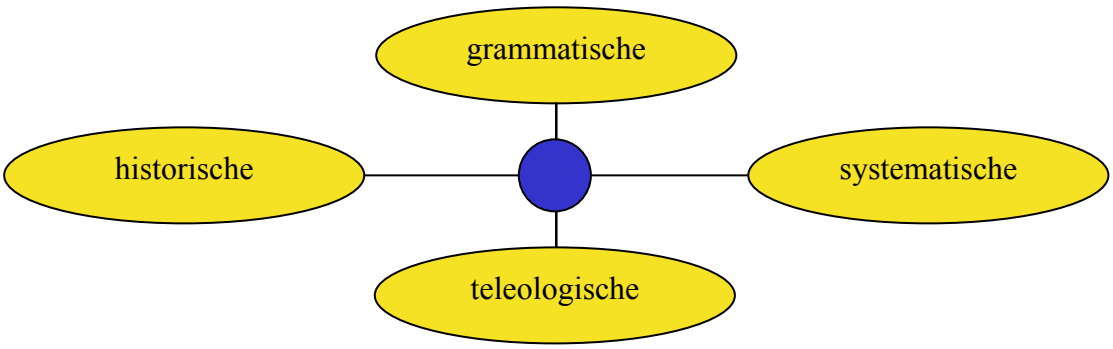
Die Verhältnismäßigkeitsprüfung ist (meist) der zentrale Punkt am Ende einer rechtlichen Fallbearbeitung. Hier zeigt sich regelmäßig die Qualität einer Klausurbearbeitung.

D. Juristische Werkzeuge und „Plattformen“

I. Auslegungsmethoden

Sehr oft müssen Normen (als Oberbegriff etwa von Gesetzen und Rechtsverordnungen) ausgelegt werden. Einer Auslegung bedarf es aufgrund der Mehrdeutigkeit und der Dynamik der Sprache des Normgebers und/oder der Existenz neuer Herausforderungen für das Rechtssystem.

Es gibt für das deutsche Rechtssystem traditionell vier Auslegungsmethoden, die im Rahmen der Vorlesung als „Werkzeuge“ bezeichnet werden.



Die **grammatische Auslegung** sucht nach dem Wortsinn.

Die **historische Auslegung** fragt nach der Motivation und den Erwägungen des (historischen) Gesetzgebers. Für den Erlass des Grundgesetzes wird auf Protokolle des Parlamentarischen Rates zurückgegriffen (Stenographische Protokolle des Parlamentarischen Rates aus dem Jahr 1948/49, Verfassungskonvent auf Herrenchiemsee, 10.-23.08.1948). Die Genese deutscher

Gesetze kann den Aufzeichnungen des Bundestages oder -rates entnommen werden (Bundestags und/oder -rats-Drucksachen).

Die **systematische** Auslegung versucht die auszulegende Norm im systematischen Gesamtzusammenhang des Gesetzes zu verorten.

Die **telelogische** Auslegung fragt nach dem Sinn und Zweck der Vorschrift (ratio legis).

Die **dynamische (technikorientierte)** Auslegung berücksichtigt den technischen Wandel, da der technische Wandel dem „historischen" Gesetzgeber nicht bekannt sein konnte.

Die **rechtsvergleichende / Europarechtliche Auslegung** versucht die Norm im Kontext der (zugrundeliegenden) entsprechenden Europarechtlichen Normen auszulegen.

II. Rechtsordnungen in einer deutschen Betrachtung

Grundsätzlich ist eine Norm eine abstrakt-generelle Regelung, das heißt sie gilt für eine Unbestimmte Vielzahl von Sachverhalten und eine unbestimmte Vielzahl von Adressaten.

Normen gibt es auf unterschiedlichen Ebenen

.Bundesrecht	**Art. 31 GG**[5]	Landesrecht

Verfassung (Grundgesetz)	Landesverfassung
Bundesgesetz	Landesgesetz
Rechtsverordnung	Rechtsverordnung
Satzung	Satzung

Adressierung an den Einzelnen erfolgt durch

⇩

Verwaltungsakt	**Verwaltungsvertrag**

[5] Art. 31 GG: Bundesrecht bricht Landesrecht.

E. Verfassungsrechtlicher Datenschutz: Das Recht auf informationelle Selbstbestimmung

I. Auslegung des Grundgesetzes

grammatische Auslegung:

Ein Grundrecht auf Datenschutz existiert nach einer grammatischen Auslegung des Grundgesetzes nicht. Nach der grammatischen Auslegung gibt es kein Grundrecht auf Datenschutz.

historische Auslegung:

Zum Zeitpunkt des Erlasses des Grundgesetzes gab es auch Datenorganisation – vorwiegend durch Akten. Gerade durch die Automatisierung und Elektronisierung der Datenorganisation (Komplexität, Qualität und Quantität änderte sich) stellte sich die Frage nach dem Recht des Einzelnen, über seine Daten zu verfügen.

Nach der historischen Auslegung (1949 ff) gibt es kein Grundrecht auf Datenschutz.

systematische Auslegung:

Die Gliederung des Grundgesetzes und insbesondere die Bestimmungen über die Grundrechte zwingen nicht zur Annahme einer systematischen Verankerung des Rechts auf Datenschutz.

Nach der systematischen Auslegung gibt es kein Grundrecht auf Datenschutz.

- **teleologische Auslegung:**

Art. 2 Abs. 1 GG
Jeder hat das recht auf die freie Entfaltung seiner Persönlichkeit, soweit…

Sinn und Zeck eines Rechts auf „freie Entfaltung der Persönlichkeit“ ist genau dieses – die Freiheit darüber zu entscheiden, wie, wann, womit, mit wem, wo man Freiheit ausübt. Art. 2 Abs. 1 GG wird deshalb von der Rechtsprechung als „Auffanggrundrecht“ konzipiert – das heißt, es wird dem Staat verwehrt, zu bewerten, welche Ausübung von Freiheit schützenswert ist – oder eben nicht (zusammengefasst: leger formuliert: „Recht auf Unsinn“).[6] Art. 2 Abs. 1 GG konstituiert die so genannte **„allgemeine Handlungsfreiheit“**. Es ist deshalb folgerichtig, wenn das Bundesverfassungsgericht (BVerfG) die Datenorganisation wegen ihrer potentiell entmutigenden Wirkung („risk of chill“) einer grundrechtlichen Prüfung unterwirft

„…wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der

[6] FEX: BVerfGE 80, 137 („Reiten im Walde“).

der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."

„… Freie Entfaltung der Persönlichkeit setzt unter **den modernen Bedingungen der Datenverarbeitung** den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[7]

Deutlich wird, dass das BVerfG eine fünfte Auslegungsmethode für die Verfassung voraussetzt: die dynamische, technikorientierte Auslegung.

- **dynamische (technikorientierte) Auslegung**

Die Auslegung von Verfassungsrecht unterscheidet sich von der Auslegung von „einfachem" Gesetzesrecht, weil

- Verfassungen nicht so oft und leicht geändert werden können wie Gesetze (Art. 79 Abs. 2 GG).

Art. 79 GG

(1) Das Grundgesetz kann nur durch ein Gesetz geändert werden, das den Wortlaut des Grundgesetzes ausdrücklich ändert oder ergänzt. (…)
(2) Ein solches Gesetz bedarf der Zustimmung von zwei Dritteln der Mitglieder des Bundestages und zwei Dritteln der Stimme des Bundesrates.
(…)

- Verfassungen, die die Lebenswirklichkeit rechtlich widerspiegeln sollen, aufgrund der Komplexität des objektiven Geltungsbereichs („Regelungsgegenstand") ohne diese größeren Befugnisse der Interpreten hunderttausende von Artikeln haben müssten;
- Verfassungen grundsätzlich eine längere Lebensdauer als Gesetze haben, und deshalb den veränderten Lebensverhältnissen angepasst werden wollen oder sollen (dynamische Auslegung; FEX: Offene Verfassungsbegriffe; Gesellschaft der Verfassungsinterpreten) um Steuerungskraft zu entwickeln
- speziell im Technikrecht die historische Auslegung versagen muss, und deswegen die dynamischen Auslegung kompensierend die Auslegungsquadriga ergänzt.

[7] BVerfGE 65, 1 (43)

Nach der teleologischen und dynamischen (technikorientierten) Auslegung gibt es ein Grundrecht auf Datenschutz.

II. Entwicklung der Rechtsprechung des Bundesverfassungsgerichts zum Grundrecht auf Datenschutz

Zur statistischen Erfassung von Personen gibt es zwei wesentliche Entscheidungen des Bundesverfassungsgerichts. In der ersten Entscheidung, vom 16.07.1969, „Mikrozensus“[8] lag dem BVerfG ein Gesetz über die Durchführung einer Repräsentativstatistik der Bevölkerung und des Erwerbslebens (Mikrozensus) vor. Das Gericht prüfte die Vereinbarkeit dieses Gesetzes mit den Art. 1 Abs. 1, Art. 2 Abs. 1 GG. Dabei stellte es grundsätzlich fest:

> „Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist.“

Angesichts moderner Strategien des „Data Mining“ und „Data Warehousing“ bedarf diese strikte Aussage einer erneuten Diskussion.

Wegweisend für die juristische Dogmatik war die Konstruktion des Rechts auf Datenschutz: aus zwei Grundrechten, nämlich der allgemeinen Handlungsfreiheit des Art. 2 Abs. 1 GG und der Menschenwürde des Art. 1 Abs. 1 GG.

Art. 1 Abs. 1GG

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Vorbild für diese „Recht auf Datenschutz“ war die Entwicklung eines allgemeinen Persönlichkeitsrechts aus den genannten Artikeln. Konsequenz dieser zweifachen Verankerung ist, dass nicht nur die Schrankentrias des Art. 2 Abs. 1 GG die Daten schützt, sondern auch Art. 1 Abs. 1 S. 2 GG.

FEX: Bereits die Lektüre des Art. 1 Abs. 1 S. 2 GG zeigt, dass sämtliche Auslegungstools zu verwenden sind – und nicht nur die grammatische.

Dieses Recht auf Datenschutz, das in zwei Artikeln verankert ist, trägt seit einem weiteren Urteil die Bezeichnung „Recht auf informationelle Selbstbestimmung“.[9] Gegenstand der sehr berühmten „Volkszählungsentscheidung“ war die Verfassungsmäßigkeit eines Gesetzes, das

[8] BVerfGE 27, 1.
[9] BVerfGE 65, 1.

eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung anordnete. Inhaltlich konturiert das BVerfG ein Recht auf informationelle Selbstbestimmung wie folgt.

Jeder hat ein Recht, zu **wissen**
- wer,
- wann,
- wofür,
- welche personenbezogenen Daten „organisiert“ und muss grundsätzlich
- **einwilligen**.

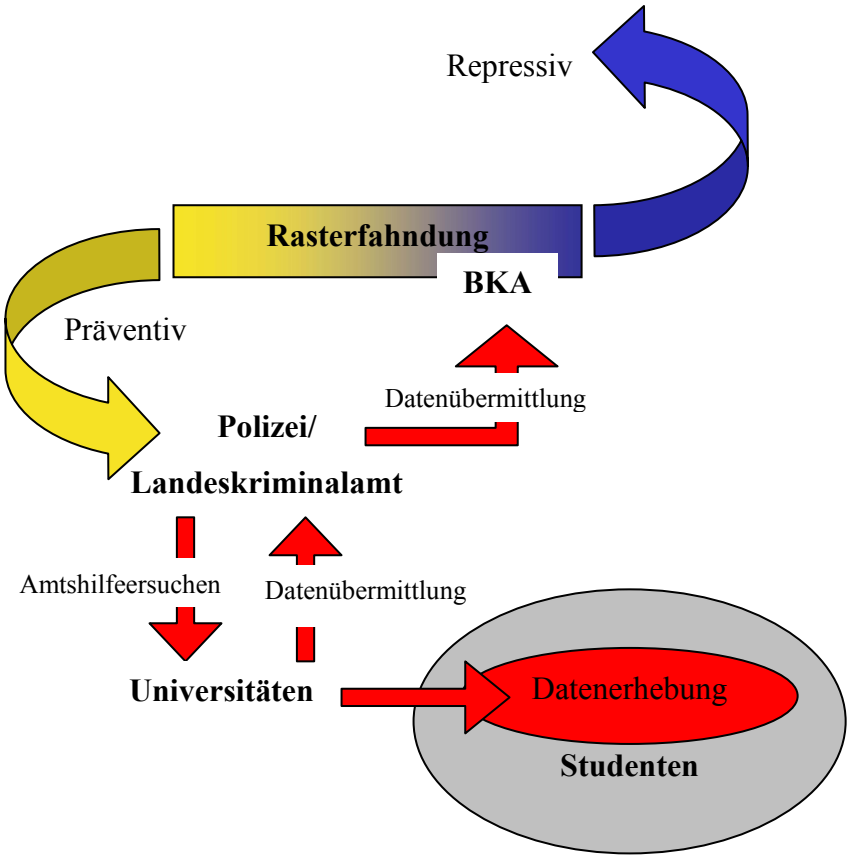
Die Verankerung des verfassungsrechtlichen Datenschutzes im Kontext des allgemeinen Persönlichkeitsrechts hat eine gravierende Folge: nur die Daten natürlicher Personen sind geschützt, da nur sie Anspruch auf Menschenwürde erheben können. (Zum verfassungsrechtlichen Datenschutz für juristische Personen siehe ein späteres Modul).

F. Rasterfahndung Falllösung unter Beschränkung auf P-Pas D

I. Sachverhalt:

Fall 1: Rasterfahndung nach dem 11. September

Es ist wohl nicht übertrieben, wenn man behauptet: „Der 11. September 2001 hat die Welt verändert." Um den Gefahren zu begegnen, verlangt die Behörde X von einer Universität mit hohem Ausländeranteil Daten über Ausländer arabischer Herkunft (Name, Alter, Staatsangehörigkeit, Semester, Studienfach). Student Y fühlt sich in seinen Rechten verletzt.



Die Differenzierung zwischen präventiver und restriktiver Rasterfahndung ist von Bedeutung für die Rechtsgrundlage (Polizeirecht oder Strafrecht) und den Rechtsweg. Das Polizeirecht fordert grundsätzlich den „Verwaltungsrechtsweg" und das Strafrecht den „ordentlichen Rechtsweg"

Art. 92 GG

Die rechtsprechende Gewalt ist den Richtern anvertraut; sie wird durch das Bundesverfassungsgericht, durch die in diesem Grundgesetze vorgesehenen Bundesgerichte und durch die Gerichte der Länder ausgeübt.

Art. 95 GG

Für die Gebiete der ordentlichen, der Verwaltungs-, der Finanz-, der Arbeits- und der Sozialgerichtsbarkeit errichtet der Bund als oberste Gerichtshöfe den Bundesgerichtshof, das Bundesverwaltungsgericht, den Bundesfinanzhof, das Bundesarbeitsgericht und das Bundessozialgericht. (...)

Bundesverfassungsgericht				
Bundesarbeitsgericht	**Bundesfinanzgericht**	**Bundesverwaltungsgericht**	**Bundessozialgericht**	**Bundesgerichtshof für Zivil- und Strafsachen (ordentliche Gerichtsbarkeit)**

I. Falllösung

1 Recht

Das Recht auf informationelle Selbstbestimmung wird nach Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 S. 1 GG geschützt, weil die Verfügungsmacht über Daten Voraussetzung der allgemeinen Handlungsfreiheit wie Teil der Menschenwürde ist („allgemeines Persönlichkeitsrecht“). Daten wie die Adresse, die Staatsanghörigkeit und die Studienrichtung haben offensichtlich Bezug zum allgemeinen Persönlichkeitsrecht. (Gegenbeispiel: Mitteilung der Anzahl der Studierenden im Fachbereich 1 „Wirtschaftsinformatik“).

2 Eingriff

Durch die polizeiliche „Organisation“ der Daten bei der Universität könnte in das Recht auf informationelle Selbstbestimmung von Studenten arabischer Herkunft eingegriffen werden. Der Eingriffsbegriff ist immer vor dem Hintergrund des betroffenen Grundrechts zu entwickeln.

> BVerfG im Volkszählungsurteil: Jeder hat ein Recht, zu **wissen** wer, wann, wofür, welche personenbezogenen Daten „organisiert“ und muss grundsätzlich **einwilligen.**

- Y wird von der Übermittlung seiner Daten (an die Polizei) nicht informiert („wissen“).
- Y kann deshalb die „Organisation“ nicht verhindern.
- Es ist nicht davon auszugehen, dass Y einverstanden ist oder eingewilligt hat.

Ein Eingriff in das Recht auf informationelle Selbstbestimmung des Y liegt vor.

3 Rechtfertigung

a) Spezielle Schranke: Art. 2 Abs. 1 GG („verfassungsmäßige Ordnung“)

Diese Schranke ist in einer grammatischen Auslegung der jeweiligen Norm, hier der Verfassung zu entnehmen. Art. 2 Abs. 1 GG schränkt die freie Entfaltung der Persönlichkeit zugunsten Rechte anderer, der verfassungsmäßigen Ordnung oder des Sittengesetzes ein. Regelmäßig reicht die Prüfung der Rechtfertigung durch die „**verfassungsmäßige Ordnung**“ aus.

Der Begriff der „verfassungsmäßigen Ordnung“ ist weit auszulegen. „Verfassungsmäßige Ordnung“ umfasst die gesamte Rechtsordnung, soweit sie formell und materiell mit der Verfassung im Einklang steht (Verfassungsmäßigkeit). Formelle Verfassungsmäßigkeit setzt die Einhaltung der

- Kompetenz-,
- Verfahrens- und
- Formvorschriften voraus.

Materielle Verfassungsmäßigkeit setzt die Vereinbarkeit von unterverfassungsrechtlichem Recht mit der Verfassung voraus. Insbesondere erfolgt im Rahmen der materiellen Verfassungsmäßigkeit die Überprüfung anhand von Grundrechten.

Die Rasterfahndung stützt sich in Hessen auf § 26 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG).

§ 26 HSOG[10]
(1) Die Polizeibehörden können von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs zur Verhütung von Straftaten erheblicher Bedeutung
1. gegen den Bestand oder die Sicherheit des Bundes oder eines Landes oder
2. bei denen Schäden für Leben, Gesundheit oder Freiheit oder gleichgewichtige Schäden für die Umwelt zu erwarten sind,
die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Verhütung dieser Straftaten erforderlich und dies auf andere Weise nicht möglich ist. Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.
(...)

Die Speicherung der Daten beim BKA in einer Verbunddatei stützt sich auf § 7 BKAG.

§ 7 BKAG
(1) Das Bundeskriminalamt kann personenbezogene Daten speichern, verändern und nutzen, soweit dies zur Erfüllung seiner jeweiligen Aufgabe als Zentralstelle erforderlich ist.
(2) Das Bundeskriminalamt kann, soweit dies zur Erfüllung seiner Aufgabe als Zentralstelle nach § 2 Abs. 2 Nr. 1 erforderlich ist, Daten zur Ergänzung vorhandener Sachverhalte oder

[10] § 26 HSOG ist mit Gesetz vom 2. September 2002 eingefügt worden.

sonst zu Zwecken der Auswertung mittels Auskünften oder Anfragen bei öffentlichen oder nichtöffentlichen Stellen erheben. Auch bei den in § 14 Abs. 1 genannten Behörden und Stellen anderer Staaten sowie bei internationalen Organisationen, die mit der Verfolgung und Verhütung von Straftaten befasst sind, kann das Bundeskriminalamt unter den Voraussetzungen des Satzes 1 Daten erheben. In anhängigen Strafverfahren steht dem Bundeskriminalamt diese Befugnis nur im Einvernehmen mit der zuständigen Strafverfolgungsbehörde zu.
(…)

Um die Rasterfahndung und insbesondere das Auskunftsersuchen an die Universität als „öffentliche Stelle“ zu rechtfertigen, müsste § 26 HSOG Bestandteil der „verfassungsmäßigen Ordnung“ sein.

aa) Formelle Verfassungsmäßigkeit von § 26 HSOG

(1) Kompetenz:

Art. 70 Abs. 1 GG

Die Länder haben das Recht der Gesetzgebung, soweit dieses Grundgesetz nicht dem Bunde Gesetzgebungskompetenz verleiht.

Das HSOG dient der inneren Sicherheit und Ordnung. Diese wird dem Bund nicht durch das Grundgesetz als Gesetzesmaterie zugewiesen. Siehe im Übrigen Art. 73 Nr. 10 GG.

Art. 73 Nr. 10 GG

Der Bund hat die ausschließliche Gesetzgebungskompetenz über
10. die Zusammenarbeit des Bundes und der Länder
a) in der Kriminalpolizei,
b) zum Schutze der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes (Verfassungsschutz) und
c) zum Schutze gegen Bestrebungen im Bundesgebiet, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,
sowie die Einrichtung eines Bundeskriminalpolizeiamtes und die internationale Verbrechensbekämpfung;

Somit fällt das Recht der inneren Sicherheit grundsätzlich in die Gesetzgebungskompetenz der Länder.

(2) Verfahren

Es wird davon ausgegangen, dass das in der hessischen Landesverfassung vorgesehene Verfahren eingehalten wurde.

EXKURS: Gesetzgebungsverfahren auf Bundesebene

Gesetzesinitiative

Jedes Gesetzgebungsverfahren wird mit einer so genannten Gesetzesinitiative eingeleitet. Das ist die Einbringung eines Gesetzentwurfs. Gesetzesinitiativen können von der Bundesregie-

rung, dem Bundesrat und „aus der Mitte des Bundestages“ eingebracht werden (Art. 76 I GG).

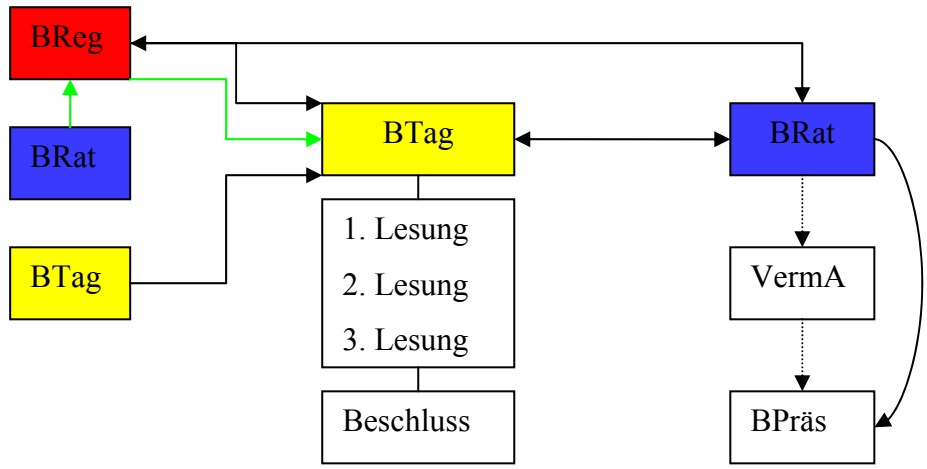
Beratung und Beschlussfassung

Bundesgesetze werden vom Bundestage beschlossen (Art. 76 I 1 GG). Das Verfahren der Beratung und Beschlussfassung im Bundestag ist nicht im Grundgesetz, sondern in der GOBT geregelt (§§ 79ff. GOBT). Danach finden drei so genannte Lesungen statt. Das sind Beratungen und Aussprachen über die einzelnen Bestimmungen des Gesetzentwurfs.

Beteiligung des Bundesrates

Nachdem der Bundestag ein Gesetz beschlossen hat, wird der Bundesrat beteiligt. Die Mitwirkungsrechte des Bundesrates sind entweder der Einspruch oder die Zustimmung.

Zusammenfassend:



Von der formellen Verfassungsmäßigkeit des § 26 HSOG ist auszugehen.

bb) Materielle Verfassungsmäßigkeit von § 26 HSOG

Das Besondere an der speziellen Schranke „Verfassungsmäßige Ordnung“ ist, dass sie im Rahmen der materiellen Verfassungsmäßigkeit die Prüfung der „allgemeinen Schranke“ – des Verhältnismäßigkeitsgrundsatzes im weiteren Sinne – verlangt.

Geeignetheit	Eingriff muss geeignet sein um den Schutz des Rechtsguts, das die Eingriffsrechtfertigung bildet (Rechtfertigungsrechtsgut), zu bewirken – Tauglichkeit des Mittels für den Zweck.
Erforderlichkeit	Es darf keine Maßnahme geben, die für den Schutz des Rechtfertigungsrechtsguts genauso geeignet und weniger eingreifend ist.
Verhältnismäßigkeit im engeren Sinne	Eingriff in das Eingriffsrechtsgut darf nicht außer Verhältnis zum Schutz des Rechtfertigungsrechtsguts stehen – Grundrechtseingriff darf in seiner Intensität nicht außer Verhältnis zum angestrebten Ziel stehen.

(1) Geeignetheit

Der Eingriff in die informationelle Selbstbestimmung muss geeignet sein, um den Schutz des Rechtfertigungsrechtsguts (Prävention von terroristischen Angriffen, die die körperliche Unversehrtheit und das Eigentum von Grundrechtsträgern bedrohen) zu bewirken. Hier sind, wie Gerichtsentscheidungen mit unterschiedlichen Ergebnissen zeigen, viele Argumente zu berücksichtigen. Insbesondere stellt sich die Frage, ob der Aufbau eines präventiven Rasterfahndungs- und Datenorganisationssystems geeignet ist Anschläge zu verhindern (siehe USA).

(2) Erforderlichkeit

Es ist zu prüfen, ob es eine Maßnahme gibt, die dem Rechtfertigungsrechtsgut ebenso dient, aber weniger das Eingriffsrechtsgut („informationelle Selbstbestimmung“) beschränkt. In Erinnerung gerufen sei die Besorgnis des Mikrozensusurteils, das zu Datensparsamkeit ermahnt. Eine Reduktion der Datenorganisation ist nicht offensichtlich ein milderes Mittel, weil § 26 Abs. 2 S. 1 HSOG bereits eine Beschränkung auf „bestimmte“ Daten vorsieht.

§ 26 Abs. 2 S. 1 HSOG

Das Übermittlungsersuchen ist auf Namen, Anschriften, Tag und Ort der Geburt sowie auf im einzelnen Falle festzulegende Merkmale zu beschränken.

Das gleiche gilt etwa für eine Reduzierung der Datenübermittlung auf Straftäter[11].

- Zwischenergebnis:

Unter der Prämisse der Geeignetheit ist eine vergleichbar effektive und effiziente Maßnahme nicht ersichtlich. Man könnte von der Erforderlichkeit ausgehen.

(3) Verhältnismäßigkeit im engeren Sinne

Hier ist der Qualität des Eingriffs in das Eingriffsrechtsgut die Qualität der Förderung des Rechtfertigungsrechtsguts gegenüberzustellen.

Qualität des Eingriffs:

- Für eine Schwere des Eingriff: Argument der Streubreite

  Die Rasterfahndung betrifft nur in sehr kleiner Anzahl eine wirklich fahndungsrelevante Gruppe. Die Datenübermittlung betrifft en Gros gesetzestreue – auch zukünftig gesetzestreue – Personen.

- Für eine Schwere des Eingriffs: Zweck der Datenerhebung

  Die Datenübermittlung zur Rasterfahndung geht über den ursprünglichen Zweck der Datenerhebung – Verwaltung des Studiums - hinaus. Grundsätzlich vertraut jede Person bei Datenabgabe darauf, dass die Daten nur für den angegebenen und abgegebenen Zweck verwendet werden.

- Für eine fehlende Schwere des Eingriffs: Argument geringer Personenbezogenheit

  In der Rasterfahndung geht es zunächst nicht um die Identifizierung Einzelner, sondern die Behandlung eines abstrakt spezifischen Datensatzes („personengruppenscharf"). Erst im Laufe der Rasterfahndung werden die Daten „personenscharf" behandelt.

- Für eine Schwere des Eingriffs: Heimlichkeit

  Welche Personen im Konkreten von der Rasterfahndung betroffen sind, ist nicht bekannt. Auch auf welche Merkmale die Rasterfahndung im Konkreten beschränkt ist, ist grundsätzlich nicht bekannt.

- Für eine Schwere des Eingriffs: Rasterfahndung als Mittel der repressiven Strafverfolgung

  Die Rasterfahndung ist ein Mittel der herkömmlichen repressiven Strafverfolgung. Wie das Wort Fahndung im allgemeinen Sprachgebrauch nahe legt, braucht es eine konkrete Zielperson, mithin einen Beschuldigten. Die präventive Rasterfahndung vermutet jedoch nur eine Gefahr, die je nach Rechtsgrundlage mehr oder weniger konkret sein muss.

§ 26 Abs. 1 S. 1 HSOG

(...) wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Verhütung dieser Straftaten erforderlich (...)

[11] Dies ist zudem ein anderes Verfahren, da an den Universitäten Straftäter zunächst identifiziert werden müssten.

- Für eine fehlende Schwere des Eingriffs: Effektivität

  Die Effektivität im präventiven Bereich unterstellen die Landesgesetzgeber durch die Einführung oder Änderung entsprechender Vorschriften - etwa des § 26 HSOG. Ob die Rasterfahndung tatsächlich mögliche Terroranschläge verhindern kann, bleibt anzuwarten.

- Für eine (fehlende) Schwere des Eingriffs: Gefährdungspotential

  Im Anschluss an den 11. September 2001 mag die Gefahr eines weitern Angriffs (geistig) präsent und das Gefährdungspotential sehr hoch gewesen sein. Nicht erst die im Laufe der Zeit erschienen Dokumente – etwa im Zusammenhang mit dem Irak-Krieg - zeigen, wie ein Gefährdungspotential zu politischen Zwecken missbraucht werden kann.

- Für eine fehlende Schwere des Eingriffs: Integration

  Die Rasterfahndung an den Universitäten stigmatisiert eine Personengruppe, deren Integration eigentliches Ziel der Allgemeinheit sein sollte.

- Für eine Schwere des Eingriffs: Behördenleitervorbehalt

  Die Rasterfahndung in Hessen steht „nur“ unter einem Behördenleitervorbehalt. In anderen Bundesländern – etwa Berlin - wird die Durchführung der Rasterfahndung von der Anordnung des Richters abhängig gemacht (Richtervorbehalt).

  § 26 Abs. 4 HSOG

  (4) Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die **Behördenleitung** und der Zustimmung des Landespolizeipräsidiums. Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte unverzüglich zu unterrichten.

  Die repressive Rasterfandung nach der Strafprozessordnung steht unter einem Richtervorbehalt. Man könnte erwägen die Verfassungsmäßigkeit der präventiven Rasterfahndung ebenfalls an einen Richtervorbehalt zu knüpfen.

- Zwischen- und Endergebnis

  Eine präventive Rasterfahndung kann je nach Konkretisierung des Verdachts und Differenzierung der Fahndungskriterien dazu führen, dass auch „Otto-Normalbürger“ das Stigma eines „Terroristen“ „verliehen“ wird. Darüber hinaus ist die Rasterfahndung ein weiterer Schritt zur virtuellen Erfassung der Persönlichkeit von Menschen. Auch die Chancen einer Rasterfahndung können kontrovers beurteilt werden. Vielleicht sollte die Rasterfahndung von einem Richtervorbehalt anhängig gemacht werden der sich auch auf einzelne Datenorganisationsprozesse erstreckt. Somit könnte die Rasterfahn-

dung und die Datenorganisation bei der Universität nicht gerechtfertigt sein und somit gegen Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verstoßen.

b) Allgemeine Schranke: Grundsatz der Verhältnismäßigkeit

Hier gilt das oben gesagte. Im Ergebnis könnte die Rasterfahndung somit nicht gerechtfertigt sein und gegen die informationelle Selbstbestimmung verstoßen.