Fachgebiet Öffentliches Recht
Prof. Dr. Viola Schmid, LL.M. (Harvard)

TECHNISCHE UNIVERSITÄT DARMSTADT

Cyberlaw

Basics in der Tradition seit 2003 (aktualisiert 12/2019)

WiP

„Cluster II"

Cyberlaw: Basics in der Tradition seit 2003 – „Cluster II" Gliederung:

TECHNISCHE UNIVERSITÄT DARMSTADT

I. Orientierung – Anspruch

II. Rechtsquellen
1. Vier Rechtsquellen mit Akronymologie
2. Cave: EU-DSGRL
3. Future law (de lege ferenda)? ePrivacy-Verordnung

III. SI²S: "Objekte" in einer **ersten** Übersicht
1. Si²S Schema (Cluster I) für den "Rasterfahndungsfall"
2. Terminologie "Personenbezogene" Daten
3. Fünf Arten personenbeziehbarer Daten

Fortsetzung auf nächster Folie

Cyberlaw: Basics in der Tradition seit 2003 – „Cluster II" Gliederung:

TECHNISCHE UNIVERSITÄT DARMSTADT

3. Fünf Arten personenbeziehbarer Daten
   a) eigene Kategorisierung
   b) Rechtsquellen
   c) "Nur" vier Legaldefinitionen
      aa) für gesundheits- und identitätsindikative Daten
      bb) DSGVO: für Sicherheitsdaten
      cc) DSGRL: für Sicherheitsdaten
   d) DSGRL: Wahrheits-, Qualitäts- und Aktualitätsstandards für Sicherheitsdaten

4. "Verarbeitung" personenbeziehbarer Daten
   a) "Verarbeitung" – Legaldefinition identisch in DSGVO und DSGRL
   b) DSGVO: Grundsätzliches "Verarbeitungsverbot" hinsichtlich der Datenkategorien 1-4

Cyberlaw: Basics in der Tradition seit 2003 – „Cluster II" Gliederung:

TECHNISCHE UNIVERSITÄT DARMSTADT

[4. …]

c) Ausnahmen für die Verarbeitung personenbeziehbarer Daten der Kategorien 1-4

aa) Übersicht

bb) Rechtsquellen

d) DSGRL: Kein grundsätzliches "Verarbeitungsverbot" hinsichtlich der Datenkategorien 1-4 (Vergleich: DSGVO)

e) DSGRL: Besondere Verarbeitungsbedingungen (Art. 9 DSGRL)

5. "Survival Guide": (nicht) personenbezogene und (nicht) personenbeziehbare Daten

a) Rechtliche Fundierung der terminologischen Differenzierung

b) Rechtsterminologische Differenzierung mit 5 „Arbeitskategorien"

IV. Gliederung des Cluster II – anschließend an Basics Cluster I

I. Orientierung – Anspruch

TECHNISCHE UNIVERSITÄT DARMSTADT

Orientierung: Didaktische „Clusterstrategie“:

→ ein Rückblick auf Teil I erfolgt, um Wiederholungen zu vermeiden: Die Gliederungsfolie hierzu findet sich im Anhang I.

→ Die „Clusterverbindung“ zwischen „Cluster I“ und „Cluster II“ beginnt deshalb mit „V.“ der Gliederung.

→ Die Gliederungen I.-IV. sind im Cluster II eigenständig.

→Quellen im „Mehrebenenmodell“* werden mit (eigenen) Akronymen versehen:

Anspruch ist:

„So wenig Recht wie möglich, so viel Recht wie nötig (und vice versa).“

* Eigene Terminologie, entgegen Art. 6 Abs. 2 EUV ist der Beitritt der EU zur EMRK bisher nicht erfolgt, weshalb eine "Systemqualität" im Verhältnis von BRD/EU/EMRK (noch) nicht gegeben ist. Vgl. EuGH, Gutachten vom 18.12.2014, Az. 2/14 und die Stellungnahme der Generalanwältin Kokott vom 13.06.2014, Az. 2/13. Einen Überblick hierzu bieten auch die Vorlesungsmaterialien zum Europarecht aus dem SoSe 2015 (vom 05.05.2015): https://www.cylaw.tu-darmstadt.de/lehre_3/lehrveranstaltungen_2/europarecht_i_2/archiv_1/sommersemester_47/europarecht_i_7.de.jsp

II. Rechtsquellen –
1. Vier Rechtsquellen mit Akronymologie:
EU-Sekundärrecht: EU-DSGVO & EU-DSGRL

TECHNISCHE UNIVERSITÄT DARMSTADT

1. EU-DSGVO: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

2. EU-DSGRL: Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (EU-DSGRL – FÖR-Akronymologie)

II. Rechtsquellen -
2. Cave: EU-DSGRL (eigene Akronymologie) und "JI-Richtlinie" (Bundesministerium des Inneren)

TECHNISCHE UNIVERSITÄT DARMSTADT

CAVE („Achtung"): Das etwa vom Bundesministerium des Inneren verwendete Akronym lautet stattdessen "JI-Richtlinie" ((Datenschutz)Richtlinie für Justiz und Inneres)/ Richtlinie für Datenschutz in Polizei und Justiz (11/2019). FÖR entscheidet sich für das hiesige Akronym, um die zeitliche und inhaltliche Parallelität von VO wie RL (Art. 288 Abs. 2 und 3 AEUV) zu verdeutlichen - wie auch deren jeweils fundamentalen Charakter („Grund").

Sailko,https://commons.wikimedia.org/w/index.php?curid=51022710

II. Rechtsquellen –
1. Vier Rechtsquellen mit Akronymologie: BRD-Sekundärrecht: BDSG & hier: HDSIG

TECHNISCHE UNIVERSITÄT DARMSTADT

3. BDSG: Bundesdatenschutzgesetz

4. HDSIG: Hessisches Datenschutz- und Informationsfreiheitsgesetz (zuletzt geändert am 12. Sept. 2018)

II. Rechtsquellen 3. Future law (de lege ferenda)? ePrivacy-Verordnung Bundesverband Digitale Wirtschaft e.V. : Timeline:

Quelle: Bundesverband Digitale Wirtschaft (BVDW) e.V., https://www.bvdw.org/themen/recht/kommunikationsrecht-eprivacy/#c3158, 03.12.2019.

II. Rechtsquellen - 3. Future law (de lege ferenda)? ePrivacy-Verordnung News (12/2019) – Eine Verbandsinformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Bundesverband Digitale Wirtschaft (BVDW) e.V.:

"UPDATE 25.11.2019 - ePrivacy-Text fällt in COREPER durch"

"**Der Ausschuss der ständigen Vertreter der EU-Mitgliedsstaaten (COREPER) hat auf seiner Sitzung am letzten Freitag (22.11.2019) den seitens der finnischen Ratspräsidentschaft vorgelegten Textentwurf für eine ePrivacy-Verordnung als Grundlage für die Beschlussfassung über einen Gemeinsamen Standpunkt des Europäischen Rates abgelehnt. Dies hätte ansonsten in der nächsten Sitzung des Telekommunikationsrates (WP TELE) am 03.Dezember auf der Tagesordnung gestanden. Damit wird es – anders als seitens der Präsidentschaft geplant – nun doch nicht mehr zur Aufnahme von Trilogverhandlungen in diesem Jahr kommen.**

[…] auch wenn ein Ende des Gesetzgebungsverfahrens damit einmal mehr in die Ferne rückt. Angesichts der zahlreichen widerstreitenden Interessen und der wachsenden Erkenntnis, dass die bislang vorgelegten Formulierungen **keine zukunftsfähige Lösung für die komplexen Anforderungen des Digitalmarktes darstellen**, liegt hierin jedoch die Chance, das Dossier neu zu denken. Bereits seit Veröffentlichung des Kommissionsentwurfs im Jahre 2017 waren insbesondere die zu befürchtenden, negativen Konsequenzen für die Angebots- und Wettbewerbsvielfalt einer der Hauptkritikpunkte an dem Entwurf."
https://www.bvdw.org/themen/recht/kommunikationsrecht-eprivacy/ (03.12.2019)

III. SI²S: Objekte in einer ersten Übersicht – 1. Si²S Schema (Cluster I) für den "Rasterfahndungsfall"

TECHNISCHE UNIVERSITÄT DARMSTADT

		Analyse
1	**Personal-aktiv**	Behörde (Ermächtigungsgrundlage?)
2 a)	**Personal-passiv** Datenschutz	Universität (Behörde) Studierende
2 b)	**Personal-passiv** Informationskosten	Universität (Kosten der Amtshilfe)
3	**Objekt**	Daten über Ausländer arabischer Herkunft – (Besondere personenbezogene Daten, Art. 9 Abs. 1 EU-DSGVO / Art. 10 EU-DSGRL / § 46 Nr. 14 BDSG / § 41 Nr. 15 HDSIG)
4	**Kausal/Zweck**	Terrorismusbekämpfung
5 a), b)	**Qualität der Informationstechnik**	Datenorganisation Erhebung durch die Universität Übermittlung von Universität an Behörde (keine Angaben im Sachverhalt zu 5 a) u. b)
6	**Verfahren**	Besondere Verfahrens- und Formvorschriften in der StPO und den Polizeigesetzen
7	**Rechtfertigung/ Verhältnismäßigkeit**	Abwägung des Interesses von Personal-aktiv (Rechtfertigungsrechtsgut (Öffentliche Sicherheit)) mit dem Interesse des Personal-passiv (Eingriffsrechtsgut (Recht auf informationelle Selbstbestimmung))

III. SI²S: Objekte in einer ersten Übersicht - 2. Terminologie "Personenbezogene Daten"

TECHNISCHE UNIVERSITÄT DARMSTADT

FÖR: "Personenbezogene" Daten

Gängig im Datenschutzrecht ist die Terminologie "personenbezogene Daten".*

Hervorzuheben ist, dass teleologisch **auch** "personen**beziehbare** Daten" gemeint sind. Siehe dazu auch Art. 4 Nr. 1 DGSVO, mit der Bestimmung "identifizierbare natürliche Person (im folgenden "betroffene Person") und "identifiziert werden kann":

Art. 4 DSGVO Begriffsbestimmungen […]

1. „personenbezogene Daten“ **alle Informationen**, die sich auf eine **identifizierte** oder **identifizierbare natürliche Person** (im Folgenden „**betroffene Person**“) **beziehen**; als **identifizierbar** wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der **physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen** oder **sozialen Identität** dieser natürlichen Person sind; […]

III. SI²S: Objekte in einer Übersicht -
3. Fünf Kategorien personenbeziehbarer Daten
a) eigene Kategorisierung

TECHNISCHE UNIVERSITÄT DARMSTADT

Rechtsquellen: Art. 9 Abs. 1 EU-DSGVO / Art. 10 EU-DSGRL / Art. 10 EU- DSGVO / Art. 6, 7 EU- DSGRL

1. **Herkunftsindikative Daten:** personenbezogener Daten, aus denen die rassische oder ethnische Herkunft
2. **Meinungsindikative Daten:** politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschafts-zugehörigkeit hervorgehen
3. **Gesundheits- und identitätsindikative Daten:** genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten
4. **Sexualindikative Daten:** Daten zum Sexualleben oder der sexuellen Orientierung
5. **"Sicherheitsdaten":** Art. 10 DSGVO / Art. 6, 7 DSGRL

III. SI²S: Objekte in einer Übersicht -
3. Fünf Kategorien personenbeziehbarer Daten
b) Rechtsquellen

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 9 Abs. 1 DSGVO: […] personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie […] genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person […].

Art. 10 DSGVO: […] personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln […] Ein umfassendes Register der strafrechtlichen Verurteilungen [...]

III. SI²S: Objekte in einer Übersicht - 3. c) "Nur" vier Legaldefinitionen aa) für gesundheits- und identitätsindikative Daten

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 4 Nr. 13–15 EU-DSGVO / Art. 3 Nr. 12–14 EU-DSGRL / § 46 Nr. 11–13 BDSG / § 41 Nr. 12–14 HDSIG [Begriffsbestimmungen]

[...] **genetische Daten** personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden [...]

[...] **biometrische Daten** mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten [...]

[…] **Gesundheitsdaten** personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen […]

III. SI²S: Objekte in einer Übersicht - 3. c) DSGVO: "Nur" vier Legaldefinitionen bb) für Sicherheitsdaten

TECHNISCHE UNIVERSITÄT DARMSTADT

"Nur"

Festzuhalten ist: Für die Kategorien 1, 2 und 4 existieren keine Legaldefinitionen. Für die hier so bezeichnete 5. Kategorie – die "Sicherheitsdaten"* - bestimmt **Art. 10 DSGVO: Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten**

[1]Die Verarbeitung **personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten** oder damit zusammenhängende **Sicherungsmaßregeln** aufgrund von Artikel 6 Absatz 1 darf nur unter **behördlicher Aufsicht** vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. [2]Ein **umfassendes Register der strafrechtlichen Verurteilungen** darf nur unter behördlicher Aufsicht geführt werden.

* Die Terminologie "Sicherheitsdaten" wurde gewählt, um jegliche Bewertung auszuschließen. Dies wäre mit der Verwendung der Terminologie "sicherheitsindikative Daten" vielleicht verbunden worden.

III. SI²S: Objekte in einer Übersicht - 3. c) bb) Verweis auf Art. 6 Abs. 1 DSGVO in Art. 10 DSGVO

TECHNISCHE UNIVERSITÄT DARMSTADT

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung **vorvertraglicher Maßnahmen** erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer **Aufgabe** erforderlich, die **im öffentlichen Interesse** liegt oder in **Ausübung öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur **Wahrung der berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, **überwiegen**, insbesondere dann, wenn es sich bei der betroffenen Person um ein **Kind** handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. […] (Hervorhebung durch Bearbeiterin)

III. SI²S: Objekte in einer Übersicht - 3. c) cc) DSGRL: für Sicherheitsdaten

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 6 EU-DSGRL: Unterscheidung verschiedener Kategorien betroffener Personen

Die Mitgliedstaaten sehen vor, dass der Verantwortliche gegebenenfalls und so weit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen klar unterscheidet, darunter:

a) Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden,

b) verurteilte Straftäter,

c) Opfer einer Straftat oder Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und

d) andere Parteien im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den unter den Buchstaben a und b genannten Personen in Kontakt oder in Verbindung stehen.

III. SI²S: Objekte in einer Übersicht - 3. d) DSGRL: Wahrheits-, Qualitäts- und Aktualitätsstandards für Sicherheitsdaten

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 7 EU-DSGRL Unterscheidung zwischen personenbezogenen Daten und Überprüfung der Qualität der personenbezogenen Daten

(1) Die Mitgliedstaaten sehen vor, dass bei personenbezogenen Daten so weit wie möglich zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten unterschieden wird.

(2) Die Mitgliedstaaten sehen vor, dass die zuständigen Behörden alle angemessenen Maßnahmen ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Zu diesem Zweck überprüft jede zuständige Behörde, soweit durchführbar, die Qualität der personenbezogenen Daten vor ihrer Übermittlung oder Bereitstellung. Bei jeder Übermittlung personenbezogener Daten werden nach Möglichkeit die erforderlichen Informationen beigefügt, die es der empfangenden zuständigen Behörde gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der personenbezogenen Daten sowie deren Aktualitätsgrad zu beurteilen.

(3) Wird festgestellt, dass unrichtige personenbezogene Daten übermittelt worden sind oder die personenbezogenen Daten unrechtmäßig übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. In diesem Fall ist gemäß Artikel 16 eine Berichtigung oder Löschung oder die Einschränkung der Verarbeitung der personenbezogenen Daten vorzunehmen.

III. SI²S: Objekte in einer Übersicht - 4. "Verarbeitung" personenbeziehbarer Daten a) "Verarbeitung" – Legaldefinition identisch in DSGVO und DSGRL

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 4 Nr. 2 DGSVO / Art. 3 Nr. 2 DSGRL

Begriffsbestimmungen
[…]
2. „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie **das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung**;
[…]

III. SI²S: Objekte in einer Übersicht - 4. b) DSGVO: Grundsätzliches "Verarbeitungsverbot" hinsichtlich der Datenkategorien 1-4

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 9 DSGVO
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person **ist untersagt**.

III. 4. c) DSGVO: Ausnahmen für die Verarbeitung personenbeziehbarer Daten der Kategorien 1-4
aa) Übersicht

TECHNISCHE UNIVERSITÄT DARMSTADT

Ausnahmen als Rechtfertigung für die Verarbeitung personenbeziehbarer Daten der Kategorien 1-4 (Art. 9 Abs. 2 DSGVO) trotz des Verarbeitungsverbots - im **Überblick**:

a. Einwilligung
b. Soziale Sicherheit
c. Lebenswichtige Interessen
d. Teilhabe an und Tätigkeit von rechtmäßigen Korporationen ohne Gewinnerzielungsabsicht
e. Offensichtliches Publikationsinteresse
f. Teilhabe am Rechtsstaat und Judikative
g. **Unions-/ Staatsvorbehalt** zur Wahrung eines erheblichen öffentlichen Interesses
h. + i. Gesundheit(svorsorge) im öffentlichen und privaten Sektor (inklusive Arbeitsmedizin)
j. **Unions-/ Staatsvorbehalt** zur Wahrung von Archivzwecken, zur Verfolgung statistischer Zwecke und für die Forschung

III. 4. c) DSGVO: Ausnahmen für die Verarbeitung personenbeziehbarer Daten der Kategorien 1-4
bb) Rechtsquellen

TECHNISCHE UNIVERSITÄT DARMSTADT

Ausnahmen als Rechtfertigung für die Verarbeitung trotz des Verarbeitungsverbots personenbeziehbarer Daten der Kategorien 1-4

Art. 9 DSGVO
Verarbeitung besonderer Kategorien personenbezogener Daten

(2) Absatz 1 **gilt nicht** in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich **eingewilligt**, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch **die Einwilligung der betroffenen Person nicht aufgehoben werden**,

b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der **sozialen Sicherheit** und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,

III. 4. c) DSGVO: Ausnahmen für die Verarbeitung personenbeziehbarer Daten der Kategorien 1-4 bb) Rechtsquellen

TECHNISCHE UNIVERSITÄT DARMSTADT

c) die Verarbeitung ist zum Schutz **lebenswichtiger Interessen** der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,

d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation **ohne Gewinnerzielungsabsicht** im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung **ausschließlich auf die Mitglieder** oder ehemalige Mitglieder der Organisation **oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten**, bezieht **und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,**

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die **betroffene Person offensichtlich öffentlich gemacht hat**,

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder **Verteidigung von Rechtsansprüchen** oder bei **Handlungen der Gerichte** im Rahmen ihrer justiziellen Tätigkeit erforderlich,

III. 4. c) DSGVO: Ausnahmen für die Verarbeitung personenbeziehbarer Daten der Kategorien 1-4
bb) Rechtsquellen

TECHNISCHE UNIVERSITÄT DARMSTADT

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den **Wesensgehalt des Rechts auf Datenschutz** wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen **eines erheblichen öffentlichen Interesses** erforderlich,

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im **Gesundheits- oder Sozialbereich** oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

III. 4. c) DSGVO: Ausnahmen für die Verarbeitung personenbeziehbarer Daten der Kategorien 1-4 bb) Rechtsquellen

TECHNISCHE UNIVERSITÄT DARMSTADT

i) die Verarbeitung ist aus Gründen des **öffentlichen Interesses** im Bereich der **öffentlichen Gesundheit**, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im **öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke** gemäß Artikel 89 Absatz 1 erforderlich.

[…]

III. SI²S: 4. d) DSGRL: Kein grundsätzliches "Verarbeitungsverbot" hinsichtlich der Datenkategorien 1-4 (Vergleich: DSGVO)

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 10 EU-DSGRL: Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung ist nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und

a) wenn sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist

b) der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder

c) wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.

III. SI²S: 4. e) DSGRL: Besondere Verarbeitungs-bedingungen (Art. 9 DSGRL)

TECHNISCHE UNIVERSITÄT DARMSTADT

(1) Personenbezogene Daten, die von zuständigen Behörden für die in Artikel 1 Absatz 1 genannten Zwecke erhoben werden, dürfen **nicht für andere als die in Artikel 1 Absatz 1 genannten Zwecke verarbeitet** werden, es sei denn, eine derartige Verarbeitung ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig. Wenn personenbezogene Daten für solche andere Zwecke verarbeitet werden, gilt die Verordnung (EU) 2016/679, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

(2) Sind nach dem Recht der Mitgliedstaaten zuständige Behörden mit der Wahrnehmung von Aufgaben betraut, die sich nicht mit den für die in Artikel 1 Absatz 1 genannten Zwecke wahrgenommenen Aufgaben decken, gilt die Verordnung (EU) 2016/679 für die Verarbeitung zu diesen Zwecken — wozu auch im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke zählen —, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

(3) Die Mitgliedstaaten sehen vor, dass immer dann, wenn nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem die übermittelnde zuständige Behörde unterliegt, für die Verarbeitung besondere Bedingungen gelten, die übermittelnde zuständige Behörde den Empfänger der Daten darauf hinweist, dass diese Bedingungen gelten und einzuhalten sind.

(4) Die Mitgliedstaaten sehen vor, dass die übermittelnde zuständige Behörde auf Empfänger in anderen Mitgliedstaaten oder nach Titel V Kapitel 4 und 5 AEUV errichtete Einrichtungen und sonstige Stellen keine Bedingungen nach Absatz 3 anwendet, die nicht auch für entsprechende Datenübermittlungen innerhalb ihres eigenen Mitgliedstaats gelten.

III. 5. "Survival Guide": (nicht)personenbezogene und (nicht)personenbeziehbare Daten
a) Rechtliche Fundierung e. terminologischen Differenzierung

TECHNISCHE UNIVERSITÄT DARMSTADT

FÖR Didaktik: Zwei Grundlagen der Unterscheidung der Daten natürlicher Personen von anderen Entitäten.

Im deutschen (Verfassungs)Recht gibt es zwei Grundlagen für die Unterscheidung der Daten

- natürlicher Personen einerseits und
- technischer wie wirtschaftlicher "Entitäten" andererseits.

Nur natürlichen Personen steht **das Recht auf** Menschenwürde wie der **Schutzanspruch** zu (Art. 1, 20, 23 Abs. 1 S. 3 GG iVm Art. 79 Abs. 3 GG). Im Cyberlaw handelt es sich insbesondere um den "absolut geschützten Kernbereich privater Lebensgestaltung", den das BVerfG gerade in der ersten Entscheidung zur akustischen Wohnraumüberwachung (*Entscheidung des BVerfG vom 03.03.2004 - 1 BvR 2378/98 und 1 BvR 1084/99, vgl. CyLaw-Report XVI: "Akustische Wohnraum-überwachung"*, https://tuprints.ulb.tu-darmstadt.de/1114/1/CyLaw_Report_XVI_06_08_10.pdf) konturiert hat. [1/2]

III. 5. "Survival Guide": (nicht)personenbezogene und (nicht)personenbeziehbare Daten
a) Rechtliche Fundierung e. terminologischen Differenzierung

TECHNISCHE UNIVERSITÄT DARMSTADT

[2/2]
Seit der Volkszählungsentscheidung aus 1983 hat das BVerfG zudem mehrere "Cyberlaw-Konkretisierungen" des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) entworfen (Recht auf informationelle Selbstbestimmung *("Volkszählung" BVerfG, Urteil v. 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83)*, Vertraulichkeit und Integrität informationstechnischer Systeme (*"Online-Durchsuchung", BVerfG, Urteil v. 27.02.2008, Az. 1 BvR 370/07, 1 BvR 595/07*), differenzierend zum Recht am (eigenen) Bild, *BVerfG. Kammerbeschl. V. 08.02.2018, Az. 1 BvR 2112/15*).

Beide Grundlagen – Recht am absolut geschützten Kernbereich privater Lebensgestaltung einerseits wie allgemeines Persönlichkeitsrecht in seinen "Cyberlawausdifferenzierungen" – zwingen dazu, personenbezogene und personenbeziehbare (und damit persönlichkeitsrechtsrelevante) von **anderen Daten** – hier als "Maschinendaten" bezeichnet - zu trennen.

III. 5. "Survival Guide": (nicht)personenbezogener und (nicht)personenbeziehbarer Daten
b) Rechtsterminologische Differenzierung mit 5 Arbeitskategorien

TECHNISCHE UNIVERSITÄT DARMSTADT

Nicht personenbeziehbare Daten		Personenbeziehbare und personenbezogene Daten		
Maschinendaten **clear case**	**Maschinendaten** **hard case**	**Personen-beziehbare Daten** **hard case**	**Personen-beziehbare Daten** **hard case**	**Personen-bezogene Daten** **clear case**
Demonstrator: In der Vorlesung zu präsentieren.				

IV. Gliederung des Cluster II – anschließend an Basics Cluster I

TECHNISCHE UNIVERSITÄT DARMSTADT

V. Rasterfahndung nach dem 11. September – „Rechtsverhalt"

VI. Time, Transition & Change Management – „Evaluation"

VII. „Evaluation": Schema für die **I**nteressenanalyse **I**nformationstechnologischer **S**achverhalte **(SI²S)** in der Tradition seit 2013/2003 mit veralteten Normquellen (11/2018)

VIII. Schema für die Schema für die **I**nteressenanalyse **I**nformationstechnologischer **S**achverhalte **(SI²S)** in der Tradition seit 2013/2003 – aktualisiert (11/2018)

1. Abstrakt
2. Abstrakt – Differenzierung „Objekt"(SI²S – 3): „Besondere Kategorien personenbezogener Daten" im „Mehrebenenmodell"
   a) EU
   b) BRD und Hessen
   c) Unterschiede im europäischen und deutschen Bundes- und Landesrecht?

III. SI²S: Objekte in einer Übersicht
4. Gliederung des Teil II – anschließend an Basics Teil I

TECHNISCHE UNIVERSITÄT DARMSTADT

3. Abstrakt – Differenzierung „Objekt"(SI²S – 3): „Besondere Kategorien personenbezogener Daten" im „Mehrebenenmodell"
4. Abstrakt – Differenzierung „Objekt"(SI²S – 3): „Informationstechnologisches Sicherheitsrecht " (eigene Terminologie) im „Mehrebenenmodell""
5. Abstrakt – Differenzierung „Kausal/Zweck" (SI²S – 4): Gefahrenbegriffe in Hessen und Bayern
6. Abstrakt – Differenzierung Qualität der Information(stechnik) „Personal–aktiv Informationsrecht" (SI²S – 5b)
7. Konkret

IX. RER-Schema

X. RER-Definition

1. Spezielle Schranken
2. Allgemeine Schranken –Verhältnismäßigkeit im weiteren Sinn

XI. RER-Prüfung

1. Recht
2. Eingriff

III. SI²S: Objekte in einer Übersicht
4. Gliederung des Teil II – anschließend an Basics Teil I

TECHNISCHE UNIVERSITÄT DARMSTADT

3. Rechtfertigung
   a) Terminologie
   b) Spezielle Schranken: Verfassungsmäßige Ordnung
   c) Allgemeine Schranken: Verhältnismäßigkeit im weiteren Sinn

XII. Falllösung

1. „Klassisch" seit 2003
2. Entscheidungen aus der Vergangenheit

XIII. Change Management

1. Hessen: Rechtsgrundlage der Rasterfahndung heute – früher
2. BRD: Rechtsgrundlagen der Rasterfahndung als ein traditionelles Kernelement des „informationstechnologischen Sicherheitsrechts"

FEX (I) Sicherheitsgesetzgebung in Deutschland – im Auszug

FEX (II) BVerfG – Sicherheitsrechtsprechung zur Rasterfahndung in Deutschland (2016)

FEX (III) Sicherheitsgesetzgebung in Deutschland (2018) – Rasterfahndung

Anhang I: Gliederung des Teil I

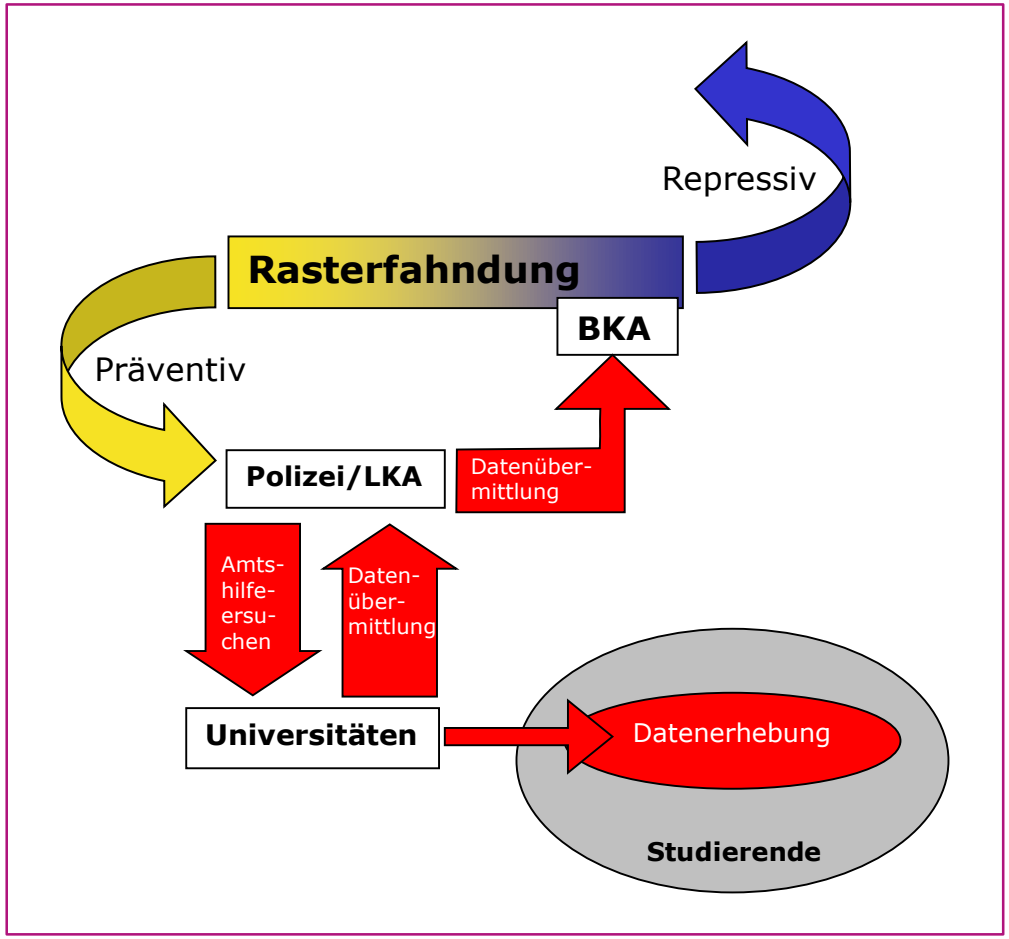
V. Rasterfahndung nach dem 11. September – „Rechtsverhalt" (eigene Terminologie)

TECHNISCHE UNIVERSITÄT DARMSTADT

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.

Es handelt sich um einen historischen Fall, der seit 2003 regelmäßig (in der Vorlesung) präsentiert wird. Er hat seitdem an Aktualität und Relevanz nichts eingebüßt. Dies rechtfertigt eine Präsentation auch in 2019 ff.
Typisch für Cyberlaw in 2019 ff. ist, dass die Herausforderungen klassische Qualität erhalten (Beleg: Rasterfahndung ist ein „Evergreen" im hier sog. informationstechnologischen Sicherheitsrecht" (eigene Terminologie)). Typisch ist ebenfalls, dass die „Antworten & Lösungen" – insbesondere im Rahmen der Verhältnismäßigkeitsprüfung im weiteren Sinne – kontext- und zeitspezifisch zu anderen Argumenten wie Entscheidungen führen können. Demzufolge stellt sich für die Vorlesung wie für die Klausurlösung für die Studierenden die Notwendigkeit zeitnaher Information wie Reflexion („Update").

V. Rasterfahndung nach dem 11. September – „Rechtsverhalt"(eigene Terminologie)



V. Rasterfahndung nach dem 11. September – „Rechtsverhalt"(eigene Terminologie) Rechtsquelle: § 26 Abs. 1 HSOG

TECHNISCHE UNIVERSITÄT DARMSTADT

Besondere Formen des Datenabgleichs

(1) Die **Polizeibehörden** können von **öffentlichen Stellen** oder nichtöffentlichen Stellen **zur Abwehr einer Gefahr** für den Bestand oder die Sicherheit des Bundes oder eines Landes oder **Leib, Leben oder Freiheit einer Person** oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn 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 dies **zur Abwehr der Gefahr erforderlich** ist. Eine solche Gefahr liegt in der Regel auch dann vor, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass terroristische Straftaten begangen werden sollen. Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.

VI. Time, Transition & Change Management – „Evaluation"

TECHNISCHE UNIVERSITÄT DARMSTADT

Cyberlaw als neue/weitere Disziplin des Rechts ist in besonderem Maße änderungsanfällig. Beim Cyberspace handelt es sich um eine 5. Dimension des Seins (neben den m³ der Realworld und der Zeit) und die Pioniererfahrungen in ökonomischer, informationstechnologischer und gesellschaftlicher wie rechtlicher Perspektive werden gegenwärtig erst gemacht. Deswegen ist der Cyberspace aus rechtlicher Sicht „Neuland" für die „Governance, Compliance & Regulation" (siehe auch die Forschungsinitiative „GoCore!") - wenn auch nicht für die Nutzung.

Deswegen ist die analytische Recherche und Präsentation des Gegenwartsrechts (**Time Management**) wie des Rechts der jüngeren Vergangenheit (Technikrechtsgeschichte) auch ein **Evaluationsargument** für Cyberlawlehre und –forschung. Demzufolge werden in die Vorlesung auch teilweise veraltete Quellen aufgenommen, wenn sie Argumente für **Konstituanten** dieser Rechtsdisziplin bieten wie die **Erhöhung von Orientierungschancen** versprechen. Diese Strategie wird mit dem Stichwort „Evaluation" gekennzeichnet. Dass darüber hinaus im Rahmen der **Verhältnismäßigkeitsprüfung im weiteren Sinne** etwa **Gefahrenanalysen** hinsichtlich terroristischer Anschläge zeitlich differieren können, verlangt ein **Change Management**. Geschuldet sind diese dogmatischen Besonderheiten des Cyberlaw der Übergangszeit der digitalen Transformation – **Transition Period**. Es sind eben derzeit noch nicht alle Funktionalitäten der digitalen Transformation rechtlich einsetz- wie beherrschbar.

VII. „Evaluation“: Schema für die Interessenanalyse Informationstechnologischer Sachverhalte (SI²S)* in der Tradition seit 2013/2003 mit veralteten Normquellen (11/2018)

TECHNISCHE UNIVERSITÄT DARMSTADT

1)	**Personal-aktiv Informationsrecht**	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an Informationen[31] interessiert ist.
2a)	**Personal-passiv Datenschutz**	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an der Reservierung- und Verfügungsmacht über Informationen interessiert ist, die ihr von der Rechtsordnung zugebilligt werden. Dazu gehört unter Umständen auch ein „Recht auf Vergessenwerden und auf Löschung“.[32]
2b)	**Personal-passiv Informationskosten**	Hierunter fallen die Kosten für die Erhebung, Speicherung, Aufbereitung und Übermittlung von Informationen durch den faktisch und rechtlich Verfügungsbefähigten (etwa den „Provider“). Dieses Argument wurde etwa in der Vorratsdatenspeicherungsentscheidung des BVerfG als vernachlässigbar qualifiziert[33] – auch wenn die Informationserhebung, -speicherung und -übermittlung nach Meinung der betroffenen Industrien erhebliche Kosten verursachen kann[34].
3)	**Objekt**	Auf Informationen **welchen Inhalts** soll zugegriffen werden? Hier kennt die Rechtsordnung die Differenzierung zwischen „sensitiven“ oder „sensiblen“ Informationen und anderen Informationen.

* Schmid, Zu den Voraussetzungen für die erfolgreiche Realisierung informationstechnologischer Projekte: die „HKA-Formel“ (Haftung – Kommunikation – Akzeptanz) und andere Herausforderungen, in: *Anzinger/Hamacher/Katzenbeisser* (Hrsg.), Schutz genetischer, medizinischer und sozialer Daten als multidisziplinäre Aufgabe, 2013, S. 219-237 unter Verweis auf Schmid, Cyberlaw – Eine neue Disziplin im Recht? in: Hendler/Marburger/Reinhardt/Schröder, Jahrbuch des Umwelt- und Technikrechts 2003, S. 449-480, 468 ff.
Auf eine Wiedergabe des Fußnotenkatalogs wird hier verzichtet und auf die Veröffentlichung verwiesen.

VII. „Evaluation“: Schema für die Interessenanalyse Informationstechnologischer Sachverhalte (SI²S)* in der Tradition seit 2013/2003 mit veralteten Normquellen (11/2018)

TECHNISCHE UNIVERSITÄT DARMSTADT

3)	**Objekt (Fortsetzung)**	Bei „sensitiven“ oder „sensiblen“ Informationen (§ 3 Abs. 9 BDSG) besteht einfachgesetzlich besonderer Begründungs- und Rechtfertigungsbedarf (§ 28 Abs. 6 BDSG). Verfassungsrechtlich besonders geschützt sind darüber hinaus Informationen, die zum „absolut geschützten Kernbereich privater Lebensgestaltung“[35] gehören (siehe auch etwa § 100c Abs. 5 S. 1 StPO). Weiter charakterisiert werden kann die Beschaffenheit des Objekts nicht nur durch den aktuellen Inhalt der Informationen, sondern durch ihren potenziellen Inhalt. Hat eine Information **Profilierungspotenzial**? Etwa dadurch, dass der Eingang eines Einfamilienhauses videoüberwacht wird, und so ein Bewegungs- und Kontaktprofil der dort wohnenden Familie erstellt werden kann[36]. Hat eine Information ein spezifisches **Kombinationspotenzial** – etwa durch die Verknüpfung mit anderen Informationen? Beispiel ist die Verknüpfung von mit RFID organisierten Informationen über ein einzelnes Produkt (Electronic Product Code) mit Kreditkartendaten.[37]
4)	**Kausal/Zweck**	Zu welchem Zweck soll auf diese Informationen zugegriffen werden (etwa: Kampf gegen den Terrorismus; Wahrung der Urheberrechte, Gesundheitsschutz als „Rechtfertigungsgüter“[38])? Differenziert werden kann dieses Kriterium noch durch den Grad der Gefährdung der Rechtfertigungsrechtsgüter. So etwa, wenn eine Videoüberwachung im Vorfeld einer Gefahr an einem „Straßenkriminalitätsbrennpunkt“ rechtmäßig sein soll.[39]

VII. „Evaluation“: Schema für die Interessenanalyse Informationstechnologischer Sachverhalte (SI²S)* in der Tradition seit 2013/2003 mit veralteten Normquellen (11/2018)

TECHNISCHE UNIVERSITÄT DARMSTADT

5a)	**Qualität der Information(stechnik) Personal-passiv Datenschutz**	Hierzu zählt die Informationstechnik, die etwa Daten vor unbefugter Einsichtnahme schützt, wie etwa die Verschlüsselung[40] oder die Zuteilung eines Passworts. Rechtsgrundlage sind unter anderem § 9 BDSG und Anlage. Die besondere Bedeutung von IT-Sicherheit für den Datenschutz von Personal-passiv ist in der BVerfG-Entscheidung zur „Vorratsdatenspeicherung“[41] betont worden.
5b)	**Qualität der Information(stechnik) Personal–aktiv Informationsrecht**	Erfasst sind alle Formen der **„Organisation“** von Daten.[42] Etwa in der Vorratsdatenspeicherungsentscheidung schließt das BVerfG den Pull-Betrieb aus und verlangt einen Push-Betrieb durch den „Provider“[43]. Die Sicherheitsbehörden dürfen also nicht selbst auf die beim Provider gespeicherten Daten ohne dessen Wissen zugreifen.
6)	**Rechtliches Verfahren**	Welches rechtliche Verfahren verlangt das Recht für die „Organisation“ und den Umgang mit diesen Daten? (Etwa: Einwilligung des Betroffenen, § 4a BDSG; Einschaltung eines Gremiums, §§ 14, 15 G 10[44]; Richtervorbehalt, etwa § 100b Abs. 1 S. 1 StPO.)
7)	**Rechtfertigung/Verhältnis-mäßigkeit**	Hier findet etwa die aus dem deutschen Verfassungsrecht bekannte Verhältnismäßigkeitsprüfung statt, die das Interesse von Personal-aktiv (Rechtfertigungsrechtsgut) und das Interesse des Personal-passiv Datenschutzes (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 10 GG, Art. 13 GG) und das Interesse der Personal-passiv Informationskosten (Art. 12, 14, 2 Abs. 1 GG) abwägt.

VIII. Schema für die Interessenanalyse Informations-technologischer Sachverhalte (SI²S) in der Tradition seit 2013/2003 – aktualisiert (11/2018)
1. Abstrakt

1)	**Personal-aktiv Informationsrecht**	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an Informationen interessiert ist.
2a)	**Personal-passiv Datenschutz**	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an der Reservierung- und Verfügungsmacht über Informationen interessiert ist, die ihr von der Rechtsordnung zugebilligt werden. Dazu gehört unter Umständen auch ein „Recht auf Vergessenwerden und auf Löschung".
2b)	**Personal-passiv Informationskosten**	Hierunter fallen die Kosten für die Erhebung, Speicherung, Aufbereitung und Übermittlung von Informationen durch den faktisch und rechtlich Verfügungsbefähigten (etwa den „Provider"). Dieses Argument wurde etwa in der ersten Vorratsdatenspeicherungsentscheidung des Bundes-verfassungsgericht* als vernachlässigbar qualifiziert – auch wenn die Informationserhebung, -speicherung und -übermittlung nach Meinung der betroffenen Industrien erhebliche Kosten verursachen kann.**
3)	**Objekt**	Auf Informationen **welchen Inhalts** soll zugegriffen werden? Hier kennt die „Rechtsordnung" (unter Berücksichtigung des „Mehrebenenmodells") bereits vor 2018 grundsätzlich die Unterscheidung zwischen „personen-bezogenen Daten" und „besonderer Kategorien personenbezogener Daten" (vgl. etwa § 3 Abs. 1 und 9 BDSG **alter Fassung**). Mit der EU-DSGVO werden die „besonderen Kategorien personenbezogener Daten" mit Legaldefinitionen weiter ausdifferenziert (siehe unter VIII. 2.-4.).

* BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08 u.a.
** So auch VG Köln, Urt. v. 20.04.2018, Az. 9 K 7417/17, Rn. 170; OVG NRW, Beschl. v. 22.06.2017, Az. 13 B 238/17, Rn. 88.

VIII. Schema für die Interessenanalyse Informations-technologischer Sachverhalte (SI²S) in der Tradition seit 2013/2003 – aktualisiert (11/2018)
1. Abstrakt

3)	**Objekt (Fortsetzung)**	Bei „besonderen Kategorien personenbezogener Daten"* besteht besonderer Begründungs- und Rechtfertigungsbedarf (Art. 9 EU-DSGVO; Art. 10 EU-DSGRL**; §§ 22, 48 BDSG; §§ 20, 43 HDSIG). Verfassungsrechtlich besonders geschützt sind darüber hinaus Informationen, die zum „absolut geschützten Kernbereich privater Lebensgestaltung" gehören (siehe etwa § 100d Abs. 1-4 StPO). Weiter charakterisiert werden kann die Beschaffenheit des Objekts nicht nur durch den aktuellen Inhalt der Informationen, sondern durch ihren potenziellen Inhalt. Hat eine Information **Profilierungspotenzial, das** als „Profiling" im Rechtssinne zu qualifizieren ist (Art. 4 Nr. 4, Art. 22 EU-DSGVO)? Hat eine Information ein spezifisches **Kombinationspotenzial** – etwa durch die Verknüpfung mit anderen Informationen? Beispiel ist die Verknüpfung von mit RFID organisierten Informationen über ein einzelnes Produkt (Electronic Product Code) mit Kreditkartendaten.
4)	**Kausal/Zweck**	Zu welchem Zweck soll auf diese Informationen zugegriffen werden (etwa: Kampf gegen den Terrorismus; Wahrung der Urheberrechte, Gesundheitsschutz als „Rechtfertigungsgüter")? Differenziert werden kann dieses Kriterium noch durch den Grad der Gefährdung der Rechtfertigungsrechtsgüter. So etwa, wenn eine Videoüberwachung im Vorfeld einer Gefahr an einem „Straßenkriminalitätsbrennpunkt" rechtmäßig sein soll.

* Art. 9 Abs. 1 EU-DSGVO / Art. 10 EU-DSGRL / § 46 Nr. 14 BDSG / § 41 Nr. 15 HDSIG.

VIII. Schema für die Interessenanalyse Informations-technologischer Sachverhalte (SI²S) in der Tradition seit 2013/2003 – aktualisiert (11/2018)
1. Abstrakt

TECHNISCHE UNIVERSITÄT DARMSTADT

5a)	**Qualität der Information(stechnik) Personal-passiv Datenschutz**	Hierzu zählt die Informationstechnik, die etwa Daten vor unbefugter Einsichtnahme schützt, wie etwa die Verschlüsselung oder die Zuteilung eines Passworts. Rechtsgrundlage sind unter anderem §§ 22 Abs. 2, 48 Abs. 2 BDSG; §§ 20 Abs. 2 und 3, 43 Abs. 2 HDSIG. Die besondere Bedeutung von IT-Sicherheit für den Datenschutz von Personal-passiv ist in der ersten BVerfG-Entscheidung zur „Vorratsdatenspeicherung" betont worden.
5b)	**Qualität der Information(stechnik) Personal–aktiv Informationsrecht**	Erfasst sind alle Formen der **„Organisation" (eigene Terminologie)** von Daten. Etwa in der ersten Vorratsdatenspeicherungsentscheidung schließt das BVerfG den Pull-Betrieb aus und verlangt einen Push-Betrieb durch den „Provider". Die Sicherheitsbehörden dürfen also nicht selbst auf die beim Provider gespeicherten Daten ohne dessen Wissen zugreifen. Spätestens seit 2018 ist „Drohnen"recht Bestandteil des hier sog. „informationstechnologischen Sicherheitsrechts". Art. 47 Bayrisches Polizeiaufgabengesetz (BayPAG) regelt – soweit ersichtlich – als Pionier im deutschen Polizeirecht den Einsatz von unbemannten Luft-fahrtsystemen sowohl für Video- als auch Audioaufnahmen (hier sog. „Peeping & Listening Drones") (Art. 47 Abs. 1 Nr. 1 BayPAG). Inwieweit wir die Welt mit „Drohnen" auch im Kontext von (land-)wirt-schaftlicher Betätigung teilen müssen und dürfen, wird vorhersehbar eine Kernaufgabe des Cyberlaw sein.

VIII. Schema für die Interessenanalyse Informations-technologischer Sachverhalte (SI²S) in der Tradition seit 2013/2003 – aktualisiert (11/2018)
1. Abstrakt

6)	**Rechtliches Verfahren**	Welches rechtliche Verfahren verlangt das Recht für die „Organisation" und den Umgang mit diesen Daten? (Etwa: Einwilligung des Betroffenen, Art. 9 Abs. 2 lit. a EU-DSGVO; Einschaltung eines Gremiums, §§ 14, 15 G 10; Richtervorbehalt, etwa § 100e Abs. 1 und 2 StPO.)
7)	**Rechtfertigung/Verhältnis-mäßigkeit**	Hier findet etwa die aus dem deutschen Verfassungsrecht bekannte Verhältnismäßigkeitsprüfung statt, die das Interesse von Personal-aktiv (Rechtfertigungsrechtsgut) und das Interesse des Personal-passiv Datenschutzes (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 10 GG, Art. 13 GG) und das Interesse der Personal-passiv Informationskosten (Art. 12, 14, 2 Abs. 1 GG) abwägt.

VIII. SI²S – aktualisiert (11/2018)
2. Abstrakt – Differenzierung „Objekt" (SI²S – 3): „Personenbezogene Daten" im „Mehrebenenmodell"

TECHNISCHE UNIVERSITÄT DARMSTADT

a) EU

Art. 4 Nr. 1 EU-DSGVO / Art. 3 Nr. 1 EU-DSGRL

Begriffsbestimmungen

[...] 1. „**personenbezogene Daten**" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann [...]

b) BRD und Hessen

§ 46 Nr. 1 BDSG / § 41 Nr. 1 HDSIG

Begriffsbestimmungen

[...] 1. „**personenbezogene Daten**" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann [...]

TECHNISCHE UNIVERSITÄT DARMSTADT

c) Unterschiede im europäischen und deutschen Bundes- und Landesrecht?

Eine Synopse wie vergleichende Analyse ergibt, dass die Unterschiede in grammatischer Auslegung minimal sind und die rechtliche Relevanz dieser Unterschiede **derzeit nicht evident** ist. Die folgenden Folien heben die Unterschiede durch Unterstreichungen hervor.*

* Einmal ergänzt das Recht der EU den Wortlaut in einer Klammer um „im Folgenden" und zum anderen wird im deutschen Bundes- und Landerecht das Adjektiv „natürlich" nicht wiedergegeben.

VIII. SI²S – aktualisiert (11/2018)
2. Abstrakt – Differenzierung „Objekt"(SI²S – 3): „Personenbezogene Daten" im „Mehrebenenmodell"

TECHNISCHE UNIVERSITÄT DARMSTADT

c) Unterschiede im europäischen und deutschen Bundes- und Landesrecht?

Art. 4 Nr. 1 EU-DSGVO / Art. 3 Nr. 1 EU-DSGRL

Begriffsbestimmungen

[...] 1. „**personenbezogene Daten**" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann [...]

§ 46 Nr. 1 BDSG / § 41 Nr. 1 HDSIG

Begriffsbestimmungen

[...] 1. „**personenbezogene Daten**" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann [...]

* Die Unterstreichungen heben die Abweichungen der verschiedenen Normtexte hervor.

VIII. 3. Abstrakt – Differenzierung „Objekt"(SI²S – 3): „Besondere Kategorien personenbezogener Daten" im „Mehrebenenmodell"

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 9 Abs. 1 EU-DSGVO / Art. 10 EU-DSGRL*

Verarbeitung besonderer Kategorien personenbezogener Daten

[…] personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie […] genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung [...]

§ 46 Nr. 14 BDSG / § 41 Nr. 15 HDSIG*

Begriffsbestimmungen

[...] **besondere Kategorien personenbezogener Daten**
a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
b) genetische Daten,
c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
d) Gesundheitsdaten und
e) Daten zum Sexualleben oder zur sexuellen Orientierung […]

* Abweichend ist lediglich die Art der Darstellung, nicht der Normtext.

VIII. 3. Abstrakt – Differenzierung „Objekt"(SI²S – 3): „Besondere Kategorien personenbezogener Daten" im „Mehrebenenmodell"

TECHNISCHE UNIVERSITÄT DARMSTADT

Legaldefinitionen: genetische-, biometrische- und Gesundheitsdaten

Art. 4 Nr. 13–15 EU-DSGVO / Art. 3 Nr. 12–14 EU-DSGRL / § 46 Nr. 11–13 BDSG / § 41 Nr. 12–14 HDSIG

Begriffsbestimmungen

[...] **genetische Daten** personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden [...]

[...] **biometrische Daten** mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten [...]

[…] **Gesundheitsdaten** personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen […]

VIII. 4. Abstrakt – Differenzierung „Objekt"(SI²S – 3): „Informationstechnologisches Sicherheitsrecht" (eigene Terminologie) im „Mehrebenenmodell"

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 10 EU-DSGVO

Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

VIII. 4. Abstrakt – Differenzierung „Objekt"(SI²S – 3): „Informationstechnologisches Sicherheitsrecht " (eigene Terminologie) im „Mehrebenenmodell"

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 6 EU-DSGRL Unterscheidung verschiedener Kategorien betroffener Personen	§ 72 BDSG / § 67 HDSIG Unterscheidung zwischen verschiedenen Kategorien betroffener Personen
Die Mitgliedstaaten sehen vor, dass der Verantwortliche gegebenenfalls und so weit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen klar unterscheidet, darunter: a) Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden, b) verurteilte Straftäter, c) Opfer einer Straftat oder Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und d) andere Parteien im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den unter den Buchstaben a und b genannten Personen in Kontakt oder in Verbindung stehen.	Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Dies betrifft insbesondere folgende Kategorien: 1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben, 2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden, 3. verurteilte Straftäter, 4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und 5. andere Personen wie insbesondere [Zeuginnen und]* Zeugen, [Hinweisgeberinnen und]* Hinweisgeber oder Personen, die mit den in den Nummern 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen. * Nur im HDSIG.

VIII. 5. Abstrakt – Differenzierung „Kausal/Zweck“ (SI²S – 4): Gefahrenbegriffe in Hessen und Bayern

TECHNISCHE UNIVERSITÄT DARMSTADT

§ 11 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) – Allgemeine Befugnisse

Die Gefahrenabwehr- und die Polizeibehörden können die erforderlichen Maßnahmen treffen, um **eine im einzelnen Falle bestehende Gefahr für die öffentliche Sicherheit oder Ordnung (Gefahr)** abzuwehren, soweit nicht die folgenden Vorschriften die Befugnisse der Gefahrenabwehr- und der Polizeibehörden besonders regeln.

Art. 11 Abs. 1 und 3 Bayrisches Polizeiaufgabengesetz (BayPAG) – Allgemeine Befugnisse

(1) Die Polizei kann die notwendigen Maßnahmen treffen, um **eine im einzelnen Fall bestehende Gefahr für die öffentliche Sicherheit oder Ordnung (Gefahr)** abzuwehren, soweit nicht die Art. 12 bis 65 die Befugnisse der Polizei besonders regeln.

(2) [...]

(3) Die Polizei kann unbeschadet der Abs. 1 und 2 die notwendigen Maßnahmen treffen, um den Sachverhalt aufzuklären und die Entstehung einer Gefahr für ein bedeutendes Rechtsgut zu verhindern, wenn im Einzelfall

1. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet oder

2. Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen den **Schluss auf ein seiner Art nach konkretisiertes Geschehen zulassen,**

wonach in absehbarer Zeit Angriffe von erheblicher Intensität oder Auswirkung zu erwarten sind (drohende Gefahr), soweit nicht die Art. 12 bis 65 die Befugnisse der Polizei besonders regeln. Bedeutende Rechtsgüter sind:

1. der Bestand oder die Sicherheit des Bundes oder eines Landes,

2. Leben, Gesundheit oder Freiheit,

3. die sexuelle Selbstbestimmung,

4. erhebliche Eigentumspositionen oder

5. Sachen, deren Erhalt im besonderen öffentlichen Interesse liegt.

VIII. 5. Abstrakt – Differenzierung „Kausal/Zweck“ (SI²S – 4): Gefahrenbegriffe in Hessen und Bayern

TECHNISCHE UNIVERSITÄT DARMSTADT

Didaktik: „Kausal/Zweck“ (SI²S – 4) und Verhältnismäßigkeit (SI²S – 7)

Grundsätzlich ist die Ermittlung von „Kausal/Zweck“ wegweisend wie aufbauend für die Argumentation und Prüfung der einzelnen Schritte der Analyse der Verhältnismäßigkeit im weiteren Sinne (SI²S – 7). Die Identifizierung von „Kausal/Zweck“ bereitet die Ermittlung des „Rechtfertigungsrechtsguts“ (eigene Terminologie) vor.

Im Kontext des „informationstechnologischen Sicherheitsrechts“ hat die Veränderung des „Gefahrenbegriffs“ **Kernbedeutung**.

TECHNISCHE UNIVERSITÄT DARMSTADT

a) Didaktische Terminologie: „Drohnen" statt „unbemannte Luftfahrtsysteme"

Soweit ersichtlich hat Bayern als einziges Bundesland eine spezielle polizeirechtliche Ermächtigungsgrundlage (grammatische Auslegung) für den „Drohnen"einsatz geschaffen. Hervorzuheben ist, dass die Rechtssprache „Drohnen" nicht kennt – sondern stattdessen „unbemannte Luftfahrtsysteme" erfasst. Weil die Definition im Luftverkehrsrecht nicht übersichtlich ist (etwa Multicopter in der systematischen Auslegung von § 21b Abs. 1 Nr. 8b LuftVO; § 1 LuftVG) wird im Folgenden an der gebräuchlichen wie umgangssprachlichen Terminologie „Drohnen" vorläufig festgehalten.

VIII. 6. Abstrakt – Differenzierung Qualität der Information(stechnik) „Personal–aktiv Informationsrecht“ (SI²S – 5b)

TECHNISCHE UNIVERSITÄT DARMSTADT

b) „Unbemannte Luftfahrtsysteme“ im Bayrischen Polizeiaufgabengesetz

Art. 47 BayPAG – Einsatz von unbemannten Luftfahrtsystemen

(1) Bei den nachfolgenden Maßnahmen dürfen Daten unter den dort genannten Voraussetzungen auch durch den Einsatz unbemannter Luftfahrtsysteme erhoben werden:

1. offene Bild- und Tonaufnahmen oder -aufzeichnungen nach Art. 33 Abs. 1 bis 3,
2. Einsatz besonderer Mittel der Datenerhebung nach Art. 36 Abs. 1,
3. Einsatz technischer Mittel in Wohnungen nach Art. 41 Abs. 1,
4. Eingriffe in den Telekommunikationsbereich nach Art. 42 Abs. 1 bis 5 und
5. verdeckter Zugriff auf informationstechnische Systeme nach Art. 45 Abs. 1 und 2.

(2) In den Fällen des Abs. 1 Nr. 1 dürfen unbemannte Luftfahrtsysteme nur dann eingesetzt werden, wenn die Offenheit der Maßnahme gewahrt bleibt. In diesen Fällen soll auf die Verwendung unbemannter Luftfahrtsysteme durch die Polizei gesondert hingewiesen werden.

(3) Soweit in den Fällen des Abs. 1 eine richterliche Anordnung erforderlich ist, muss diese auch den Einsatz von unbemannten Luftfahrtsystemen umfassen.

(4) Diese unbemannten Luftfahrtsysteme dürfen nicht bewaffnet werden.

c) FEX: „Drohnen"einsatz in anderen Bundesländern

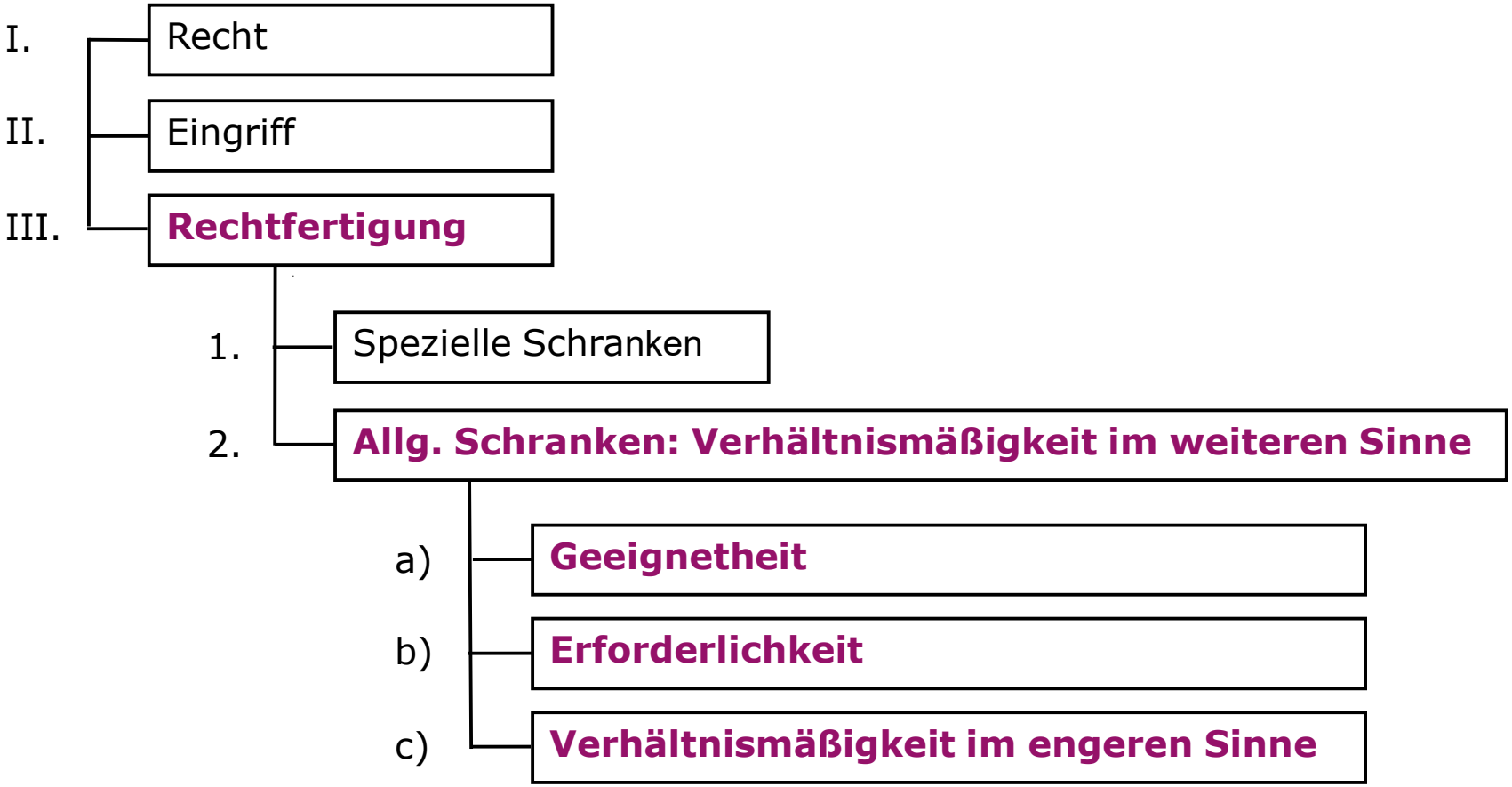
Vertiefend ist darauf hinzuweisen, dass aus der Abwesenheit einer speziellen Regelung in anderen Polizei- und Sicherheitsgesetzen nicht geschlossen werden kann, dass ein „Drohnen"einsatz rechtlich ausgeschlossen ist. Hier kommen theoretisch und wissenschaftlich allgemeine Ermächtigungsgrundlagen (sog. polizeirechtliche Generalklauseln) oder die Ermächtigungsgrundlagen für Bild- und Videoaufnahmen in Betracht (vgl. §§ 11, 14, 15 HSOG).

Insoweit ist vorhersehbar, dass eine weitere wissenschaftliche und rechtliche Klärung – jenseits dieser Basics – erfolgen wird.

VIII. Schema für die Interessenanalyse Informationstechno-logischer Sachverhalte (SI²S) in der Tradition seit 2013/2003 – aktualisiert (11/2018)
7. Konkret

		Analyse
1	**Personal-aktiv**	Behörde (Ermächtigungsgrundlage?)
2 a)	**Personal-passiv** Datenschutz	Universität (Behörde) Studierende
2 b)	**Personal-passiv** Informationskosten	Universität (Kosten der Amtshilfe)
3	**Objekt**	Daten über Ausländer arabischer Herkunft – (Besondere personenbezogene Daten, Art. 9 Abs. 1 EU-DSGVO / Art. 10 EU-DSGRL / § 46 Nr. 14 BDSG / § 41 Nr. 15 HDSIG)
4	**Kausal/Zweck**	Terrorismusbekämpfung
5 a), b)	**Qualität der Informationstechnik**	Datenorganisation Erhebung durch die Universität Übermittlung von Universität an Behörde (keine Angaben im Sachverhalt zu 5 a) u. b)
6	**Verfahren**	Besondere Verfahrens- und Formvorschriften in der StPO und den Polizeigesetzen
7	**Rechtfertigung/ Verhältnismäßigkeit**	Abwägung des Interesses von Personal-aktiv (Rechtfertigungsrechtsgut (Öffentliche Sicherheit)) mit dem Interesse des Personal-passiv (Eingriffsrechtsgut (Recht auf informationelle Selbstbestimmung))

IX. RER-Schema



X. RER-Definition
1. Spezielle Schranken

„Spezielle Schranken“ sind solche Schranken, die im Normtext (hier GG) genannt sind oder kraft Auslegung die Grundrechts-verwirklichung einschränken (etwa im Wege der Konkordanz oder der Wechselwirkung).

X. RER-Definition
2. Allgemeine Schranken: Verhältnismäßigkeit im weiteren Sinn

TECHNISCHE UNIVERSITÄT DARMSTADT

Geeignetheit	Eingriff muss geeignet sein, um den Schutz des Rechtsguts, das die Eingriffsrechtsfertigung bildet (**Rechtfertigungsrechtsgut - eigene Terminologie**), zu bewirken. → Tauglichkeit des Mittels für den Zweck.
Erforderlichkeit	Es darf keine Eingriffsmaßnahme geben, die für den Schutz des „Rechtfertigungsrechtsguts" genauso geeignet und weniger eingreifend ist.
Verhältnismäßigkeit im engeren Sinn	Schwere des Eingriffs in das Eingriffsrechtsgut (eigene Terminologie) darf nicht außer Verhältnis zur Qualität der Förderung des Rechtfertigungsrechtsguts stehen. → Grundrechtseingriff darf in seiner Intensität nicht außer Verhältnis zum angestrebten Ziel stehen.

XI. RER-Prüfung
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 Staatsangehörigkeit und die Studienrichtung haben offensichtlich Bezug zum allgemeinen Persönlichkeitsrecht. (Gegenbeispiel: Mitteilung der Anzahl der Studierenden im Fachbereich 1 „Wirtschaftsinformatik".)

Bei Daten über „Ausländer arabischer Herkunft" handelt es sich um Angaben, die Rückschlüsse etwa auf die die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen (Art. 3 Nr. 1, Art. 10 EU-DSGRL*) zulassen. Insoweit ist ein **besonderer Menschenwürdebezug** (Art. 1 Abs. 1 GG) gegeben.

XI. RER-Prüfung
1. Recht

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 3 Nr. 1 EU-DSGRL – Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck:

1. „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

Art. 10 EU-DSGRL - Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung ist nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und

a) wenn sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist

b) der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder

c) wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.

XI. RER-Prüfung
1. Recht

TECHNISCHE UNIVERSITÄT DARMSTADT

Art. 2 Abs. 1 GG

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

Art. 1 Abs. 1 GG

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

XI. RER-Prüfung
2. Eingriff

TECHNISCHE UNIVERSITÄT DARMSTADT

Der Eingriffsbegriff ist immer vor dem Hintergrund des betroffenen Grundrechts zu entwickeln.
BVerfG im Volkszählungsurteil (in der FÖR-Interpretation): Jeder hat ein Recht zu **wissen,** wer, wann, wofür, wo, welche personenbezogenen Daten „organisiert" und muss grundsätzlich **einwilligen.**

FÖR-Terminologie und Sophistikation: „w⁶"
Jeder hat ein Recht **zu wissen, wer, wann, wofür, wo, welche** personenbezogenen Daten „organisiert" und muss grundsätzlich einwilligen bzw. es bedarf einer „gesetzlichen" Ermächtigung **(„w⁶")**.

- 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.

XI. RER-Prüfung – 3. Rechtfertigung
a) Terminologie

„Spezielle Schranken" sind solche Schranken, die im Normtext (hier GG) genannt sind oder kraft Auslegung die Grundrechtsverwirklichung einschränken (etwa im Wege der Konkordanz oder der Wechselwirkung).

TECHNISCHE UNIVERSITÄT DARMSTADT

Spezielle Schranke: Art. 2 Abs. 1 GG

➢ Diese Schranke ist in einer grammatischen Auslegung der jeweiligen Norm, hier der Verfassung, zu entnehmen: Art. 2 Abs. 1 GG: „Rechte anderer", „verfassungsmäßige Ordnung" oder das „Sittengesetz".

FÖR-Strategie: 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).

FÖR-Terminologie: Umschreibung für „Gesetzesvorbehalt"*

* Vgl. auch Di Fabio in: Maunz/Dürig, Grundgesetz Kommentar, Art. 2 Abs. 1, Rn. 37, 38.

XI. RER-Prüfung – 3. Rechtfertigung
b) Spezielle Schranke: Verfassungsmäßige Ordnung

TECHNISCHE UNIVERSITÄT DARMSTADT

Formelle und materielle Verfassungsmäßigkeit der **Rechtsgrund-lage**:

- **Formelle Verfassungsmäßigkeit** setzt die Einhaltung der

  Kompetenz-,
  Verfahrens- und
  Formvorschriften voraus. (**KVF-Prüfung)**

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

XI. RER-Prüfung – 3. Rechtfertigung
b) Spezielle Schranke: Verfassungsmäßige Ordnung

TECHNISCHE UNIVERSITÄT DARMSTADT

<table>
<tr><td rowspan="11">Teil 1: Zulässigkeit</td><td colspan="3">Teil 2: Begründetheit</td></tr>
<tr><td colspan="2">A. Formelle Rechtmäßigkeit</td><td>B. Materielle Rechtmäßigkeit</td></tr>
<tr><td colspan="2">I. Kompetenz</td><td>I. Verfassungsprinzipien</td></tr>
<tr><td colspan="2">II. Verfahren</td><td>II. Grundrechtsprüfung</td></tr>
<tr><td colspan="2">III. Form</td><td>(1) Recht</td></tr>
<tr><td colspan="2" rowspan="5"></td><td>(2) Eingriff</td></tr>
<tr><td>(3) Rechtfertigung</td></tr>
<tr><td colspan="2">Spezielle Schranke: „verfassungsmäßige Ordnung“: sämtliche Rechtsnormen, die mit der Verfassung formell und materiell in Einklang stehen (formell und materiell rechtmäßig sind)</td></tr>
<tr><td>a) Formelle Rechtmäßigkeit</td><td>b) Materielle Rechtmäßigkeit</td></tr>
<tr><td>Hier kann auf A. verwiesen werden</td><td>aa) Geeignetheit</td></tr>
<tr><td></td><td>bb) Erforderlichkeit</td></tr>
<tr><td></td><td>cc) Verhältnismäßig-keit im engeren Sinne</td></tr>
</table>

TECHNISCHE UNIVERSITÄT DARMSTADT

Rechtsgrundlage für die Rasterfahndung

§ 26 Abs. 1 HSOG, Besondere Formen des Datenabgleichs

(1) Die Polizeibehörden können von öffentlichen Stellen oder nichtöffentlichen Stellen zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn 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 dies zur Abwehr der Gefahr erforderlich ist. Eine solche Gefahr liegt in der Regel auch dann vor, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass terroristische Straftaten begangen werden sollen. Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.

XI. RER-Prüfung – 3. Rechtfertigung
b) Spezielle Schranke: Verfassungsmäßige Ordnung

TECHNISCHE UNIVERSITÄT DARMSTADT

Formelle und materielle Verfassungsmäßigkeit der **Rechtsgrundlage**:

- **Formelle Verfassungsmäßigkeit** setzt die Einhaltung der

  Kompetenz-,
  Verfahrens- und
  Formvorschriften voraus. (**KVF-Prüfung)**

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

TECHNISCHE UNIVERSITÄT DARMSTADT

aa) Formelle Verfassungsmäßigkeit von § 26 HSOG: Kompetenz

Art. 70 Abs. 1 GG

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

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 […] auswärtige Belange der Bundesrepublik Deutschland gefährden,

sowie die Einrichtung eines Bundeskriminalpolizeiamtes und die internationale Verbrechensbekämpfung; […]

TECHNISCHE UNIVERSITÄT DARMSTADT

bb) und cc) Formelle Verfassungsmäßigkeit von § 26 HSOG: Verfahren und Form

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

Von der formellen Verfassungsmäßigkeit des § 26 HSOG ist auszugehen.

TECHNISCHE UNIVERSITÄT DARMSTADT

dd) 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 Verhältnismäßigkeits-grundsatzes im weiteren Sinne – verlangt.

Bei der Prüfung der Rechtfertigung nach Art. 2 Abs. 1 GG mündet also die spezielle Schranke unmittelbar in die allgemeine Schranke. In der Gliederungsstruktur wird deswegen in Anschluss an 3a dd) die Prüfung der allgemeinen Schranke unter 4. fortgesetzt.

FEX-Prüfungsstrategie: Grundsätzlich verlangt die allgemeine Schranke mit ihren Abwägungsanforderungen komplexe und differenzierte Ausführungen. Diese komplexe Prüfung wird durch den Aufbau und die Aufteilung nach Recht (1.), Eingriff (2.) und Rechtfertigung (3.) – spezielle Schranke – vorbereitet. Die rechtliche Gesamtbewertung wird mit der Prüfung der allgemeinen Schranke abgeschlossen (4.).

TECHNISCHE UNIVERSITÄT DARMSTADT

aa) 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 Datenorganisations-systems geeignet ist Anschläge zu verhindern (siehe USA).

TECHNISCHE UNIVERSITÄT DARMSTADT

bb) 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.

TECHNISCHE UNIVERSITÄT DARMSTADT

cc) Verhältnismäßigkeit im engeren Sinne

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

➢ **Für** eine Schwere des Eingriffs:

- Argumentation mit der Streubreite

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

- Argumentation mit der „Heimlichkeit" der Datenerhebung

  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.

TECHNISCHE UNIVERSITÄT DARMSTADT

cc) Verhältnismäßigkeit im engeren Sinne

➢ **Für** eine Schwere des Eingriffs:

- Argumentation mit der Betroffenheit sensibler Daten (Art. 10 sowie Erwägungsgründe 37, 51 EU-DSGRL)
- Argumentation mit der fehlenden Qualität des Verfahrens der Datenorganisation: 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). Dasselbe gilt für die repressive Rasterfahndung nach der Strafprozessordnung.

TECHNISCHE UNIVERSITÄT DARMSTADT

cc) Verhältnismäßigkeit im engeren Sinne

- **Gegen** eine Schwere des Eingriffs:

  Argumentation der prozessbedingten geringen 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.

TECHNISCHE UNIVERSITÄT DARMSTADT

cc) Verhältnismäßigkeit im engeren Sinne

- **Für** eine qualitative Förderung des Rechtfertigungsrechtsguts:
  Argumentation mit dem gestiegenen terroristischen Bedrohungspotenzial:
  Durch die aktuelle politische Weltlage (Irak, Afghanistan, Anschläge in Madrid, Istanbul, Syrien… (ohne Wertung in der Reihenfolge)) könnte eine erhöhte Gefahr bestehen, dass Terroristen auch in Deutschland Anschläge vorbereiten. Universitäten könnten hierzu sowohl zu Kontaktzwecken als auch zur Know-How-Erlangung genutzt werden.

TECHNISCHE UNIVERSITÄT DARMSTADT

cc) Verhältnismäßigkeit im engeren Sinne

- **Gegen** eine qualitative Förderung des Rechtfertigungsrechtsguts:
  Argumentation mit der nur hypothetischen Effektivität der Rasterfahndung:
  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 abzuwarten.

TECHNISCHE UNIVERSITÄT DARMSTADT

cc) Verhältnismäßigkeit im engeren Sinne

- **Gegen** eine qualitative Förderung des Rechtfertigungsrechtsguts:
  Argumentation mit dem geringen Gefährdungspotenzial:
  Im Anschluss an den 11. September 2001 mag die Gefahr eines weiteren Angriffs (geistig) präsent und das Gefährdungspotenzial sehr hoch gewesen sein. Nicht erst die im Laufe der Zeit erschienen Dokumente – etwa im Zusammenhang mit dem Irak-Krieg – die zeigen, wie ein Gefährdungspotenzial zu politischen Zwecken miss-braucht werden kann.

XII. Falllösung
1. „Klassisch" seit 2003

TECHNISCHE UNIVERSITÄT DARMSTADT

- Eine präventive Rasterfahndung kann je nach Konkretisierung des Verdachts und Differenzierung der Fahndungskriterien dazu führen, dass auch „Otto-Normalbürgern" das Stigma eines „Terroristen" „verliehen" wird.
- Darüber hinaus ist die Rasterfahndung ein weiterer Schritt zur virtuellen Erfassung der Persönlichkeit von Menschen.
- Die Chancen einer Rasterfahndung können kontrovers beurteilt werden.
- Vielleicht sollte die Rasterfahndung von einem Richtervorbehalt abhängig gemacht werden, der sich auf einzelne Daten-„organisations"prozesse erstreckt.

→ Somit könnte die Rasterfahndung und die Datenorganisation bei der Universität nicht gerechtfertigt sein und gegen das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) verstoßen.

XII. Falllösung
2. Entscheidungen aus der Vergangenheit

TECHNISCHE UNIVERSITÄT DARMSTADT

- BVerfG, Beschl.v. 04.04.2006, 1 BvR 518/02
- VGH Kassel, Beschl.v. 04.02.2003, 10 TG 3112/02 (Juris)
- OVG Koblenz, Beschl.v. 22.03.2002, 12 B 10331/02 (Juris)
- VG Trier, Beschl.v. 11.06.2002, 1 L 620/02 (Juris)
- OVG Bremen, Beschl.v. 08.07.2002, 1 B 155/02 (Juris)
- VG Gießen, Beschl.v. 08.11.2002, 10 G 4510/02 (Juris)
- VG Wiesbaden, Beschl.v. 31.03.2003, 5 G 1883/02 (Juris)

XIII: Change Management

1. Hessen: Rechtsgrundlage der Rasterfahndung heute – früher*

§ 26 Abs. 1 HSOG – Besondere Formen des Datenabgleichs

TECHNISCHE UNIVERSITÄT DARMSTADT

Ab 04.07.2018	**23.12.2009 bis 03.07.2018**
(1) [1]Die Polizeibehörden können von öffentlichen Stellen oder **nichtöffentlichen Stellen** zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes **oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,** oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind, die Übermittlung von personenbezogenen Daten bestimmter Personen-gruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn dies zur Abwehr der Gefahr erforderlich ist. **[2]Eine solche Gefahr liegt in der Regel auch dann vor, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass terroristische Straftaten begangen werden sollen.** [3]Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.	(1) [1]Die Polizeibehörden können von öffentlichen Stellen oder **Stellen außerhalb des öffentlichen Bereichs** zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes **oder für Leben, Gesundheit oder Freiheit** oder wenn 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 dies zur Abwehr der Gefahr erforderlich ist. [2]Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.

* Die Unterstreichungen heben die Abweichungen der verschiedenen Normtexte hervor. Berücksichtigt wurden die letzten 3 Geltungszeiträume (ab 04.07.2018, 25.05.2018–03.07.2018, 23.12.2009–24.05.2018). Abs. 2 enthält keine Änderungen.

XIII: Change Management

1. Hessen: Rechtsgrundlage der Rasterfahndung heute – früher § 26 Abs. 3 HSOG – Besondere Formen des Datenabgleichs

TECHNISCHE UNIVERSITÄT DARMSTADT

Ab 25.05.2018	**23.12.2009 bis 24.05.2018**
(3) [1]Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten auf dem Datenträger zu löschen und die Unterlagen, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, unverzüglich zu vernichten. **[2]Die getroffenen Maßnahmen sind zu dokumentieren. [3]Diese Dokumentation ist gesondert aufzubewahren und durch technische und organisatorische Maßnahmen zu sichern. [4]Sie ist sechs Monate nach der Benachrichtigung nach § 29 Abs. 5 oder nach dem endgültigen Zurückstellen der Benachrichtigung nach § 29 Abs. 6 zu löschen; ist die Datenschutzkontrolle nach § 29a noch nicht beendet, ist die Dokumentation bis zu deren Abschluss aufzubewahren.**	(3) [1]Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten auf dem Datenträger zu löschen und die Unterlagen, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, unverzüglich zu vernichten. **[2]Über die getroffenen Maßnahmen ist eine Niederschrift anzufertigen. [3]Diese Niederschrift ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Vernichtung der Unterlagen nach Satz 1 folgt, zu vernichten.**

XIII: Change Management

1. Hessen: Rechtsgrundlage der Rasterfahndung heute – früher § 26 Abs. 4 u. 5 HSOG – Besondere Formen des Datenabgleichs

TECHNISCHE UNIVERSITÄT DARMSTADT

Ab 04.07.2018	**25.05.2018 bis 03.07.2018**	**23.12.2009 bis 24.05.2018**
(4) [1]Die Maßnahme darf nur aufgrund **richterlicher Anordnung auf Antrag der Behördenleitung getroffen werden. [2]Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. [3]Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit vom 17. Dezember 2008 (BGBl. I S. 2586, 2587), zuletzt geändert durch Gesetz vom 20. Juli 2017 (BGBl. I S. 2780), entsprechend.** [4]Die oder der Hessische Datenschutzbeauftragte ist **durch die Polizeibehörde unverzüglich über die Anordnung** zu unterrichten.	(4) [1]Die Maßnahme **nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums.** [2]Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte unverzüglich zu unterrichten.	(4) [1]Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums. [2]Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte unverzüglich zu unterrichten. **(5) [1]Personen, gegen die nach Abschluss einer Maßnahme nach Abs. 1 weitere Maßnahmen durchgeführt werden, sind hierüber durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zweckes der weiteren Datennutzung erfolgen kann. [2]§ 29 Abs. 6 Satz 4 und 5 und Abs. 7 gilt entsprechend.**

XIII: Change Management

2. BRD: Rechtsgrundlagen der Rasterfahndung als ein traditionelles Kernelement des „informationstechnologischen Sicherheitsrechts" (eigene Terminologie)

TECHNISCHE UNIVERSITÄT DARMSTADT

04.07.2018 – Hessen

25.05.2018 – Bayern

08.07.2017 – Rheinland-Pfalz

28.07.2015 – Bremen

01.05.2015 – Schleswig-Holstein

21.04.2015 – Berlin

19.12.2014 – Saarland

30.04.2014 – Hamburg

17.10.2013 – Sachsen-Anhalt

28.09.2013 – Thüringen

01.01.2013 – Sachsen

29.11.2012 – Baden-Württemberg

20.12.2011 – Brandenburg

01.04.2011 – Mecklenburg-Vorpommern

24.02.2010 – Nordrhein-Westfalen

01.01.2008 – Niedersachsen

FEX (I): Sicherheitsgesetzgebung in Deutschland – im Auszug

TECHNISCHE UNIVERSITÄT DARMSTADT

- Im Kontext der „Rasterfahndung" wird etwa auf den Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland vom 28.08.2013 hingewiesen.
- Hinzuweisen ist des Weiteren auf den Erlass des **Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus vom 26. Juli 2016** (BGBl. I Nr. 37 v. 29.07.2016, S. 1818) – sog. **Antiterrorpaket**.
- Aktuelle Entwicklungen: Maßnahmenpaket zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 18.10.2019, unter anderem soll diese die Identifizierung bei Hasskriminalität im Netzverbessern und die Strafbarkeit von Cyber-Stalking, Hetze und aggressiver Beleidigung anpassen.

FEX (I): Sicherheitsgesetzgebung in Deutschland – im Auszug

TECHNISCHE UNIVERSITÄT DARMSTADT

- Dieses (Artikel-)Gesetz änderte u.a. folgende Gesetze:
- Bundesverfassungsschutzgesetz (Art. 1 G. v. 26.07.2016)
- BND-Gesetz (Art. 2 G. v. 26.07.2016)
- Bundespolizeigesetz (Art. 3 G. v. 26.07.2016)
- Artikel 10-Gesetz (Art. 5 G. v. 26.07.2016)
- BKA-Gesetz (Art. 7 G. v. 26.07.2016)
- StGB (Art. 8 G. v. 26.07.2016)
- TKG (Art. 9 G. v. 26.07.2016)

FEX (II): BVerfG – Sicherheitsrechtsprechung zur Rasterfahndung in Deutschland (2016)

TECHNISCHE UNIVERSITÄT DARMSTADT

Verfassungswidrige Rechtsgrundlage für die Rasterfahndung im BKA-Gesetz vom 01.01.2009 bis 24.05.2018 ?

Durch das Urteil des BVerfG vom 20.04.2016, Az.1 BvR 966/09 u. 1 BvR 1140/09 – „BKA-Gesetz" wurde § 20j Abs. 3 S. 3 BKAG a.F. bezüglich der Regelung zur Aufbewahrung der sogenannten Löschprotokolle für **nicht vereinbar mit der Verfassung** erklärt (siehe Urteilstenor zu 3 sowie Rn. 272, 273.).

§ 20j BKAG a.F. war jedoch bis zu einer Neuregelung, die am 25.05.2018 in Kraft getreten ist, (längstens jedoch bis zum 30.06.2018 laut BVerfG) **weiter anwendbar** (siehe Urteilstenor zu 4.).

Dass § 20j Abs. 3 S. 3 BKAG a.F. für „lediglich" mit der Verfassung unvereinbar, nicht jedoch für verfassungswidrig und nichtig erklärt würde, begründete das BVerfG damit, dass die Verfassungswidrigkeit dieser Vorschriften „nicht den Kern der mit ihnen eingeräumten Befugnisse, sondern nur einzelne Aspekte ihrer rechtsstaatlichen Ausgestaltung" betreffe, sodass der Gesetzgeber entsprechend nachbessern könne (Rn. 357). Konkret gerügt wurden etwa zu kurze Fristen zur Löschung der Löschprotokolle (§ 20j Abs. 3 S. 3 BKAG a.F.) (Rn. 272 f.).

FEX (II): BVerfG – Sicherheitsrechtsprechung zur Rasterfahndung in Deutschland (2016)

TECHNISCHE UNIVERSITÄT DARMSTADT

Verfassungswidrige Rechtsgrundlage für die Rasterfahndung im BKA-Gesetz*?

Rasterfahndung (§ 20j BKAG a.F.)

(1) Das Bundeskriminalamt kann von öffentlichen oder nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten von bestimmten Personengruppen aus Dateien zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist, erforderlich ist; eine solche Gefahr liegt in der Regel auch dann vor, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 4a Abs. 1 Satz 2 begangen werden soll. Von den Verfassungsschutzämtern des Bundes und der Länder, dem Militärischen Abschirmdienst sowie dem Bundesnachrichtendienst kann die Übermittlung nach Satz 1 nicht verlangt werden.

Abs. 2-4 auf nächsten Folien

* Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Artikel 1 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminal-polizeilichen Angelegenheiten) (Bundeskriminalamtgesetz - BKAG) vom 7. Juli 1997 (BGBl. I S. 1650), das durch Artikel 7 des Gesetzes vom 26. Juli 2016 (BGBl. I S. 1818) geändert worden ist.

FEX (II): BVerfG – Sicherheitsrechtsprechung zur Rasterfahndung in Deutschland (2016)

TECHNISCHE UNIVERSITÄT DARMSTADT

Verfassungswidrige Rechtsgrundlage für die Rasterfahndung im BKA-Gesetz?

Rasterfahndung (§ 20j BKAG a.F.)

(2) Das Übermittlungsersuchen ist auf Namen, Anschrift, Tag und Ort der Geburt sowie auf andere im Einzelfall festzulegende Merkmale zu beschränken; es darf sich nicht auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Von Übermittlungsersuchen nicht erfasste personenbezogene Daten dürfen übermittelt werden, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwands eine Beschränkung auf die angeforderten Daten nicht möglich ist; diese Daten dürfen vom Bundeskriminalamt nicht verwendet werden.

Abs. 3 u. 4 auf nächster Folie

FEX (II): BVerfG – Sicherheitsrechtsprechung zur Rasterfahndung in Deutschland (2016)

TECHNISCHE UNIVERSITÄT DARMSTADT

Verfassungswidrige Rechtsgrundlage für die Rasterfahndung im BKA-Gesetz?

Rasterfahndung (§ 20j BKAG a.F.)

(3) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen und die Akten zu vernichten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind. Die getroffene Maßnahme ist zu dokumentieren. **Diese Dokumentation ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Löschung der Daten oder der Vernichtung der Akten nach Satz 1 folgt, zu vernichten.**

(4) Die Maßnahme darf nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden.

FEX (III): Sicherheitsgesetzgebung in Deutschland (2018) – Rasterfahndung

TECHNISCHE UNIVERSITÄT DARMSTADT

- Aufgrund des Urteils des Bundesverfassungsgericht wurde das BKAG überarbeitet und neustrukturiert.*
- Diese Änderungen traten am 25.05.2018 in Kraft (Art. 13 Abs. 1).
- Die Rasterfahndung (§ 48 BKAG) befindet sich nunmehr in Abschnitt 5 (Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus)
- Geändert wurde lediglich die Vorschrift über die Aufbewahrung der Löschprotokolle (§ 48 Abs. 3 S. 4 f.)

Rasterfahndung (§ 48 BKAG)

(3) [...] Sie ist sechs Monate nach der Benachrichtigung nach § 74 oder sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutzkontrolle nach § 69 Absatz 1 noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

* Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 01.07.2017, BGBl. 2017 Teil I Nr. 33, S. 1354 ff.

Cyberlaw

Basics in der Tradition seit 2003 (aktualisiert 12/2019)

„Cluster II"

Anhang I: Gliederung des „Cluster I“

TECHNISCHE UNIVERSITÄT DARMSTADT

A. Rahmenbedingungen

I. Vorlesungsetikette
II. Organisatorisches
III. Literatur

B. Basics

Teil I:

I. Rechtsnormenhierarchie
II. Klassische Auslegungsmethoden
III. Recht auf informationelle Selbstbestimmung
IV. Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
V. Rasterfahndung nach dem 11. September