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

TECHNISCHE UNIVERSITÄT DARMSTADT

Basics für Cyberlaw

DEMONSTRATOR:

Rasterfahndung

(SI²S & RER-Prüfung)

in der Tradition seit 2003

(Work in Progress)

Wintersemester 2023/2024

Agenda – Schnellübersicht projektiert:

TECHNISCHE UNIVERSITÄT DARMSTADT

Dreiteiliger Foliensatz:

A. **Konturen des „Didaktikinkubators“**
B. **Basics für Cyberlaw - DEMONSTRATOR: Rasterfahndung (SI²S & RER-Prüfung)**
C. **Basics für Cyberlaw - SI²S & Informationsobjekte (Datenkategorien)**

Agenda – Schnellübersicht
Work in Progress und Tradition

TECHNISCHE UNIVERSITÄT DARMSTADT

Es handelt sich um einen Foliensatz, der seit 2003 erweitert wurde. Auch die Versionen in 2023 weisen nur geringe redaktionelle Veränderungen auf. Insbesondere bei den Veranstaltungsslides „Basics für Cyberlaw - DEMONSTRATOR: Rasterfahndung (SI²S & RER-Prüfung)" wurden Argumentationen aus 2003 beibehalten, die heute nicht mehr in diesem Wording gefasst werden würden. Der Originalwortlaut wird aber beibehalten, um die Tradition der Herausforderungen im „informationstechnologischen Sicherheitsrecht" zu belegen. Die weitere Überarbeitung und Aktualisierung bleibt weiteren Veröffentlichungen vorbehalten. Die Überarbeitung des Foliensatzes (bestehend aus drei Clustern) in 2023 soll didaktischen Zwecken genügen und beschränkt sich inhaltlich im Wesentlichen auf die Folien 16-19, 44-45, 48-51.

Agenda - Gesamtübersicht

TECHNISCHE UNIVERSITÄT DARMSTADT

A. Time, Transition & Change Management – „Evaluation“
B. Rechtsquellen
    I. Aktuelles (Datenschutz-)Recht
    II. Future Law (de lege ferenda?)
C. Rasterfahndung nach dem 11. September
    I. „Rechtsverhalt
    II. Klassische Didaktik (beginnend 2003)
D. Schema für die Interessenanalyse Informationstechnologischer Sachverhalte (SI²S)
    I. Abstrakt
    II. Konkret
E. RER-Prüfung
    I. RER-Schema
    II. Definitionen

Agenda - Gesamtübersicht

TECHNISCHE UNIVERSITÄT DARMSTADT

E. RER-Prüfung

III. Falllösung

1. Recht

2. Eingriff

3. Rechtfertigung

a. Spezielle Schranke: Verfassungsmäßige Ordnung

b. Formelle Verfassungsmäßigkeit (Kein Schwerpunkt)

c. Materielle Verfassungsmäßigkeit

aa. Geeignetheit

bb. Erforderlichkeit

cc. Verhältnismäßigkeit im engeren Sinne

4. Ergebnis (2003)

5. Ergebnis (2023)?

A. 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.

B. Rechtsquellen für Cyberlaw
I. Aktuelles (Datenschutz-)Recht

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 […] 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

3. BDSG: Bundesdatenschutzgesetz (zuletzt geändert am 01. Dez. 2021)

4. HDSIG: Hessisches Datenschutz- und Informationsfreiheitsgesetz (zuletzt geändert am 15. Nov. 2021)

B. Rechtsquellen für Cyberlaw
I. Aktuelles (Datenschutz-)Recht
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

TECHNISCHE UNIVERSITÄT DARMSTADT

5. Digital Services Act; EU-DSA: Verordnung (EU) 2022/2065 […] vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste)

6. Digital Markets Act; EU-DMA: Verordnung (EU) 2022/1925 des […] vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte)

7.E-Evidence VO: Verordnung (EU) 2023/1543 […] vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren

B. Rechtsquellen für Cyberlaw
II. Future Law (de lege ferenda?)

TECHNISCHE UNIVERSITÄT DARMSTADT

8. „Datengesetz“: Vorschlag für eine Verordnung […] über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung, COM(2022) 68 final

9. „KI-Verordnung“: Vorschlag für eine Verordnung […] zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz […], COM(2021) 206 final **sowie** Abänderungen des Europäischen Parlaments vom 14. Juni 2023, P9 TA(2023)0236

10. „ePrivacy-Verordnung“: Vorschlag für eine Verordnung des […] über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation […] COM(2017) 10, final, **sowie** Entwurf des Europäischen Parlaments vom 20.10.2017, A8-0324/2017

11. Vorschlag für eine […] zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, COM/2022/209 final

B. Rechtsquellen
II. Future law (de lege ferenda)?
ePrivacy-Verordnung-Historie (Stand 2019)

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

C. Rasterfahndung nach dem 11. September
I. „Rechtsverhalt"

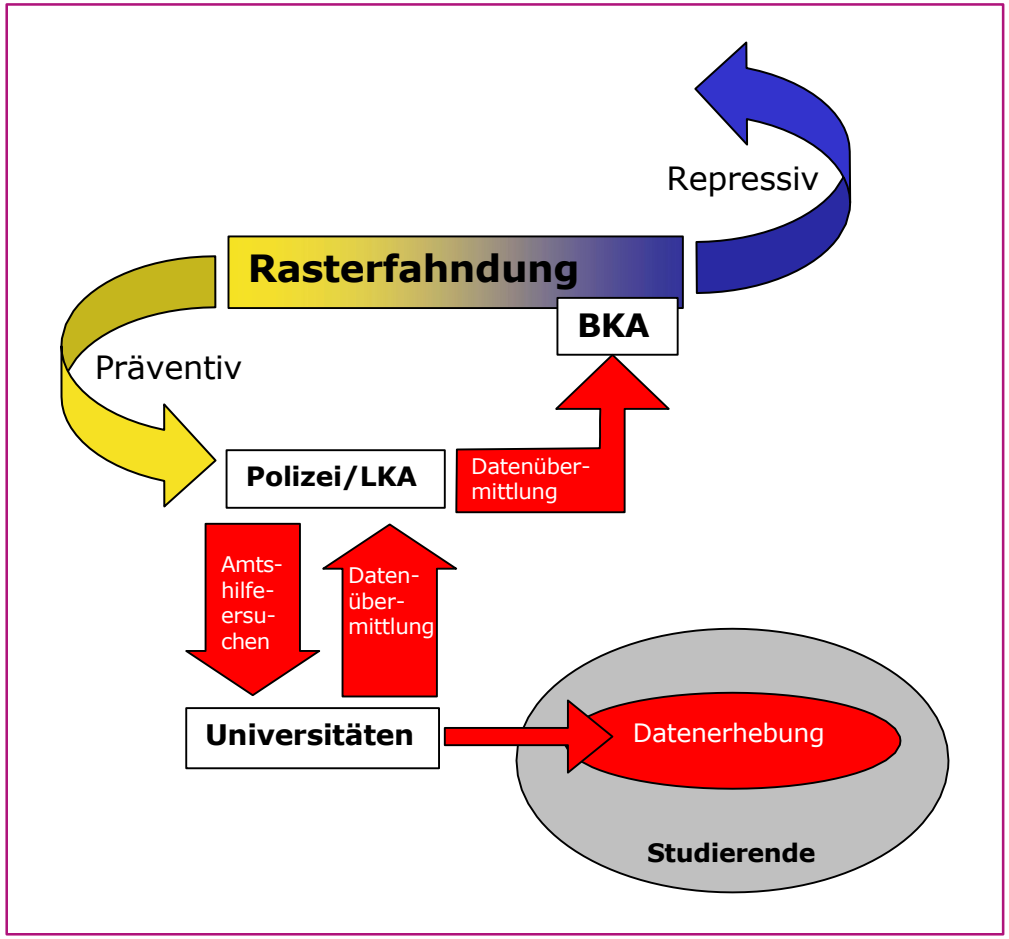
TECHNISCHE UNIVERSITÄT DARMSTADT

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 Aktualität und Relevanz behalten. Dies rechtfertigt eine Präsentation auch in 2023.

C. Rasterfahndung nach dem 11. September
I. „Rechtsverhalt"



C. Rasterfahndung nach dem 11. September
I. „Rechtsverhalt"
Rechtsgrundlage: § 26 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.

(2) Das Übermittlungsersuchen ist auf Namen, Anschriften, Tag und Ort der Geburt sowie auf im einzelnen Falle festzulegende Merkmale zu beschränken. Werden wegen technischer Schwierigkeiten, die mit angemessenem Zeit- oder Kostenaufwand nicht beseitigt werden können, weitere Daten übermittelt, dürfen diese nicht verwertet werden.

C. Rasterfahndung nach dem 11. September
I. „Rechtsverhalt"
Rechtsgrundlage: § 26 HSOG

TECHNISCHE UNIVERSITÄT DARMSTADT

Besondere Formen des Datenabgleichs

(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 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) [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 5. Oktober 2021 (BGBl. I S. 4607), entsprechend. [4]Die oder der Hessische Datenschutzbeauftragte ist durch die Polizeibehörde unverzüglich über die Anordnung zu unterrichten.

C. Rasterfahndung nach dem 11. September
II. Klassische Didaktik (beginnend 2003)

TECHNISCHE UNIVERSITÄT DARMSTADT

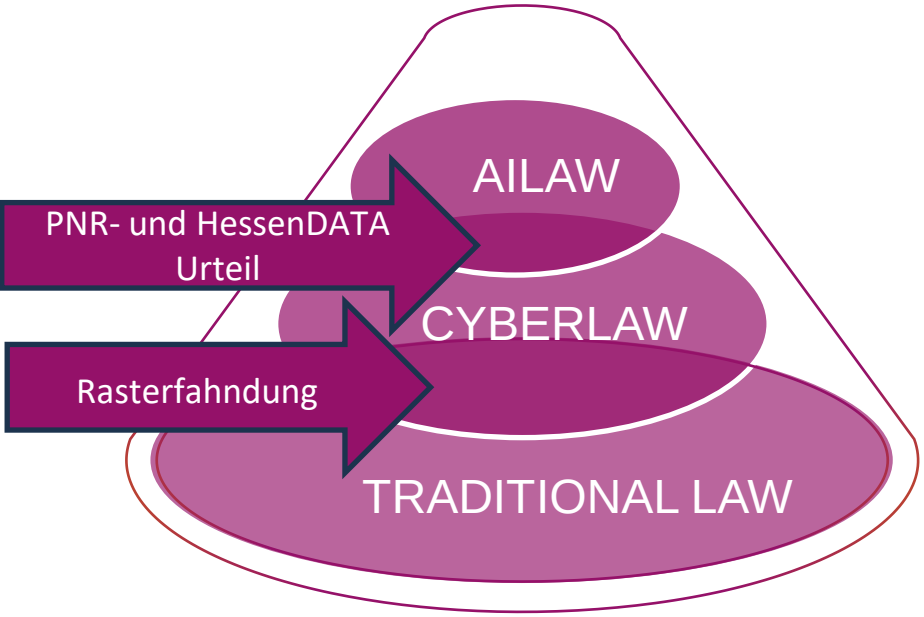
Es handelt sich um einen historischen Fall, der seit 2003 regelmäßig (in der Vorlesung) präsentiert wird. Er hat seitdem Aktualität und Relevanz behalten. Dies rechtfertigt eine Präsentation auch in 2023 aus folgenden Gründen:

1. EVALUATION

Typisch für Cyberlaw in 2023 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/ Ergebnissen führen können. Demzufolge stellt sich für die Vorlesung wie für die Klausurlösung für die Studierenden die Notwendigkeit zeitnaher Information wie Reflexion („Update").

* Schmid: Schlussbericht vom 13.09.2013 zum BMBF-Projekt „Sicherheit im öffentlichen Raum – SIRA", S. 4.

C. Rasterfahndung nach dem 11. September
II. Klassische Didaktik (beginnend 2003)



2. Von der Automatisierung zur Autonomisierung?

Das Rasterfahndungsszenario aus der Vorlesung seit 2002 bereitet auf eine fortschreitende Automatisierung (und Autonomisierung?) der „Datenorganisationen" vor. In 2022 und 2023 spiegelt sich diese Bedeutung von Informationen für die staatliche/ unionale Sicherheitsvorsorge in 2 höchstrichterlichen Urteilen wieder:

1. "HessenDATA"-Urteil des BVerfG vom 16.02.2023, 1 BvR 1547/19
2. "PNR" – Urteil des EuGH vom 21.06.2022, C-817/19

C. Rasterfahndung nach dem 11. September
II. Klassische Didaktik (beginnend 2003)

TECHNISCHE UNIVERSITÄT DARMSTADT

3. EEDAA-Formel*

Vorausgesetzt wird die Unterscheidung von
1. Elektrifizierung,
2. Elektronisierung,
3. Digitalisierung,
4. Automatisierung,
5. Autonomisierung

Angesichts der derzeit fehlenden deutschen/ unionalen Legaldefinition zu „Künstlicher Intelligenz"* wird pragmatisch eine solche Differenzierung vorgeschlagen.

* Zur EDAA Formel: CyLaw Report XXXXII aus 01/2023: "„Weltrecht^2 Backbone Documents" here "PAPER": "MULTIDISCIPLINARY CONSTITUTIONAL LAW SCHOLARSHIP FROM GERMANY AND THE EU" S. 8, 14, 17

** Der AI Act der EU ist derzeit nur de lege ferenda. Siehe bereits in der Literatur 2022 *Nida-Rümelin* in: Chibanguza et. al. (Hrsg.), Künstliche Intelligenz, S. 29 f; 75 ff. zu mehreren Definitionen in unterschiedlichen Disziplinen und Sprachen. Des Weiteren ist auf den englischen Sprachgebrauch in der Bletchley Declaration vom 1. November 2023 zu verweisen.

D. SCHEMA FÜR DIE INTERESSENANALYSE INFORMATIONSTECHNOLOGISCHER SACHVERHALTE (SI²S)*

TECHNISCHE UNIVERSITÄT DARMSTADT

„Fast jedem Einsatz von Informationstechnologie ein Interessenschema „unterlegen", das hier als „Schema für die Interessenanalyse informationstechnologischer Sachverhalte" bezeichnet wird. Abgekürzt wird diese Überschrift mit dem „mathematischen Bild" SI²S – zum Ausdruck gebracht werden soll damit, dass sich Interessenanalyse und Informationstechnologie in einem quadratischen Verhältnis zueinander befinden. Die Schematisierung wie Einbindung in einen juristisch zu subsumierenden Sachverhalt erfolgt in einem Rahmen, der dieses Quadrat einfasst. Dieses Interessensschema ermöglicht die Kategorisierung eines Projekts als rechtlich mehr oder minder komplex."

Bspw. gilt: „Je höher die Rechtsordnung die Qualität des betroffenen Objekts (3.)** einschätzt, desto höhere Anforderungen werden rechtlich an die Qualität der Ermächtigungsgrundlage […] sowie IT-Sicherheit […] gestellt."

* *V. 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; insb. S. 223, 226 **Auf eine Wiedergabe des Fußnotenkatalogs wird hier verzichtet und auf die Veröffentlichung verwiesen.**

** Siehe dazu gleich bei SI²S

D. SCHEMA FÜR DIE INTERESSENANALYSE INFORMATIONSTECHNOLOGISCHER SACHVERHALTE (SI²S; aktualisierte Normbelege)

I. 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" (vgl. Art. 17 Abs. 1 DSGVO).
2b)	**Personal-passiv Informationskosten**	Hierunter fallen die Kosten für die Erhebung, Speicherung, Aufbereitung und Übermittlung von Informationen durch den faktisch und rechtlich Verfügungsbefähigten (etwa „Provider"). Dieses Argument wurde etwa in der ersten Vorratsdatenspeicherungsentscheidung des Bundes-verfassungsgerichts* 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? Mit der DSGVO differenziert die Rechtsordnung zwischen „personen- bezogenen Daten" und „besonderer Kategorien personenbezogener Daten".

* BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, Rn. 302 f. 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.

D. SCHEMA FÜR DIE INTERESSENANALYSE INFORMATIONSTECHNOLOGISCHER SACHVERHALTE (SI²S; aktualisierte Normbelege)
I. 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). 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.

D. SCHEMA FÜR DIE INTERESSENANALYSE INFORMATIONSTECHNOLOGISCHER SACHVERHALTE (SI²S; aktualisierte Normbelege)

I. Abstrakt

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.

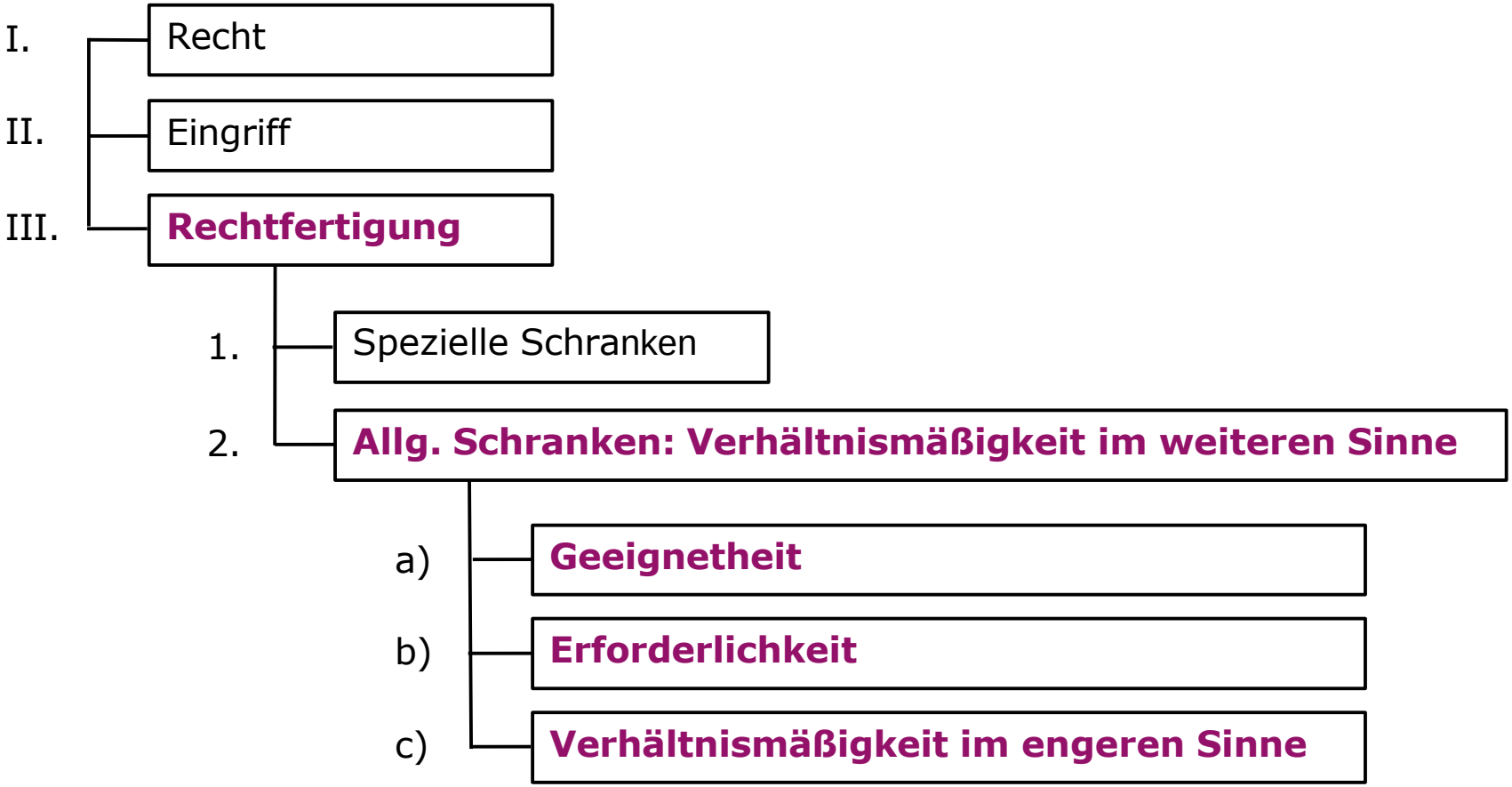
D. SCHEMA FÜR DIE INTERESSENANALYSE INFORMATIONSTECHNOLOGISCHER SACHVERHALTE (SI²S; aktualisierte Normbelege)
I. Abstrakt

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, 2 StPO oder § 26 Abs. 4 S. 1 HSOG.)
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.

D. SCHEMA FÜR DIE INTERESSENANALYSE INFORMATIONSTECHNOLOGISCHER SACHVERHALTE (SI²S; aktualisiert)
II. 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))

E. RER-Prüfung
I. Schema



TECHNISCHE UNIVERSITÄT DARMSTADT

„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).

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

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.

E. RER-Prüfung
III. Falllösung
1. Recht

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.

TECHNISCHE UNIVERSITÄT DARMSTADT

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 (siehe auch Art. 3 Nr. 1, Art. 10 EU-DSGRL*) zulassen. Insoweit ist ein **besonderer Menschenwürdebezug** (Art. 1 Abs. 1 GG) gegeben.

E. RER-Prüfung
2. Konkret
a. Recht

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.

E. RER-Prüfung
III. Falllösung
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, welche personenbezogenen Daten „organisiert" und muss grundsätzlich **einwilligen** bzw. es bedarf einer „gesetzlichen" Ermächtigung**.**

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.

*s. auch BVerfG Urteil vom 15.12.1983 - 1 BvR 209/83 -, Rn. 146

E. RER-Prüfung
III. Falllösung 3. Rechtfertigung
a. Spezielle Schranke: „Verfassungsmäßige Ordnung" (Art. 2 Abs. 1 GG)

TECHNISCHE UNIVERSITÄT DARMSTADT

➢ 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: Dürig/Herzog/Scholz, Grundgesetz Kommentar, 101. EL, 2023, Art. 2 Abs. 1, Rn. 37, 38.

E. RER-Prüfung
III. Falllösung
3. Rechtfertigung
a. 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.

E. RER-Prüfung
III. Falllösung
3. Rechtfertigung
a. Spezielle Schranke: Verfassungsmäßige Ordnung

TECHNISCHE UNIVERSITÄT DARMSTADT

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

*(Verfassungs)mäßigkeit

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.

TECHNISCHE UNIVERSITÄT DARMSTADT

b) Formelle Verfassungsmäßigkeit von § 26 HSOG: aa) 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

b) Formelle Verfassungsmäßigkeit von § 26 HSOG: bb) + cc) 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

c) Materielle Verfassungsmäßigkeit von § 26 HSOG

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

Bei der Prüfung der Rechtfertigung nach Art. 2 Abs. 1 GG mündet also die spezielle Schranke (nach Bejahung der formellen Verfassungsmäßigkeit) in die allgemeine Schranke.

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 – spezielle Schranke – vorbereitet. Die rechtliche Gesamtbewertung wird mit der Prüfung der allgemeinen Schranke abgeschlossen .

E. RER-Prüfung
III. Falllösung
3. Rechtfertigung
a. Spezielle Schranke: Verfassungsmäßige Ordnung

TECHNISCHE UNIVERSITÄT DARMSTADT

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

*(Verfassungs)mäßigkeit

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 (siehe auch Art. 10 sowie Erwägungsgründe 37, 51 EU-DSGRL)

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.

E. RER-Prüfung
III. Falllösung
4. Ergebnis (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

- In 2003 wurde formuliert:

„Vielleicht sollte die Rasterfahndung von einem Richtervorbehalt abhängig gemacht werden, der sich auf einzelne Daten-„organisations"prozesse erstreckt."

Inzwischen kennt § 26 Abs. 4 S. 1 HSOG nicht nur einen Behördenleiter – sondern auch einen Richtervorbehalt.

E. RER-Prüfung
III. Falllösung
4. Ergebnis (2003)

TECHNISCHE UNIVERSITÄT DARMSTADT

Entscheidungen aus der Vergangenheit

- 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)

E. RER-Prüfung
III. Falllösung
5. Ergebnis (2023)?

TECHNISCHE UNIVERSITÄT DARMSTADT

Inzwischen ist der Richtervorbehalt in § 26 Abs. 4 HSOG neben dem Antragsvorbehalt des Behördenleiters geltendes Recht:

- Auch die Gefahrenlage hat sich in zwei Jahrzehnten (in ihrer Wahrnehmung durch die Sicherheitsbehörden und Gerichte) geändert. Nach den Grundsätzen des Time-, Change, Transitionmanagements kommt es deswegen auf die Qualität der Argumentation(-smethodik) an, wie die Klausurlösung bewertet wird. Ausdrücklich wurden seit 2003 unterschiedliche Klausurergebnisse (mit Hilfsgutachten) zugelassen und deswegen 2003 folgendes didaktische Ergebnis in der Vorlesung als möglich präsentiert:

→ **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.**

Annex

Annex:

Change Management - § 26 HSOG Rechtsgrundlage der Rasterfahndung heute – früher

Change Management
Rechtsgrundlage der Rasterfahndung heute – früher
§ 26 Abs. 4 HSOG – Besondere Formen des Datenabgleichs

TECHNISCHE UNIVERSITÄT DARMSTADT

Rechtsgrundlage seit 12.07.2023: Die statische Verweisung auf das FamFG wurde aktualisiert. Siehe im Übrigen zur Veränderung die folgende Folie.	(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 5. Oktober 2021 (BGBl. I S. 4607), entsprechend. [4]Die oder der Hessische Datenschutzbeauftragte ist durch die Polizeibehörde unverzüglich über die Anordnung zu unterrichten.

Change Management
Rechtsgrundlage der Rasterfahndung heute – früher
§ 26 Abs. 4 HSOG – Besondere Formen des Datenabgleichs

TECHNISCHE UNIVERSITÄT DARMSTADT

Fassung vom	Gültig ab	Gültig bis	Wortlaut des § 26 Abs. 4 HSOG
25.06.2018	04.07.2018	12.07.2023	„Die Maßnahme darf nur aufgrund **richterlicher Anordnung auf Antrag der Behördenleitung getroffen werden**. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. 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. Die oder der Hessische Datenschutzbeauftragte ist durch die Polizeibehörde unverzüglich über die Anordnung zu unterrichten.“
03.05.2018	25.05.2018	03.07.2018	„Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums. […]“
14.12.2009	23.12.2009	24.05.2018	„Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums. […]“
14.01.2005	22.12.2004	22.12.2009	„Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums. […]“
06.09.2002	12.09.2002	21.12.2004	„Die Maßnahme nach Abs. 1 bedarf der **schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums**. Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte **unverzüglich** zu unterrichten.“
22.12.2000	01.01.2001	11.09.2002	„Die Maßnahme bedarf **außer bei Gefahr im Verzug der richterlichen Anordnung**. […] Haben die Polizeibehörden bei Gefahr im Verzug die Anordnung getroffen, so beantragen sie unverzüglich die richterliche Bestätigung der Anordnung. Die Anordnung tritt außer Kraft, wenn nicht binnen drei Tagen eine richterliche Bestätigung erfolgt. Die oder der Datenschutzbeauftragte ist durch die Polizeibehörde zu unterrichten.“

Change Management
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.

Change Management
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.**