

# **Cyberlaw**

## **Basics in der Tradition seit 2003 (aktualisiert 11/2018)**

### **Teil II („Cluster II“)**

# Didaktische „Clusterstrategie“: Gliederung des Teil I wird vorausgesetzt → Anhang I



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

Anspruch ist:

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

- ein Rückblick auf Teil I erfolgt, um Wiederholungen zu vermeiden: Die Gliederungsfolie findet sich im Anhang I.
- Die „Clusterverbindung“ zwischen „Cluster I“ und „Cluster II“ beginnen deshalb mit „V.“ der Gliederung – anschließend an Teil I („Cluster I“).



- V. Rasterfahndung nach dem 11. September – „Rechtsverhalt“**
- VI. Time, Transition & Change Management – „Evaluation“**
- VII. „Evaluation“: Schema für die Interessenanalyse Informationstechnologischer Sachverhalte (SI<sup>2</sup>S) in der Tradition seit 2013/2003 mit veralteten Normquellen (11/2018)**
- VIII. Schema für die Interessenanalyse Informationstechnologischer Sachverhalte (SI<sup>2</sup>S) in der Tradition seit 2013/2003 – aktualisiert (11/2018)**
  - 1. Abstrakt
  - 2. Abstrakt – Differenzierung „Objekt“(SI<sup>2</sup>S – 3): „Besondere Kategorien personenbezogener Daten“ im „Mehrebenenmodell“
    - a) EU
    - b) BRD und Hessen
    - c) Unterschiede im europäischen und deutschen Bundes- und Landesrecht?

## Gliederung des Teil II

---

3. Abstrakt – Differenzierung „Objekt“(SI<sup>2</sup>S – 3): „Besondere Kategorien personenbezogener Daten“ im „Mehrebenenmodell“
4. Abstrakt – Differenzierung „Objekt“(SI<sup>2</sup>S – 3): „Informationstechnologisches Sicherheitsrecht “ (eigene Terminologie) im „Mehrebenenmodell“
5. Abstrakt – Differenzierung „Kausal/Zweck“ (SI<sup>2</sup>S – 4): Gefahrenbegriffe in Hessen und Bayern
6. Abstrakt – Differenzierung Qualität der Information(stechnik) „Personalaktiv Informationsrecht“ (SI<sup>2</sup>S – 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

## Gliederung des Teil II

---

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)**

**FEX (II)**

**FEX (III)**

**Anhang I: Gliederung des Teil I**

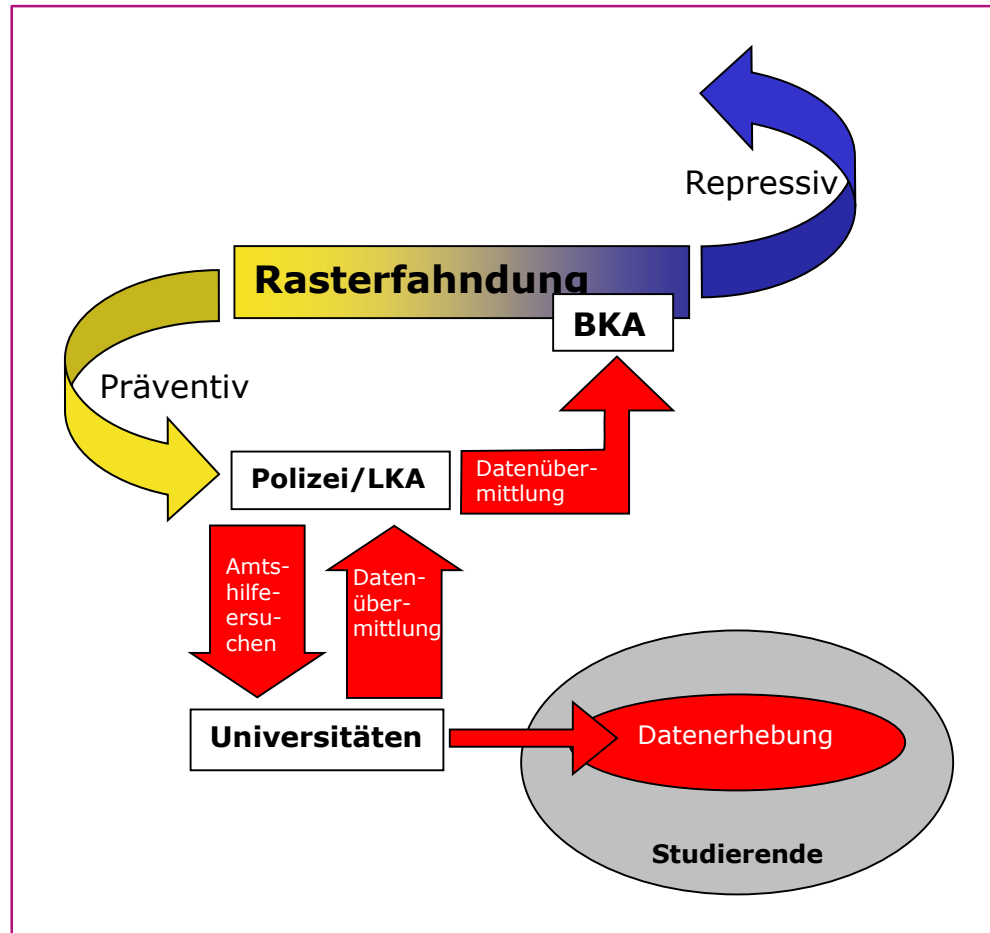
---

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

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 2018 ff. Typisch für Cyberlaw in 2018 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)



## VI. Time, Transition & Change Management – „Evaluation“

Cyberlaw als neue/weitere Disziplin des Rechts ist in besonderem Maße änderungsanfällig. Grund ist, dass es sich um „Neuland“ für die „Governance, Compliance & Regulation“ (siehe auch die Forschungsinitiative „GoCore!“) handelt. Es handelt sich um eine 5. Dimension des Seins (neben den m<sup>3</sup> der Realworld und der Zeit) und die Pioniererfahrungen in ökonomischer, informationstechnologischer und gesellschaftlicher wie rechtlicher Perspektive werden gegenwärtig erst gemacht.

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 **Konstituenten** dieser weiteren 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 (SI<sup>2</sup>S)\* in der Tradition seit 2013/2003 mit veralteten Normquellen (11/2018)



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

1)	<b>Personal-aktiv Informationsrecht</b>	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an Informationen <sup>31</sup> interessiert ist.
2a)	<b>Personal-passiv Datenschutz</b>	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“. <sup>32</sup>
2b)	<b>Personal-passiv Informationskosten</b>	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 <sup>33</sup> – auch wenn die Informationserhebung, -speicherung und -übermittlung nach Meinung der betroffenen Industrien erhebliche Kosten verursachen kann <sup>34</sup> .
3)	<b>Objekt</b>	Auf Informationen <b>welchen Inhalts</b> 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: Hendlar/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 (SI<sup>2</sup>S)\* in der Tradition seit 2013/2003 mit veralteten Normquellen (11/2018)



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

3)	<b>Objekt (Fortsetzung)</b>	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“ <sup>35</sup> 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 <b>Profilierungspotenzial</b> ? Etwa dadurch, dass der Eingang eines Einfamilienhauses videoüberwacht wird, und so ein Bewegungs- und Kontaktprofil der dort wohnenden Familie erstellt werden kann <sup>36</sup> . Hat eine Information ein spezifisches <b>Kombinationspotenzial</b> – 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. <sup>37</sup>
4)	<b>Kausal/Zweck</b>	Zu welchem Zweck soll auf diese Informationen zugegriffen werden (etwa: Kampf gegen den Terrorismus; Wahrung der Urheberrechte, Gesundheitsschutz als „Rechtfertigungsgüter“ <sup>38</sup> )? 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. <sup>39</sup>

## VII. „Evaluation“: Schema für die Interessenanalyse Informationstechnologischer Sachverhalte (SI<sup>2</sup>S)\* in der Tradition seit 2013/2003 mit veralteten Normquellen (11/2018)



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

5a)	<b>Qualität der Information(stechnik) Personal-passiv Datenschutz</b>	Hierzu zählt die Informationstechnik, die etwa Daten vor unbefugter Einsichtnahme schützt, wie etwa die Verschlüsselung <sup>40</sup> 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“ <sup>41</sup> betont worden.
5b)	<b>Qualität der Information(stechnik) Personal-aktiv Informationsrecht</b>	Erfasst sind alle Formen der „ <b>Organisation</b> “ von Daten. <sup>42</sup> Etwa in der Vorratsdatenspeicherungsentscheidung schließt das BVerfG den Pull-Betrieb aus und verlangt einen Push-Betrieb durch den „Provider“ <sup>43</sup> . Die Sicherheitsbehörden dürfen also nicht selbst auf die beim Provider gespeicherten Daten ohne dessen Wissen zugreifen.
6)	<b>Rechtliches Verfahren</b>	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 <sup>44</sup> ; Richtervorbehalt, etwa § 100b Abs. 1 S. 1 StPO.)
7)	<b>Rechtfertigung/Verhältnismäßigkeit</b>	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 (SI<sup>2</sup>S)** in der Tradition seit 2013/2003 – **aktualisiert (11/2018)**



## 1. Abstrakt

<b>1)</b>	<b>Personal-aktiv Informationsrecht</b>	Hierunter werden Rechte einer natürlichen oder juristischen Person verstanden, die an Informationen interessiert ist.
<b>2a)</b>	<b>Personal-passiv Datenschutz</b>	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“.
<b>2b)</b>	<b>Personal-passiv Informationskosten</b>	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 Bundesverfassungsgericht* als vernachlässigbar qualifiziert – auch wenn die Informationserhebung, -speicherung und -übermittlung nach Meinung der betroffenen Industrien erhebliche Kosten verursachen kann.**
<b>3)</b>	<b>Objekt</b>	Auf Informationen <b>welchen Inhalts</b> soll zugegriffen werden? Hier kennt die „Rechtsordnung“ (unter Berücksichtigung des „Mehrebenenmodells“) bereits vor 2018 grundsätzlich die Unterscheidung zwischen „personenbezogenen Daten“ und „besonderer Kategorien personenbezogener Daten“ (vgl. etwa § 3 Abs. 1 und 9 BDSG <b>alter Fassung</b> ). 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 (SI<sup>2</sup>S) in der Tradition seit 2013/2003 – aktualisiert (11/2018)



## 1. Abstrakt

3)	<b>Objekt (Fortsetzung)</b>	<p>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 <b>Profilierungspotenzial</b>, das als „Profiling“ im Rechtssinne zu qualifizieren ist (Art. 4 Nr. 4, Art. 22 EU-DSGVO)?</p> <p>Hat eine Information ein spezifisches <b>Kombinationspotenzial</b> – 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.</p>
4)	<b>Kausal/Zweck</b>	<p>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.</p>

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

# VIII. Schema für die **Interessenanalyse** **Informationstechnologischer Sachverhalte (SI<sup>2</sup>S)** in der Tradition seit 2013/2003 – aktualisiert (11/2018)



## 1. Abstrakt

<b>5a)</b>	<b>Qualität der Information(technik) Personal-passiv Datenschutz</b>	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 „Vorratsdaten-speicherung“ betont worden.
<b>5b)</b>	<b>Qualität der Information(technik) Personal-aktiv Informationsrecht</b>	Erfasst sind alle Formen der „ <b>Organisation</b> “ ( <b>eigene Terminologie</b> ) 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 Luftfahrtsystemen 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-)wirtschaftlicher Betätigung teilen müssen und dürfen, wird vorhersehbar eine Kernaufgabe des Cyberlaw sein.

# VIII. Schema für die Interessenanalyse Informationstechnologischer Sachverhalte (SI<sup>2</sup>S) in der Tradition seit 2013/2003 – aktualisiert (11/2018)



## 1. Abstrakt

6)	<b>Rechtliches Verfahren</b>	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)	<b>Rechtfertigung/Verhältnismäßigkeit</b>	Hier findet etwa die aus dem deutschen Verfassungsrecht bekannte Verhältnismäßigkeitsprüfung statt, die das Interesse von Personalaktiv (Rechtfertigungsrechtsgut) und das Interesse des Personalpassiv Datenschutzes (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 10 GG, Art. 13 GG) und das Interesse der Personalpassiv Informationskosten (Art. 12, 14, 2 Abs. 1 GG) abwägt.

# VIII. SI<sup>2</sup>S – aktualisiert (11/2018)

## 2. Abstrakt – Differenzierung „Objekt“ (SI<sup>2</sup>S – 3): „Personenbezogene Daten“ im „Mehrebenenmodell“

### 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 [...]



## VIII. SI<sup>2</sup>S – aktualisiert (11/2018)

### 2. Abstrakt – Differenzierung „Objekt“ (SI<sup>2</sup>S – 3): „**Personenbezogene Daten**“ im „Mehrebenenmodell“



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 Landesrecht das Adjektiv „natürlich“ nicht wiedergegeben.

# VIII. SI<sup>2</sup>S – aktualisiert (11/2018)

## 2. Abstrakt – Differenzierung „Objekt“(SI<sup>2</sup>S – 3): „Personenbezogene Daten“ im „Mehrebenenmodell“



### 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“(SI<sup>2</sup>S – 3): „**Besondere Kategorien personenbezogener Daten**“ im „**Mehrebenenmodell**“



### **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“(SI<sup>2</sup>S – 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“(SI<sup>2</sup>S – 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 Sicherungsmaßnahmen 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“(SI<sup>2</sup>S – 3): „Informationstechnologisches Sicherheitsrecht “ (eigene Terminologie) im „Mehrebenenmodell“



### 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.

### § 72 BDSG / § 67 HDSIG

#### Unterscheidung zwischen verschiedenen Kategorien betroffener Personen

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“ (SI<sup>2</sup>S – 4): Gefahrenbegriffe in Hessen und Bayern

### § 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“ (SI<sup>2</sup>S – 4): Gefahrenbegriffe in Hessen und Bayern

### Didaktik: „Kausal/Zweck“ (SI<sup>2</sup>S – 4) und Verhältnismäßigkeit (SI<sup>2</sup>S – 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 (SI<sup>2</sup>S – 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**.



## VIII. 6. Abstrakt – Differenzierung Qualität der Information(stechnik) „Personal-aktiv Informationsrecht“ (SI<sup>2</sup>S – 5b)



### 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 Rechtsprache „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“ (SI<sup>2</sup>S – 5b)

### 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.

## VIII. 6. Abstrakt – Differenzierung Qualität der Information(stechnik) „Personal-aktiv Informationsrecht“ (SI<sup>2</sup>S – 5b)



### 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 (SI<sup>2</sup>S) in der Tradition seit 2013/2003 – aktualisiert (11/2018)

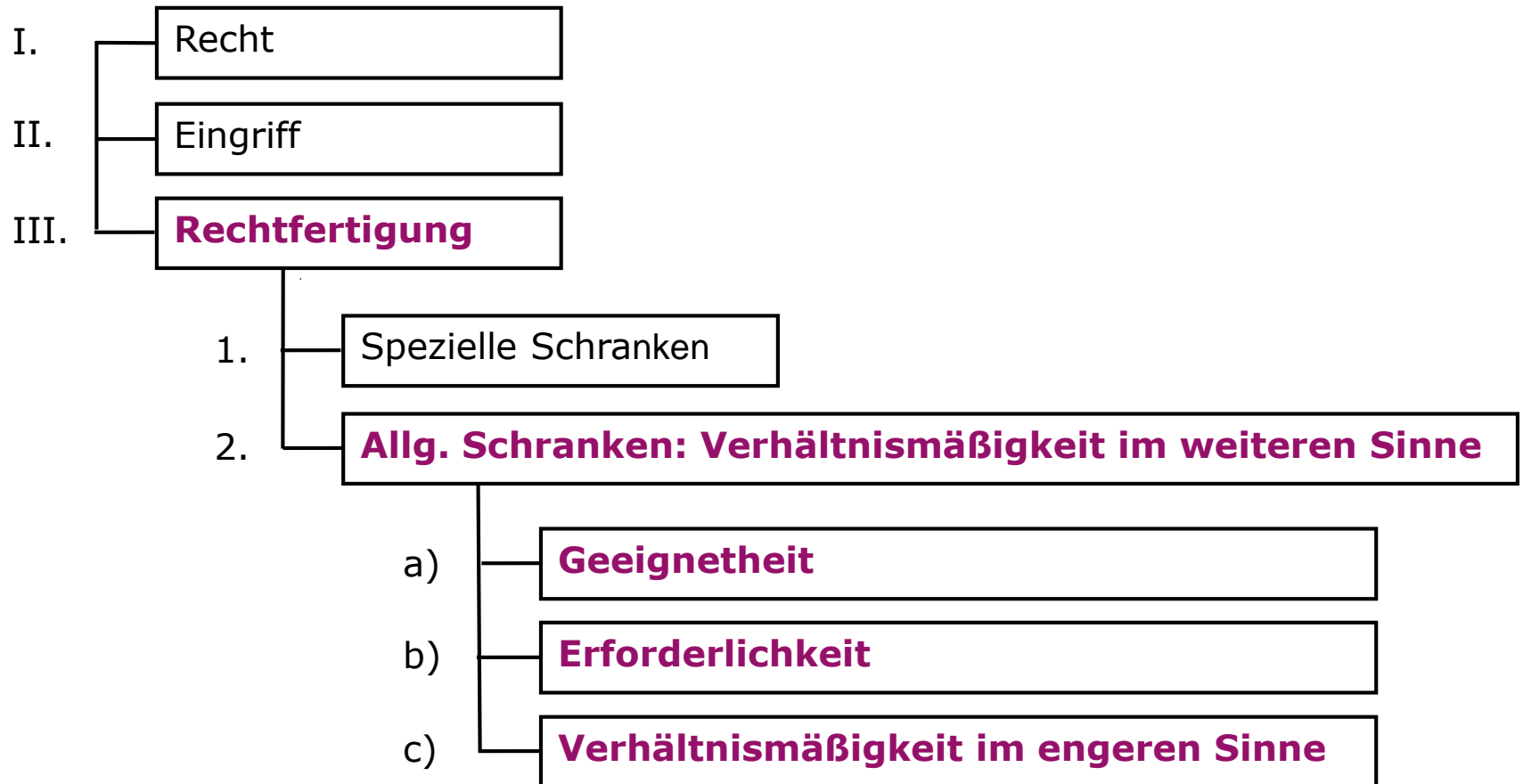


TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

## 7. Konkret

		Analyse
1	<b>Personal-aktiv</b>	Behörde (Ermächtigungsgrundlage?)
2 a)	<b>Personal-passiv</b> Datenschutz	Universität (Behörde) Studierende
2 b)	<b>Personal-passiv</b> Informationskosten	Universität (Kosten der Amtshilfe)
3	<b>Objekt</b>	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	<b>Kausal/Zweck</b>	Terrorismusbekämpfung
5 a), b)	<b>Qualität der Informationstechnik</b>	Datenorganisation Erhebung durch die Universität Übermittlung von Universität an Behörde (keine Angaben im Sachverhalt zu 5 a) u. b)
6	<b>Verfahren</b>	Besondere Verfahrens- und Formvorschriften in der StPO und den Polizeigesetzen
7	<b>Rechtfertigung/ Verhältnismäßigkeit</b>	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 Grundrechtsverwirklichung einschränken (etwa im Wege der Konkordanz oder der Wechselwirkung).

# X. RER-Definition

## 2. Allgemeine Schranken: Verhältnismäßigkeit im weiteren Sinn



Geeignetheit	Eingriff muss geeignet sein, um den Schutz des Rechtsguts, das die Eingriffsrechtsfertigung bildet (Rechtfertigungsrechtsgut), 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 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.

\* [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-Terminologie)



# XI. RER-Prüfung

## 1. 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.

# XI. RER-Prüfung

## 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.

# XI. RER-Prüfung

## 2. Eingriff

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 Sophistikaion: „w<sup>6</sup>“**

Jeder hat ein Recht **zu wissen, wer, wann, wofür, wo, welche** personenbezogenen Daten „organisiert“ und muss grundsätzlich einwilligen bzw. es bedarf einer „gesetzlichen“ Ermächtigung („w<sup>6</sup>“).

- 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).

# XI. RER-Prüfung – 3. Rechtfertigung

## b) Spezielle Schranke: Verfassungsmäßige Ordnung



### 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“

# XI. RER-Prüfung – 3. Rechtfertigung

## b) Spezielle Schranke: Verfassungsmäßige Ordnung



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.

# XI. RER-Prüfung – 3. Rechtfertigung

## b) Spezielle Schranke: Verfassungsmäßige Ordnung

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) Verhältnismäßigkeit im engeren Sinne		

# XI. RER-Prüfung – [...] b) Spezielle Schranke: Verfassungsmäßige Ordnung – § 26 Abs. 1 HSOG

## 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



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.

# XI. RER-Prüfung – 3. Rechtfertigung

## b) Spezielle Schranke: Verfassungsmäßige Ordnung



### 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; [...]

# XI. RER-Prüfung – 3. Rechtfertigung

## b) Spezielle Schranke: Verfassungsmäßige Ordnung



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.

# XI. RER-Prüfung – 3. Rechtfertigung

## b) Spezielle Schranke: Verfassungsmäßige Ordnung

### 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 Gliederungs-struktur 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.).

# XI. RER-Prüfung – 3. Rechtfertigung

## c) Allgemeine Schranke: Verhältnismäßigkeit im weiteren Sinne



### 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).

# XI. RER-Prüfung – 3. Rechtfertigung

## c) Allgemeine Schranke: Verhältnismäßigkeit im weiteren Sinne



### 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 milderer Mittel, weil § 26 Abs. 2 S. 1 HSOG bereits eine Beschränkung auf „bestimmte“ Daten vorsieht.

#### § 26 Abs. 2 S. 1 HSOG

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

# XI. RER-Prüfung – 3. Rechtfertigung

## c) Allgemeine Schranke: Verhältnismäßigkeit im weiteren Sinne



### 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 ein 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.

# XI. RER-Prüfung – 3. Rechtfertigung

## c) Allgemeine Schranke: Verhältnismäßigkeit im weiteren Sinne



### 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.



# XI. RER-Prüfung – 3. Rechtfertigung

## c) Allgemeine Schranke: Verhältnismäßigkeit im weiteren Sinne



### 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.

# XI. RER-Prüfung – 3. Rechtfertigung

## c) Allgemeine Schranke: Verhältnismäßigkeit im weiteren Sinne



### 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 ...) 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.

# XI. RER-Prüfung – 3. Rechtfertigung

## c) Allgemeine Schranke: Verhältnismäßigkeit im weiteren Sinne



### 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.

# XI. RER-Prüfung – 3. Rechtfertigung

## c) Allgemeine Schranke: Verhältnismäßigkeit im weiteren Sinne



### 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 erschienenen Dokumente – etwa im Zusammenhang mit dem Irak-Krieg – zeigen, wie ein Gefährdungspotenzial zu politischen Zwecken missbraucht werden kann.

## XII. Falllösung

### 1. „Klassisch“ seit 2003

- Eine präventive Rasterfahndung kann je nach Konkretisierung des Verdachts und Differenzierung der Fahndungskriterien dazu führen, dass auch „Otto-Normalbürger“ das Stigma eines „Terroristen“ „verliehen“ wird.
  - Darüber hinaus ist die Rasterfahndung ein weiterer Schritt zur virtuellen Erfassung der Persönlichkeit von Menschen.
  - 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

- [BVerfG, Beschl.v. 04.04.2006, 1 BvR 518/02](#)
- [VGH Kassel, Beschl.v. 04.02.2003, 10 TG 3112/02](#)
- [OVG Koblenz, Beschl.v. 22.03.2002, 12 B 10331/02](#)
- [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



### Ab 04.07.2018

(1) <sup>1</sup>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.

<sup>2</sup>Eine solche Gefahr liegt in der Regel auch dann vor, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass terroristische Straftaten begangen werden sollen.

<sup>3</sup>Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.

### 23.12.2009 bis 03.07.2018

(1) <sup>1</sup>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.

<sup>2</sup>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



### Ab 25.05.2018

(3) <sup>1</sup>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.

<sup>2</sup>Die getroffenen Maßnahmen sind zu dokumentieren.

<sup>3</sup>Diese Dokumentation ist gesondert aufzubewahren und durch technische und organisatorische Maßnahmen zu sichern. <sup>4</sup>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.

### 23.12.2009 bis 24.05.2018

(3) <sup>1</sup>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.

<sup>2</sup>Über die getroffenen Maßnahmen ist eine Niederschrift anzufertigen. <sup>3</sup>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



### Ab 04.07.2018

(4) <sup>1</sup>Die Maßnahme darf nur aufgrund richterlicher Anordnung auf Antrag der Behördenleitung getroffen werden. <sup>2</sup>Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. <sup>3</sup>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.

<sup>4</sup>Die oder der Hessische Datenschutzbeauftragte ist durch die Polizeibehörde unverzüglich über die Anordnung zu unterrichten.

### 25.05.2018 bis 03.07.2018

(4) <sup>1</sup>Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums.

<sup>2</sup>Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte unverzüglich zu unterrichten.

### 23.12.2009 bis 24.05.2018

(4) <sup>1</sup>Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums.

<sup>2</sup>Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte unverzüglich zu unterrichten.

(5) <sup>1</sup>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. <sup>2</sup>§ 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)



**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

- 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**. 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)



## 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)

## 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 kriminalpolizeilichen 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)

## Verfassungswidrige Rechtsgrundlage für die Rasterfahndung im BKA-Gesetz?

### Rasterfahndung (§ 20j BKAG a.F.)

(2) Das Übermittlungersuchen 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 Übermittlungersuchen 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

## 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



- 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 11/2018)

### Teil II („Cluster II“)

# Anhang I: Gliederung des Teil I („Cluster I“)

## 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**