Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 1a)

Vorlesung im Sommersemester 2009
an der Universität Ulm
von Bernhard C. Witt

Zum Dozenten

it.sec
security for your information

Bernhard C. Witt

- Berater für Datenschutz und IT-Sicherheit
- geprüfter fachkundiger Datenschutzbeauftragter
- Industriekaufmann, Diplom-Informatiker
- seit 1998 selbstständig
- seit 2005 Lehrbeauftragter an der Universität Ulm
- Autor zu Datenschutz & IT-Sicherheit in Fachbücher & Artikel

Fachliche Zuordnung

- Vorlesung (VL) im Hauptstudium / Master (CS8925) mit 2+2 SWS = 6 LP

  in den Informatik-Studiengängen wie folgt anrechenbar:

Medieninformatik & Diplom-Informatik & Master:

- **Kernfach** Praktische und Angewandte Informatik

Diplom-Informatik & Master of Computer Science:

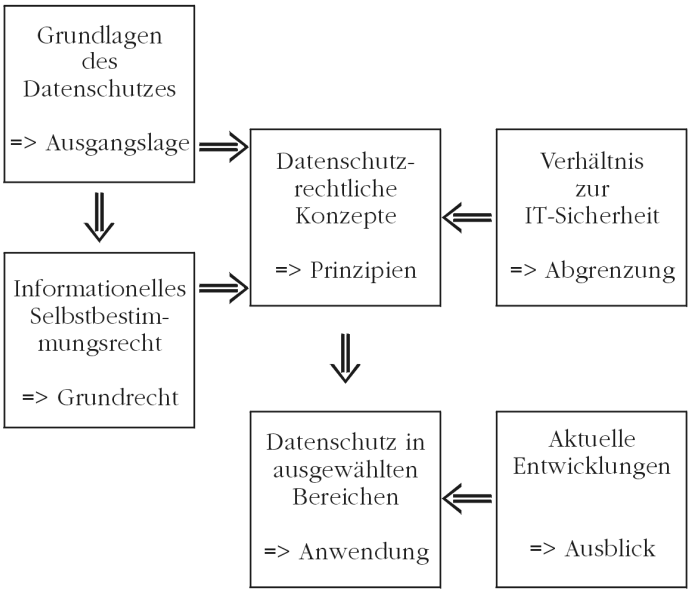
- (alternativ) **Vertiefungsgebiet/Spezialisierung** Informatik und Gesellschaft

Übersicht zur Vorlesung

Grundlagen des Datenschutzes		**Grundlagen der IT-Sicherheit**	
	Geschichte des Datenschutzes		Anforderungen zur IT-Sicherheit
	Datenschutzrechtliche Prinzipien		Mehrseitige IT-Sicherheit
	Technischer Datenschutz		Risiko-Management
	Schwerpunktthema zur Vertiefung		Konzeption von IT-Sicherheit

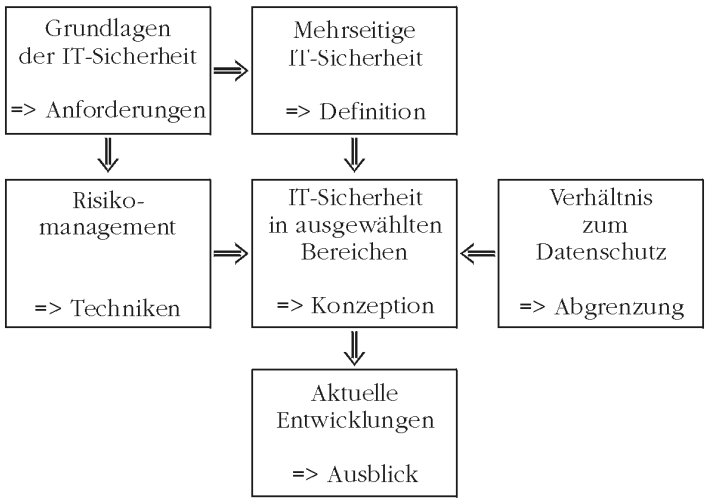
- jeweils **montags** und **mittwochs** 16 – 18 Uhr im H21
- **Vorlesungsmaterial** vorab im Netz unter: www.informatik.uni-ulm.de/datenschutz
- **Übungsblätter + Musterlösungen** ebenfalls
- **Übungen ergänzen (!) Vorlesung**
- **Klausurtermin** noch zu vereinbaren
- Lehrveranstaltung wird didaktisch ausgewertet

Lehrbuch statt Skript (1)



Vorlesung erstreckt sich über alle Kapitel

Lehrbuch statt Skript (2)



Vorlesung erstreckt sich über alle Kapitel

Hinweise

Scheinkriterien:

- 50 % Votieren der (~ 10*5) Aufgaben
  (→ 25 Votierpunkte; Lösungsidee gibt 0,5 Punkte)
  & 5 Aufgabenlösungen erfolgreich präsentieren*
  * bzw. anteilig weniger bei dauerhaft mehr als 10 Teilnehmern

Prüfung:

- Klausur!
  (1/3 Vorlesung, 1/3 Übung, 1/3 Anwendungen)
- Erfahrungen: Schnitt bisher ~ 1,8 (bei 96 Prüfungen)
  Aktive Teilnahme an Übungen → Noten besser!

Literaturhinweise: Datenschutz

In Semesterapparat verfügbar:

- Alexander Roßnagel (Hrsg): Handbuch Datenschutzrecht; München, C.H. Beck, 2003
- Bernhard C. Witt: Datenschutz an Hochschulen; Ulm, LegArtis, 2004
- Marie-Theres Tinnefeld, Eugen Ehmann, Rainer W. Gerling: Einführung in das Datenschutzrecht; München, Oldenbourg, 2005
- Bernhard C. Witt: Datenschutz kompakt und verständlich; Wiesbaden, Vieweg, 2008

Zum Hintergrund der Vorlesung empfehlenswert:

- Gerhard Kongehl (Hrsg), Sebastian Greß, Gerhard Weck, Hannes Federrath: Datenschutz-Management; Planegg, WRS, Loseblattsammlung, Stand: Januar 2008
- Tätigkeitsberichte des BfDI & der LfDs
- Zeitschriften: Datenschutz und Datensicherheit, Recht der Datenverarbeitung, Computer und Recht, MultiMedia und Recht

Literaturhinweise: IT-Sicherheit

Im Semesterapparat verfügbar:

- Bernhard C. Witt: IT-Sicherheit kompakt und verständlich; Wiesbaden, Vieweg, 2006
- Bruce Schneier: Secrets & Lies – IT-Sicherheit in einer vernetzten Welt; Heidelberg, dpunkt, 2001
- Claudia Eckert: IT-Sicherheit; München, Oldenbourg, 2006, 4. Auflage [im Semesterapparat noch die 3. Auflage von 2004]

Zum Hintergrund der Vorlesung empfehlenswert:

- Hans-Peter Königs: IT-Risiko-Management mit System; Wiesbaden, Vieweg, 2005
- Günter Müller & Andreas Pfitzmann (Hrsg): Mehrseitige Sicherheit in der Kommunikationstechnik; Bonn, Addison Wesley, 1997
- Zeitschriften: <kes>, hakin9, IEEE security & privacy, IT-SICHERHEIT

Motivation

- Informationen besonders eigenartiger „Rohstoff“
- Anwendungsbezug der Informatik
- Entwurf von Systemen ggf. mit Personenbezug
- Compliance: Übereinstimmung mit gesetzlichen Erfordernissen bzw. Standards (& Vereinbarungen)
- Berufliche Perspektive (CIO, CISO, Admins etc.)
- Abwehr von Industriespionage
- Ubiquitous Computing
- Kenntnisse in IT-Sicherheit auf Arbeitsmarkt gesucht

Gegenstand der Vorlesung

- grundlegende Einführung in Datenschutz & IT-Sicherheit
- Kennenlernen & Anwendung rechtlicher Anforderungen
- Methoden des (IT-) Risikomanagements
- Konzeption eines Informationssicherheitsmanagements
- Einblick in internationale Standards
- Anwendung gängiger Vorgehensmodelle
- Falldiskussionen & Praxisbeispiele

Lehrziele: Methoden

- Strukturieren und Analysieren auch umfangreicher Texte
- Abstrahieren von Sachverhalten
- Verknüpfung verschiedener Sichtweisen (aus Jura, Informatik und Wirtschaftswissenschaften)
- selbstständiges Aufarbeiten neuen (und ungewohnten) Stoffes
- Beherrschen der Nomenklatur
- Einübung typischer Fertigkeiten
- Anwendung von Kenntnissen in praxisrelevanten Fällen

→ **Erleichterung des Einstiegs in die Berufspraxis**

Lehrziele: Inhalte

- Angabe, Analyse und Anwendung grundlegender Rechtsnormen
- Beherrschen der Nomenklatur
- Erläuterung des informationellen Selbstbestimmungsrechts
- Angabe der Grundsätze beim Datenschutz
- Übertragung der Grundsätze auf neue Problemfälle
- Angabe und Anwendung der Ziele mehrseitiger IT-Sicherheit
- Benennung von Bedrohungen und deren Wirkungen
- Konstruktion von Maßnahmen gegen Bedrohungen
- Kenntnis gängiger Vorgehensmodelle
- Erstellung eines Sicherheitskonzepts/Notfallvorsorgekonzepts
- Durchführung von Risikoanalysen
- Entscheidung über den Umgang mit festgestellten Risiken

Zum Vergleich von Informatik und Jura

- **Informatik und Jura**: konsequente Verwendung definierter Systematik & Fachtermini
- **Informatik** → Definition/Satz/Anwendung;
  Jura → Legaldefinition/Norm/Auslegung mit Abwägung
- **Informatik** → Analogien;
  Jura → Einzelfälle (außer Verfassungsauslegung!)
- **Informatik** → gröbere Bezüge;
  Jura → Detailnachweise

Zur Blitzumfrage

Schwerpunktthema zur Auswahl:

A) Mitarbeiterdatenschutz

- Bewerbung & Personalaktenführung & Mitarbeiterkontrolle
- Mitarbeiterdatenverarbeitung am Beispiel von ERP-Systemen

B) Kundendatenschutz

- Gewinnung & Betreuung/Bindung & Analyse von Kunden
- Kundendatenverarbeitung am Beispiel von CRM-Systemen

C) Sozialdatenschutz

- Umgang mit besonders sensiblen Daten
- Sozialdatenverarbeitung am Beispiel von Krankenkassen

→ ausschlaggebend für Übungsaufgaben!

1. Grundlagen des Datenschutzes

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
→	Geschichte des Datenschutzes		Anforderungen zur IT-Sicherheit
	Datenschutzrechtliche Prinzipien		Mehrseitige IT-Sicherheit
	Technischer Datenschutz		Risiko-Management
	Schwerpunktthema zur Vertiefung		Konzeption von IT-Sicherheit

- Klassische Geschichtsdarstellung (Zeitskala)
- Alternative Geschichtsdarstellung (Schutzziele)
- Rechtsgeschichte (Gesetze & Rechtsprechung)
- Informationelles Selbstbestimmungsrecht
- Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Klassische Geschichtsübersicht

1) Anfänge (vor 1977)

- Persönlichkeitsrecht (Herrenreiter-Urteil) → Privatsphäre
- weltweit 1. Datenschutzgesetz in Hessen

2) 1. BDSG (1977)

- Schutz personenbezogener Daten vor Missbrauch der Beeinträchtigung schutzwürdiger Belange der Betroffenen bei der Datenverarbeitung

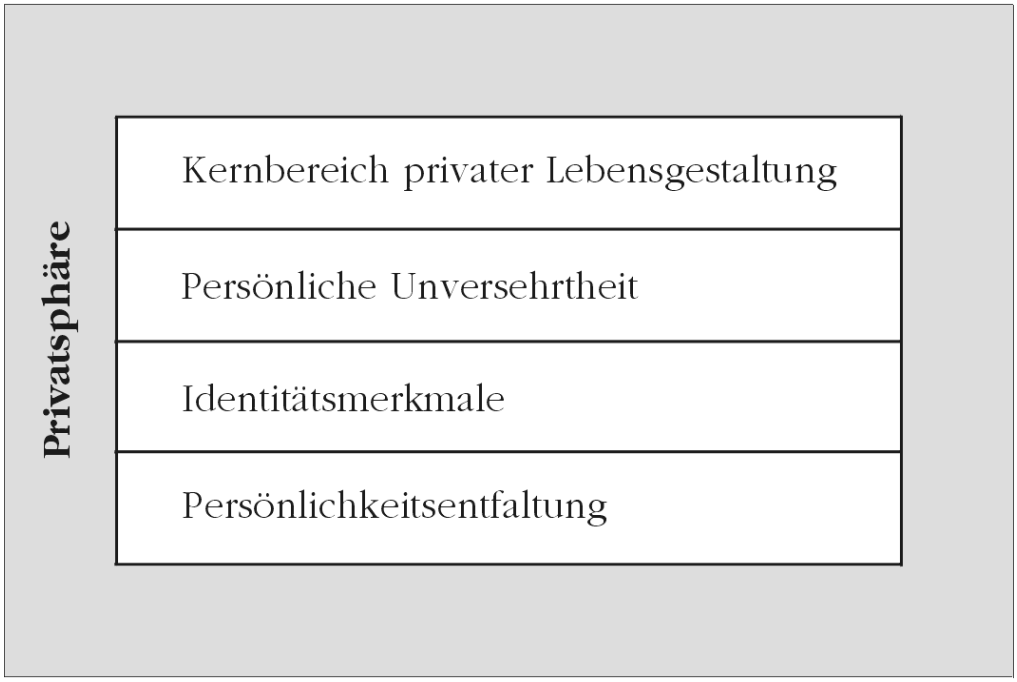
3) 2. BDSG nach Volkszählungsurteil (1990)

- Informationelles Selbstbestimmungsrecht (Volkszählungsurteil)
- Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit personenbezogenen Daten

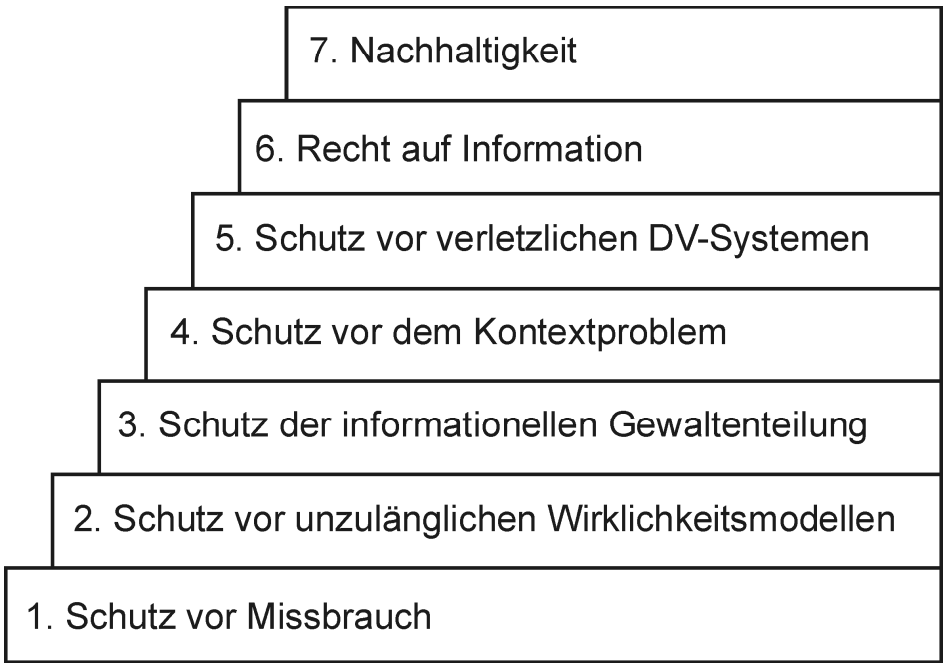
4) 3. BDSG nach EU-DSRL (2001)

- international vergleichbarer Datenschutz
- Vorabkontrolle besonders sensibler Datenverarbeitungen

Bestandteile der Privatsphäre



Alternative Geschichtsübersicht anhand der 7 Schutzziele

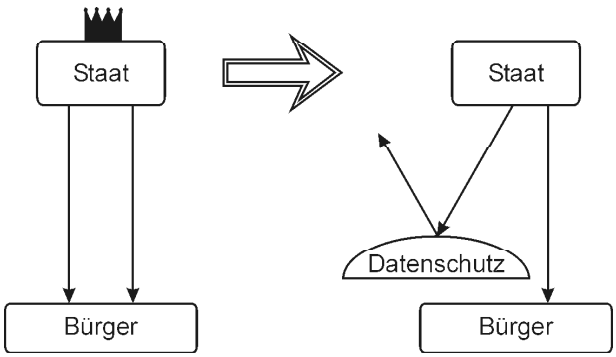


Datenschutz als Abwehrrecht (1)

- Ausgleich des Ungleichgewichtes

→ **Schutz vor Missbrauch** (Ende 60er)

→ Kontrolle durch Datenschutz-beauftragte!



Datenschutz als Abwehrrecht (2)

- im Zuge der 1. Rasterfahndung

Merkmal 1:	A	B	**D**	G	**H**
Merkmal 2:	A	C	**D**	E	**H**
Merkmal 3:	B	**D**	E	F	**H**

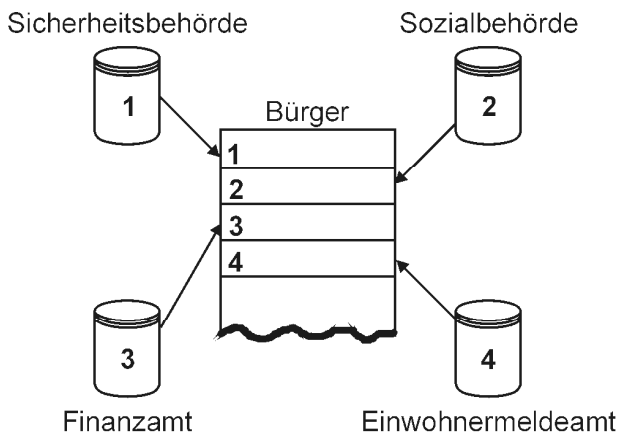
→ **Schutz vor unzulänglichen Wirklichkeitsmodellen** (Ende 70er)

→ Person D & H weisen alle 3 Merkmale auf!

→ keine automatisierte Einzelentscheidung!

Datenschutz als Abwehrrecht (3)

- gegen die Sammelwut des Staates



→ **Schutz der informationellen Gewaltenteilung** (Anfang 80er)

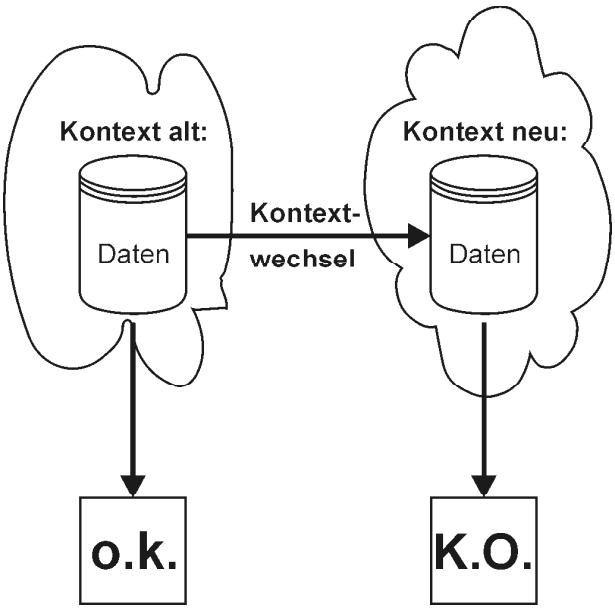
→ personenbezogene Daten anonymisieren!

Datenschutz als Abwehrrecht (4)

- gegen die Vernachlässigung des „Alterns“ von Daten

→ **Schutz vor dem Kontextproblem** (Ende 80er)

→ Beachtung von Löschungsfristen!

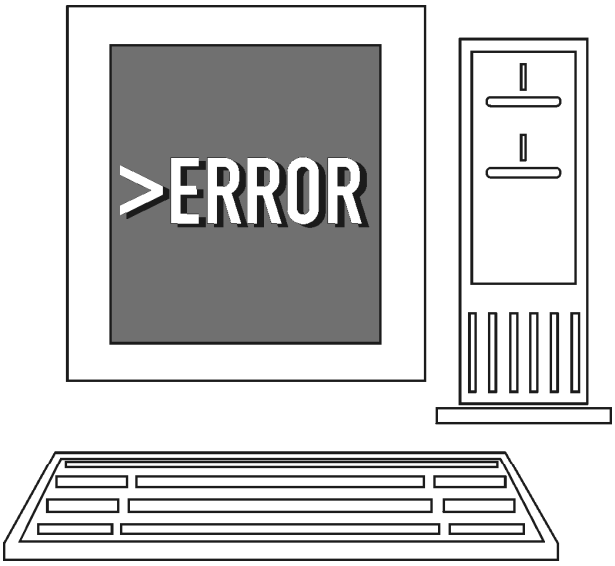


Datenschutz als Abwehrrecht (5)

- gegen den Irrglauben unfehlbarer Software

→ **Schutz vor verletzlichen DV-Systemen** (Anfang 90er)

→ Regelungen zum Schadensersatz!



Datenschutz zur Gestaltung (1)

- die Verwirklichung eigener Rechte erfordert Zugang zu Informationen

→ **Recht auf Information**
(Ende 90er)

→ Akteneinsichtsrecht!

Datenschutz zur Gestaltung (2)

- an Erfordernissen künftiger Generationen orientieren

→ **Nachhaltigkeit**
(Anfang 10er?)

- Reversibilität von Entscheidungen!
  z.B. durch Verfallsdatum von Gesetzen
- Übernahme der Verantwortlichkeit für Handlungen!

Ergebnis der 7 Schutzziele

- Datenschutz hat viele Facetten
- Datenschutz entstanden als Abwehrrecht gegen übermächtigen Staat
- Ausrichtung des Datenschutzes verändert sich
- Datenschutz ist eher Schutz der Informationen über Personen
- Datenschutz ist Schutz vor unerwünschten Verfahren
- Informationstechnik beschleunigt Entwicklung des Datenschutzes

Rechtsgeschichte: Gesetze

1970 Hessen: (erstes!) Datenschutzgesetz
1977 BRD: Bundesdatenschutzgesetz (Version 1)
1978 NRW: Grundrecht auf Datenschutz in Landesverfassung
1980 BRD: Sozialgesetzbuch X
1990 BRD: Bundesdatenschutzgesetz (Version 2)
1995 EU: Datenschutzrichtlinie
1997 BRD: Informations- u. Kommunikationsdienstegesetz
1998 Brandenburg: Akteneinsichts- u. Informationszugangsgesetz
1998 BRD: Großer Lauschangriff
2001 BRD: Bundesdatenschutzgesetz (Version 3)
2002 BRD: Terrorismusbekämpfungsgesetz
2006 BRD: Informationsfreiheitsgesetz
2006 BRD: Bürokratieabbaugesetz → BDSG (Version 4)

Rechtsgeschichte: Urteile (1)

1958 **BGH: Herrenreiterurteil**
(Schadensersatz für die Verletzung des Persönlichkeitsrechts)

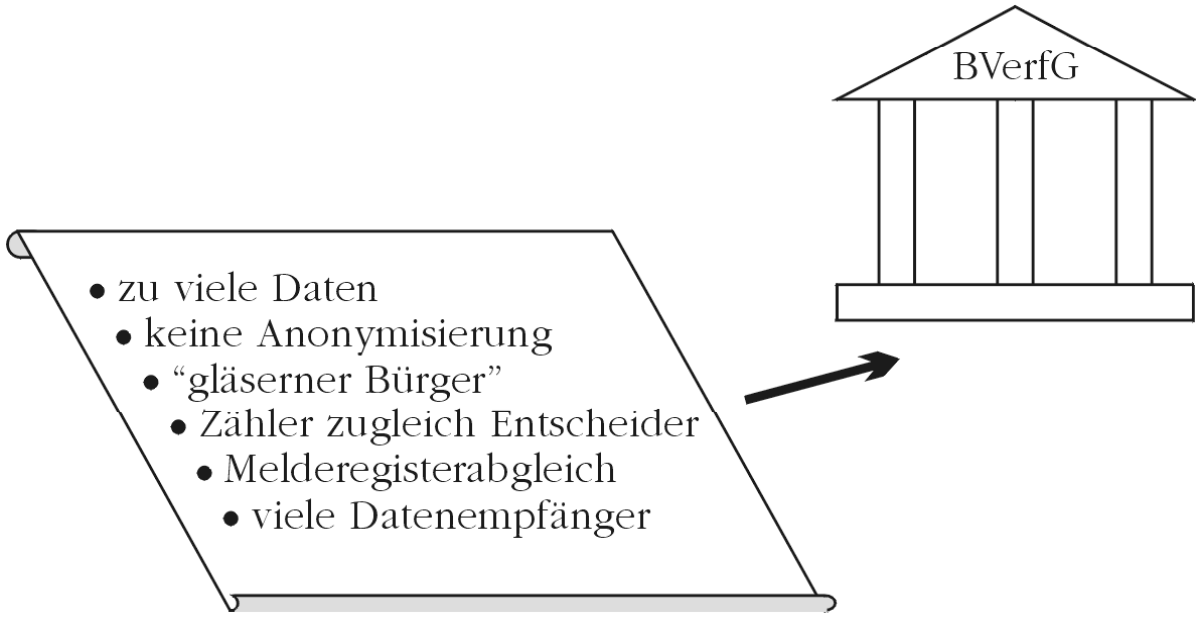
1969 **BVerfG: Mikrozensusbeschluss**
(Menschen nicht als Sachen behandeln)

1970 **BVerfG: Scheidungsaktenbeschluss**
(unantastbarer Bereich privater Lebensführung)

1973 **BVerfG: Lebachurteil**
(Eingriff ins Persönlichkeitsrecht zeitlich begrenzt)

1983 **BVerfG: Volkszählungsurteil**
(informationelles Selbstbestimmungsrecht)

Gründe für Volkszählungsurteil



Definition „informationelles Selbstbestimmungsrecht“

- Zitat aus BVerfGE 65, 1 [43]:
  „Das Grundrecht (des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

Definition 1: Informationelles Selbstbestimmungsrecht

Grundrecht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen

Informationelles Selbstbestimmungsrecht

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.

i.V.m.

Art. 1 Abs. 1 GG: Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

→ Schrankentrias als Schranken!

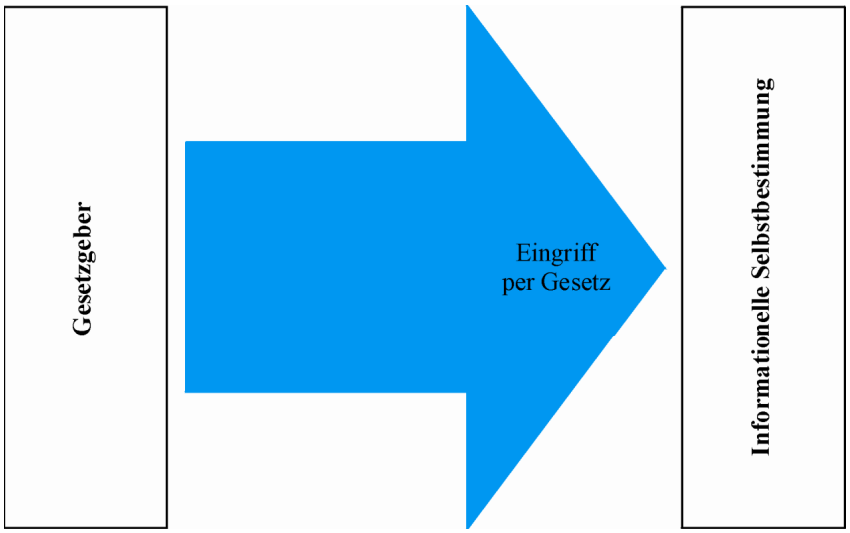
Einschränkung des inform. Selbstbestimmungsrechts (1)

- Zitate aus BVerfGE 65, 1 [43f]
  (Hervorhebung von mir)
  „Der Einzelne ... ist ... eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit."
  → „Grundsätzlich muß daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung **im überwiegenden Allgemeininteresse** hinnehmen."
  „Diese Beschränkungen bedürfen ... einer (verfassungsmäßigen) gesetzlichen Grundlage ... die damit dem rechtsstaatlichen Gebot der **Normenklarheit** entspricht (und dem) Grundsatz der **Verhältnismäßigkeit**"

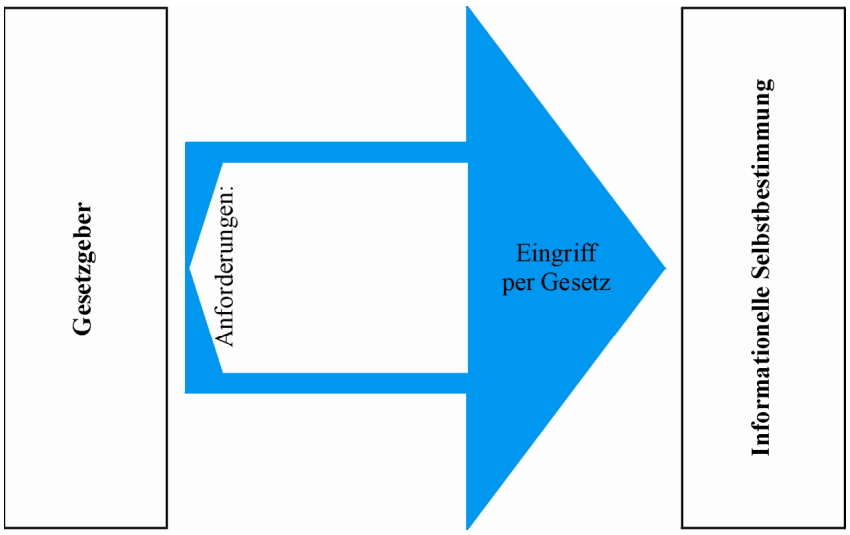
Einschränkung des inform. Selbstbestimmungsrechts (2)

- Zitate aus BVerfGE 65, 1 [44f]
  (Hervorhebung von mir)
  Es gibt „unter den Bedingungen der automatischen Datenverarbeitung **kein ‚belangloses' Datum** mehr."
  „Erst wenn Klarheit darüber besteht, zu welchem **Zweck** Angaben verlangt werden und welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten."
  „Ein überwiegendes Allgemeininteresse wird regelmäßig überhaupt nur an Daten mit Sozialbezug bestehen"

Informationelle Selbstbestimmung (1)

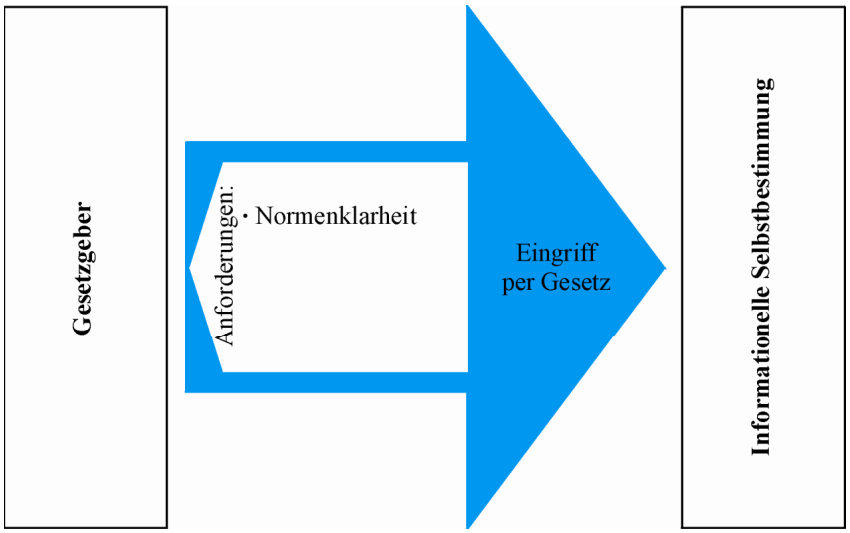


Informationelle Selbstbestimmung (2)



Eingriff erfordert:

Informationelle Selbstbestimmung (3)

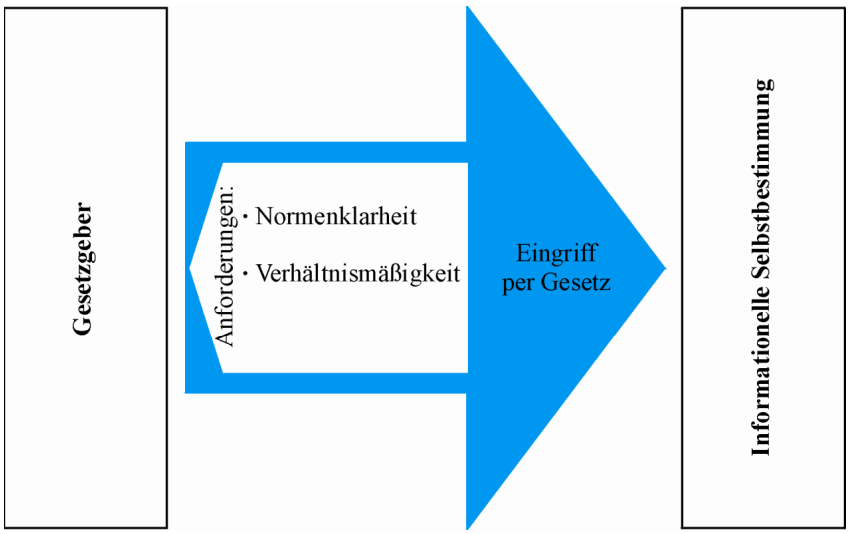


Eingriff erfordert:

Normenklar-heit

Verwendungs-zweck bereichs-spezifisch und präzise bestimmt

Informationelle Selbstbestimmung (4)

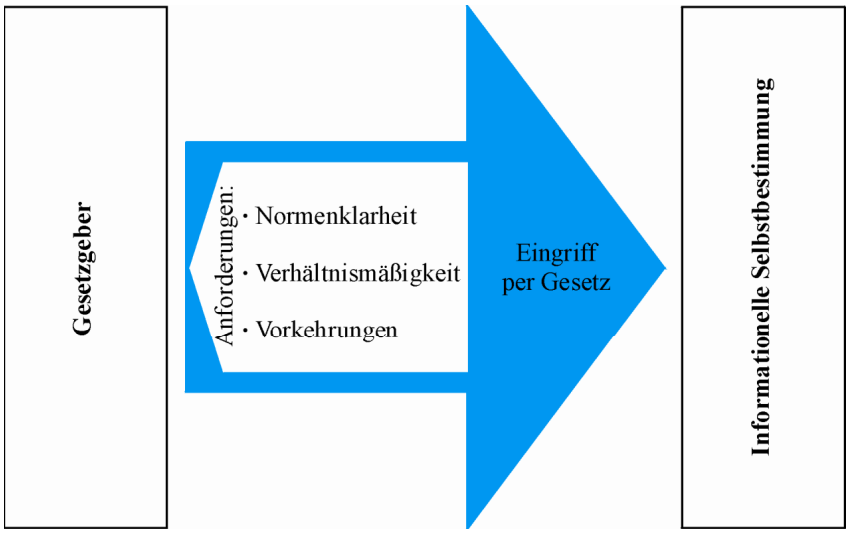


Eingriff erfordert:

Verhältnis-mäßigkeit

personenbezogene Daten müssen für Zweck geeignet und erforderlich sein

Informationelle Selbstbestimmung (5)



Eingriff erfordert:

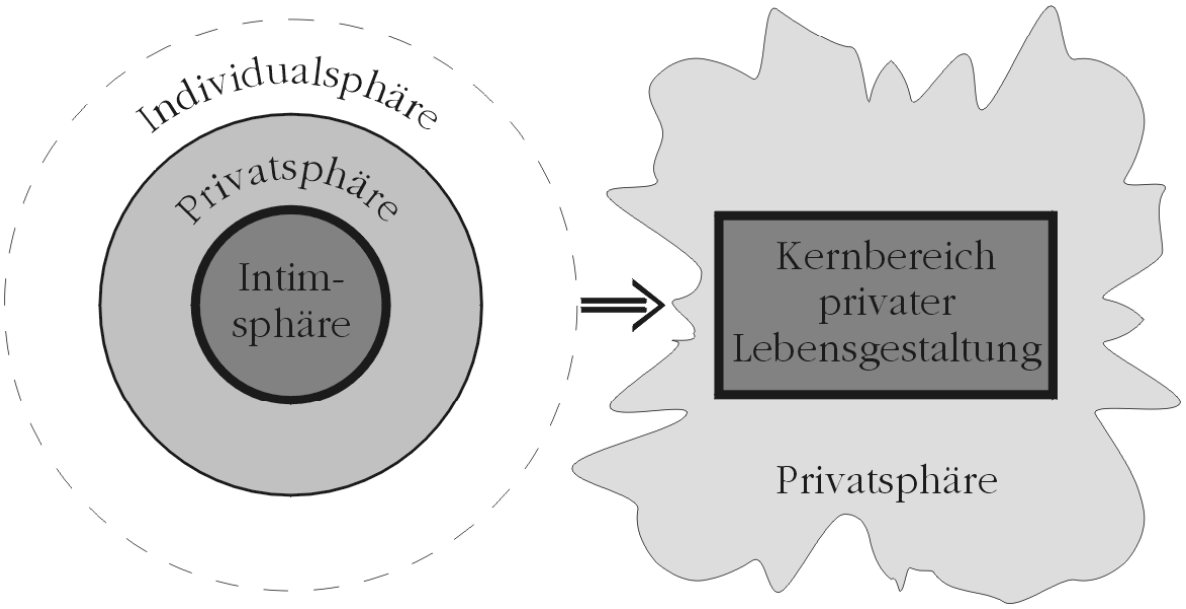
Vorkehrungen

organisatorische & verfahrensabhängige Maßnahmen, insbesondere im Sinne der Datensparsamkeit

„Schranken-Schranken“

- Das informationelle Selbstbestimmungsrecht ist durch die Schrankentrias der Handlungsfreiheit beschränkt
  (= Schranken)
- Jeder Eingriff ins informationelle Selbstbestimmungsrecht erfordert gesetzliche Grundlage!
- Das Gesetz wiederum muss normenklar & verhältnismäßig sein und geeignete Vorkehrungen enthalten!
  (= Schranken-Schranken)

Auflösung der Sphärentheorie



Rechtsgeschichte: Urteile (2)

1999 **BVerfG: Fernmeldeüberwachungsurteil**
(Sicherheitsbehörden haben Einschreitschwellen zu berücksichtigen)

2004 **BVerfG: Urteil zum Großen Lauschangriff**
(absolut geschützter Kernbereich privater Lebensgestaltung)

2006 **BVerfG: Rasterfahndungsbeschluss**
(Eingriff durch Sicherheitsbehörden erst bei hinreichend konkreter Gefahr für hochrangige Rechtsgüter)

2008 **BVerfG: Urteil zur Online-Durchsuchung**
(Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)

Hinweis zum Fernmeldegeheimnis

Grundlage: **Art. 10 Abs. 1 GG**
„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich."

Ausprägungen:

- Telekommunikation → Fernmeldegeheimnis
  § 88 TKG: „Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche."

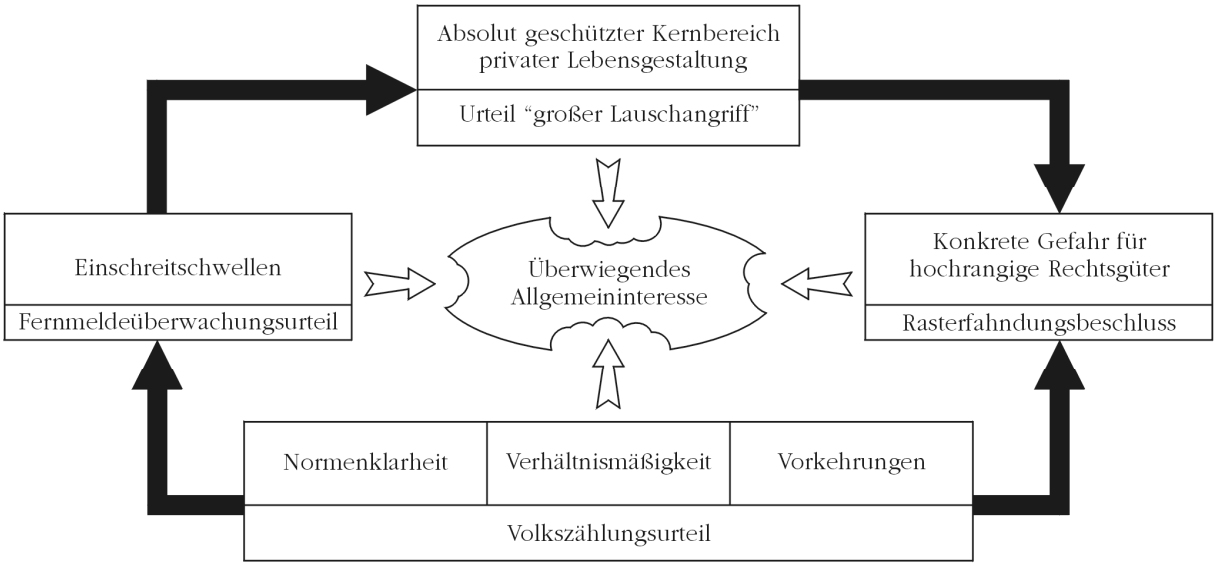
Allgemeines Persönlichkeitsrecht

Grundlage: **Art. 2 Abs. 1 GG**

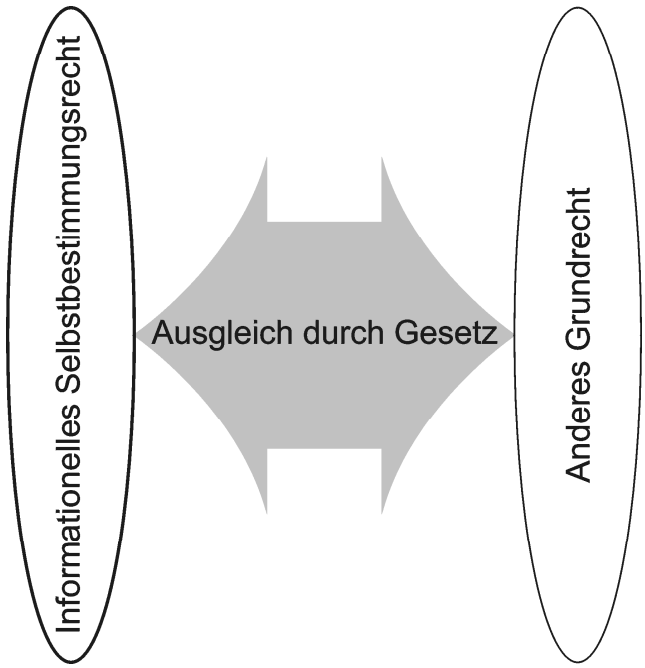
Ausprägungen:

- Informationelles Selbstbestimmungsrecht → Datenschutz
- Urheberrecht → Urheberschutz (§ 2 UrhG)
- Recht am eigenen Namen → Namensschutz (§ 12 BGB)
- Recht am eigenen Bild → Bildnisschutz
  analog: KunstUrhG
  digital: BDSG, soweit KunstUrhG nicht prioritär
- Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

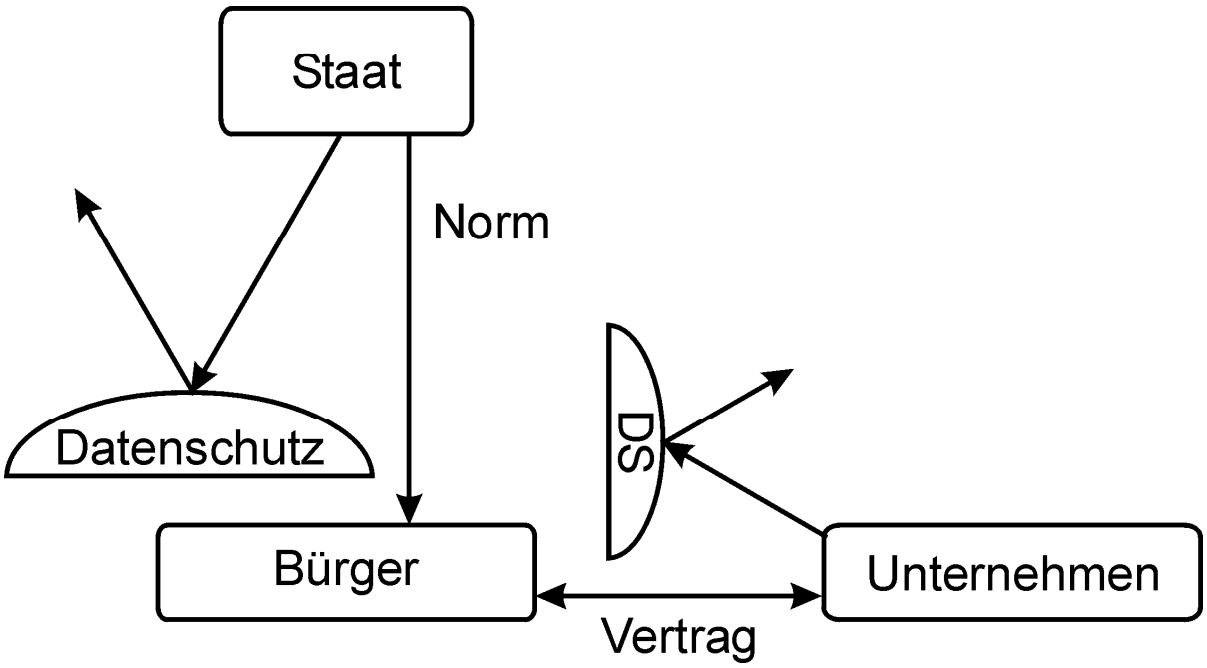
Beschränkung beim „überwiegenden Allgemeininteresse“



Ausgleich zwischen kollidierenden Grundrechten



Ausstrahlungswirkung



Zum „neuen“ Grundrecht (1)

→ Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

- Grundrechte zum Fernmeldegeheimnis (Art. 10 I GG) und zur Unverletzlichkeit der Wohnung (Art. 13 I GG) und zum informationellen Selbstbestimmungsrecht (Art. 2 I GG i.V.m. Art. 1 I GG) vorrangig!
- Hintergrund für neue Ausprägung:
  - allgegenwärtige IT
  - zentrale Bedeutung für Lebensführung vieler Bürger
  - hohe Leistungsfähigkeit vernetzter Systeme

Zum „neuen“ Grundrecht (2)

→ Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

- sog. „Quellen-Telekommunikationsüberwachung“ zur Ausspähung des gesamten Systems geeignet
- Messung elektromagnetischer Abstrahlungen auch zur Überwachung von offline IT-Systemen geeignet
- Zusatzinformationen bzw. Kontextdaten zur umfassenden Persönlichkeitsbewertung geeignet
- „neues“ Grundrecht betrifft nur IT-Systeme, über die eine natürliche Person selbstbestimmt verfügt