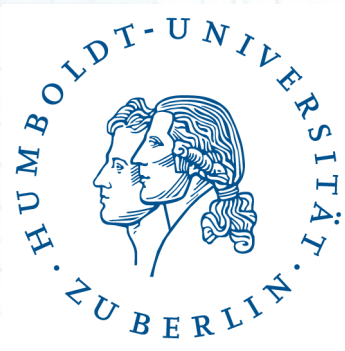
Humboldt Universität zu Berlin
Institut für Informatik
Informatik in Bildung und Gesellschaft



Überwachung, Vorratsdatenspeicherung, Bundestrojaner, Computergrundrecht

Swetlana Klaus
Andreas Grüner

03.06.2009

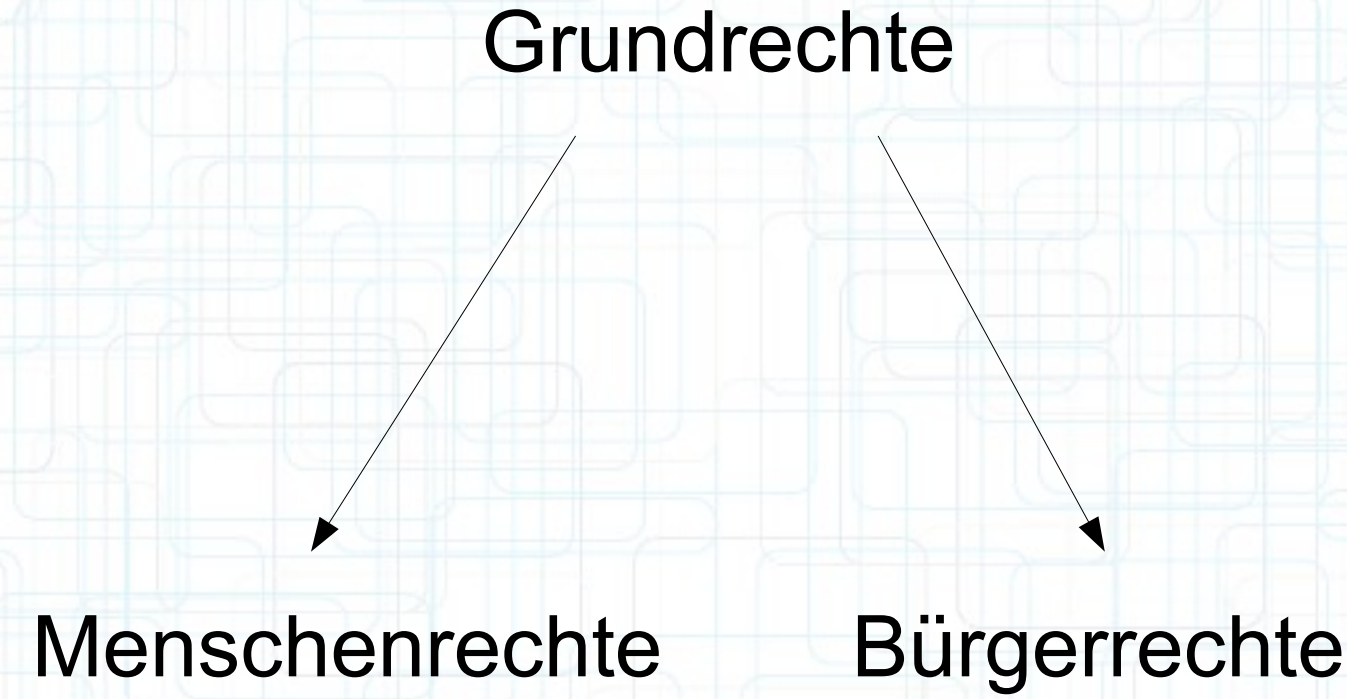
Gliederung

- Einführung Grundrechte
- Telekommunikationsüberwachung
- Vorratsdatenspeicherung
- Online-Durchsuchung / Computergrundrecht

Einführung Grundrechte

- Große Bedeutung für Demokratie
- Grundrechtsfunktionen:
  - Abwehrrecht
  - Nichtdiskriminierung
- Einteilung in verschiedene Grundrechtsarten
- Gültigkeit der Grundrechte

Einführung Grundrechte



Einführung Grundrechte

- Grundrechtseingriff

  „jedes staatliche Handeln, das dem Einzelnen ein Verhalten im Schutzbereich eines Grundrechts versagt oder beschränkt“

- Rechtfertigung des Eingriffs
  - Schranken
  - Schranken-Schranken
- Besonderer Schutz der Grundrechtsordnung

Quelle: http://www.lexexakt.de/glossar/grundrechtseingriff.php

Begriffsbestimmungen

- Inhaltsdaten
- Bestandsdaten
- Verkehrsdaten
- Standortdaten

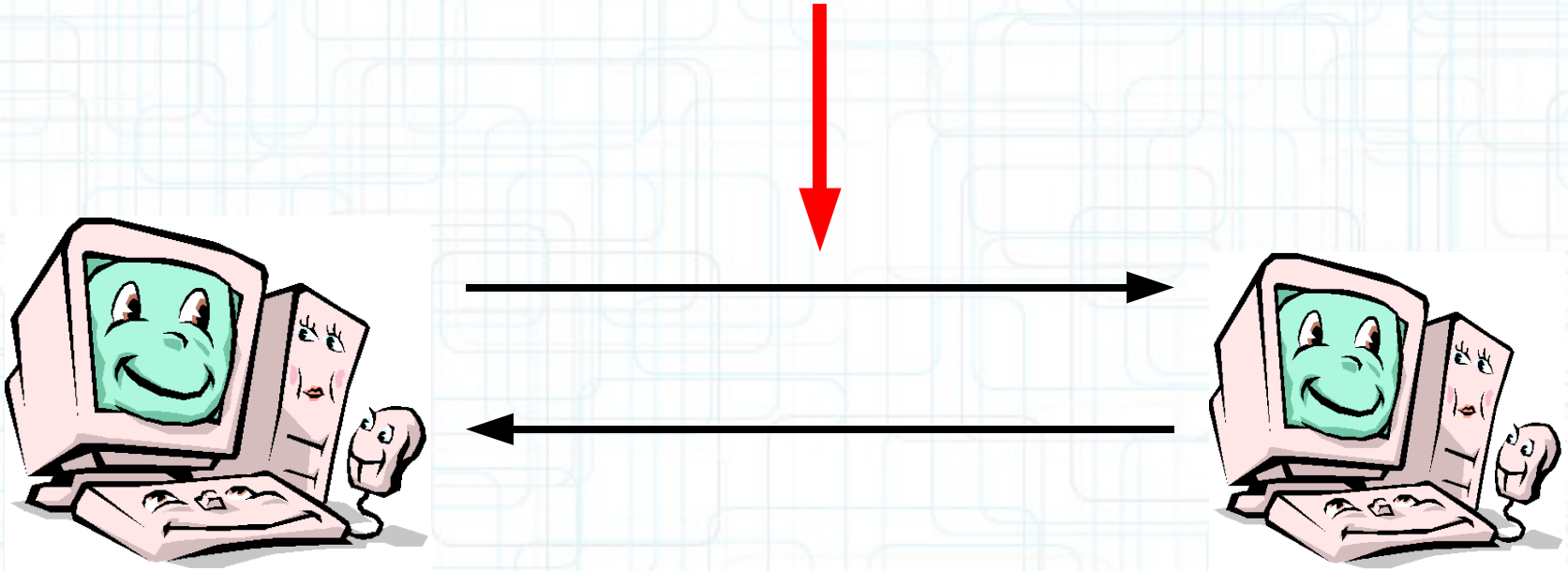
Artikel 10 Grundgesetz

„(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.“

Schutzbereich Art. 10 GG

Inhaltsdaten und Verkehrsdaten



Quelle: http://www.selmigerheide.schulnetz.hamm.de/starnet/media/computer.gif

Telekommunikationsüberwachung

- Strafprozeßordnung (StPo)
  - §100a StPo (Voraussetzungen der Telekommunikationsüberwachung)
  - §100b StPo (Anordnung und Durchführung)
  - §100g StPo (Erhebung von Verkehrsdaten)

Telekommunikationsüberwachung

- Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10-Gesetz)
  - §1 G10-Gesetz (Gegenstand des Gesetzes)
  - §2 G10-Gesetz (Verpflichtungen der Telekommunikationsanbieter)
  - §3 G10-Gesetz (Voraussetzungen)

Telekommunikationsüberwachung

- Anwendung G10 – Gesetz
  - Routinekontrolle (keine Anwendung G10-Gesetz)
  - Strategische Kontrolle (§5 G10-Gesetz)
  - Innerdeutsche Verbindungen (§1 G10-Gesetz)

Vorratsdatenspeicherung

- Speicherung von Verkehrsdaten durch Telekommunikationsdiensteanbieter
- Dauer: 6 Monate
- Relevante Bereiche: Telefonie, E-Mail, Internet-Access
- Gesetzliche Grundlagen: EG-Richtlinie 2006/24/EG und Telekommunikationsgesetz (TKG)

Vorratsdatenspeicherung

- Verpflichtung der Telekommunikationsdiensteanbieter in §113a I TKG
- Zu speichernde Daten:
  - §113a II TKG Telefondienst
  - §113a III TKG E-Mail
  - §113a IV TKG Internetzugangsdienste
- Verwendung gespeicherter Daten nach §113b TKG

Vorratsdatenspeicherung

- Verfassungsmäßigkeit der Vorratsdatenspeicherung noch ungeklärt
  - Unverhältnismäßigkeit
  - Bevölkerung unter Generalverdacht
  - Existenz grundrechtsschonenderer Alternative (Quick-Freeze)
  - Formelle und materielle Mängel der EG Richtlinie
- Verfassungsbeschwerde anhängig

Bundestrojaner: Begriffsklärung

- Online-Durchsuchung
  - Heimlicher Zugriff staatlicher Stellen mittels technischer Mittel auf fremde informationstechnische Systeme
  - Informationstechnisches System
    - System aus Hardware, Software und Daten, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient
  - Online-Durchsicht: Einmalige Durchsuchung
  - Online-Überwachung: Überwachung eines IT-Systems über einen gewissen Zeitraum
- Remote-Forensic-Software (RFS)
  - Interne Bezeichnung des BKA für die zu verwendende Software

Wozu Online-Durchsuchung

- Grenzen von Beschlagnahme und Durchsuchungen
  - Gelöschte Nachrichten und Dokumente
  - Verschlüsselt gespeicherte Daten und Passwortschutz
  - Daten auf leicht zerstör- oder löschbarem Datenträger
- Ziele der Online-Durchsuchung
  - Zugriff auf alle (verschlüsselten) Daten
  - Passwörter, Krypto-Keys

Technische Umsetzungsmöglichkeiten

- Physischer Zugriff
  - Herumliegenlassen / Zusenden von CDs, USB-Sticks, …
  - Wlan, Bluetooth
  - Heimliches Eindringen in Räumlichkeiten
- Zugriff über Kommunikationsnetze
  - Angriffe per E-Mails / Instant-Messages
  - Manipulierte Web-Seiten
  - Ausnutzen von Sicherheitslücken in Programmen oder Betriebssystemen
  - Infektionen von Downloads

Rechtsgrundlage

- 2005-2007 Online-Untersuchungen aufgrund der Dienstanweisungen von Bundesinnenminister
- 31.01.2007 BGH erklärt verdeckte Online-Durchsuchungen für unzulässig
- 20.12.2006 Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen
  - § 5 VSG gestattet zur Informationsbeschaffung:
    - „[...] heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. [...]“
- 27.02.2008 vom BverfG für verfassungswidrig erklärt

Das Computer-Grundrecht

- Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
  - Ist anzuwenden, wenn ein Eingriff Systeme erfasst, die:
    - „ personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.“
- Abgeleitet aus dem allgemeinen Persönlichkeitsrecht
- Schließt Schutzlücken zwischen:
  - Art. 10 GG Telekommunikationsgeheimnis
  - Art. 13 GG Unverletzlichkeit der Wohnung
  - Recht auf informationelle Selbstbestimmung

Abgrenzung zu Art. 10 GG (Telekommunikationsgeheimnis)

- Schutz der laufenden Kommunikation, des Inhalts und der Verbindungsdaten
- Nicht erfasst:
  - Überwachung und Durchsuchung des gesamten Systems, nicht nur Kommunikationsdaten
  - Nach Abschluss eines Kommunikationsvorganges gespeicherte Inhalte und Umstände der Telekommunikation

Abgrenzung zu Art. 13 GG (Unverletzlichkeit der Wohnung)

- Schutz der „räumlichen Sphäre, in der sich das Privatleben entfaltet“
- Schutz vor physischen Eindringen und heimlicher Wahrnehmung der Vorgänge in der als Wohnung geschützten Räumlichkeit
- „kein genereller, von den Zugriffsmodalitäten unabhängiger Schutz vor Infiltration“
- IT-Systeme außerhalb der Wohnung sind nicht geschützt:
  - Eingriffe erfolgen unabhängig vom Standort des Systems

Abgrenzung zum Recht auf informationelle Selbsbestimmung

- Art 2. Abs. 1 i.V.m. Art. 1 Abs. 1 GG
- Schutz von Selbstbestimmung über die Preisgabe und Verwendung persönlicher Daten
  - Volkszählungsurteil 1983
- Schutz vor einzelnen Datenerhebungen
- Nicht geschützt:
  - Zugriff auf das IT-System insgesamt

Eingriffsvoraussetzungen

- Erforderlichkeit
  - Offene Durchsuchung als milderes Mittel vorzugswürdig
- Verhältnismäßigkeit
  - Tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut
- Vorbehalt richterlicher Anordnung
- Schutz des Kernbereichs privater Lebensgestaltung
  - 1. Stufe: Erhebung
    - Zugriffe auf Kernbereichs-Informationen soweit wie möglich vermeiden
  - 2. Stufe: Auswertung
    - Erhobene kernbereichsrelevante Daten sind unverzüglich zu löschen und von der Weitergabe / Verwertung auszuschließen

BKA-Gesetz

- 12.12.2008 Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKA-Gesetz)
- 1.1.2009 in Kraft getreten
- §20 BKA-Gesetz „Verdeckter Eingriff in informationstechnische Systeme“
  - Wichtige Rechtsgüter
  - Richterliche Anordnung
  - Schutz des Kernbereichs
  - Protokollierung
  - Max. 3 Monate

Beweiskraft der Online-Durchsuchung

- Grundlage der IT-Forensik:
  - Das zu untersuchende System, darf nicht mehr verändert werden, es nur an einer Image-Kopie gearbeitet
- Probleme bei Online-Durchsuchungen:
  - Allein das Einbringen einer RFS verändert das System
  - Weitere Veränderungen nicht ausgeschlossen
  - Zuordnung von Daten und Aktivitäten zu einem Verdächtigen technisch nicht belegbar

Weitere Kritikpunkte

- Reichweite der Eingriffe
- IT-Sicherheitsrisiko für den Zielrechner
- Schutz des Kernbereichs privater Lebensgestaltung
- Auswirkungen auf das Vertrauen in die IT-Infrastruktur
- Wenig Erfolg versprechend

Überwachungsstaat

„Wer Sicherheit der Freiheit vorzieht, ist zu Recht ein Sklave.“

Aristoteles

Quellenverzeichnis

Hesselberger, Dieter: Das Grundgesetz. Kommentar für die politische Bildung. 13. Auflage. Bonn: Bundeszentrale für politische Bildung. 2003.

Keller, Christoph: Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen. Suttgart: Richard Boorberg Verlag. 2008.

Riegel, Reinhard: Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses. München: C. H. Beck Verlag. 1997.

Holzner, Stefan: Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts. Kenzingen: Centaurus Verlag. 2009.

Roggan, Fredrik (Hrsg.): Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008. Berlin: BWV Berliner Wissenschaft-Verlag. 2008.

Quellenverzeichnis

Hoeren, Thomas: Internet-Recht.
Internet: http://www.uni-muenster.de/Jura.itm/hoeren/inhalte/lehre/lehrematerialien.htm [02.06.2009].

Bundesministerium des Innern,Fragekatalog des Bundesministeriums der Justiz. 2007.
Internet: http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf [02.06.2009].

Entscheidungen des BVerfG: Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008. Zitierung: BVerfG. 1 BvR 370/07 vom 27.2.2008. Absatz-Nr. (1 – 333). 2008.
Internet: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1 [02.06.2009].