Rechtsfragen der IT Sicherheit

Prof. Dr.-Ing. Dipl.-Math. Bernd Eylert
TH Wildau

Quelle: **Eylert,** Bernd (Hrg.), *Informationssicherheit*, Wildau Verlag 2014, ISBN 978-3-945560-01–6,
Kap. 9, *Rechtsfragen der IT-Sicherheit*, von RA‘in Juliane Holtz

© Prof. Dr. B. Eylert, RA'in J. Holtz

Recht in der Informationssicherheit

- Der Autor hat kurzfristig für den abwesenden Referenten einen themengleichen Vortrag übernommen.
- Eine ausführliche Beschreibung dieses Themas findet sich in

  Eylert, Bernd (Hrg.), *Informationssicherheit*, Wildau Verlag 2014, ISBN 978-3-945560-01-6, Kap. 9, *Rechtsfragen der IT-Sicherheit*, von RA‘in Juliane Holtz

Rechtliche Anforderungen an die IT Sicherheit - Grundrechte

Grundrechte sind Abwehrrechte

- schützen den Bürger gegen hoheitlichen Maßnahmen,
  - in erster Linie vor staatlichen Zugriffen.
  - über die sogenannte *mittelbare Drittwirkung* auch im Privatrecht und damit auch, wenn ein Unternehmen oder Privatpersonen diese Rechte verletzen

Rechtliche Anforderungen an die IT Sicherheit – Grundrechte GG

Grundgesetz

Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG)
Persönlichkeitsrecht
⇒

Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfG, Urteil vom 27. Februar 2008) und

Recht auf informationelle Selbstbestimmung (BVerfG, Urteil vom 15. Dezember 1983 – BVerfGE 65, 1ff.)

Art. 10 Abs. 1 GG
Fernmeldegeheimnis
⇒

Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände (§ 88 Abs.1 Telekommunikationsgesetz (TKG))

Datensicherungspflichten

Rechtliche Anforderungen an die IT Sicherheit - BDSG

Bundesdatenschutzgesetz (BDSG)

Geltungsbereich

öffentlich-rechtliche Institutionen und *natürliche und juristische Personen* des Privatrechts (Privatwirtschaft) (§ 1 Abs. 2 Nr. 3 BDSG)

Datenschutzpflicht

§ 3 Abs. 1, § 9 BDSG

Datenschutzgrundsätze

Zweckbindungsgrundsatz (§§ 28, 29 BDSG)

Erforderlichkeitsgrundsatz

Grundsatz der Datenvermeidung und *Grundsatz der Datensparsamkeit* (§ 3a BDSG)

⇒ Kontrollpflichten

Rechtliche Anforderungen an die IT Sicherheit - BDSG

Kontrollpflichten des Speichernden

- Zutrittkontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle und
- Datentrennungskontrolle

Rechtliche Anforderungen an die IT Sicherheit - BDSG

- Auskunftspflicht (§ 34 Abs. 1 Satz 1 BDSG)
- Löschpflicht (§ 35 Abs. 2 Satz 2 Nr. 1 BDSG)
- Schadensersatzpflicht (§ 7 Satz 1 BDSG)
- Sorgfaltspflicht (§ 7 Satz 2 BDSG)
- Benennung eines Beauftragter für den Datenschutz (§ 4f Abs. 1 BDSG)
- Aufgaben des Beauftragten für den Datenschutz (§ 4g BDSG)

Neu

Die Europäische Datenschutz-Grundverordnung (25. Mai 2018)

s. Vortrag Brückmann

Rechtliche Anforderungen an die IT Sicherheit - TKG

Telekommunikationsgesetz (TKG)

- **Fernmeldegeheimnis und personenbezogene Daten**
  - Betreffen Inhalt der Telekommunikation und ihre näheren Umstände (§ 88 Abs.1 TKG) und
  - Beschaffung und Weitergabe von Inhalt und Umständen (§ 88 Abs. 3 TKG)
- **Diensteanbieter**
  - Geschäftsmäßiger Anbieter von Telekommunikationsdiensten (§ 3 Abs. 6a TKG)
- **angemessene technische Vorkehrungen oder sonstige (Schutz-)Maßnahmen** (§ 109 Abs. 1 TKG)
- **Bestellung eines IT-Beauftragter** (§ 109 Abs. 3 TKG)
- **Anspruch auf Beseitigung und** … **auf Unterlassung sowie auf Schadenersatz** (§ 44 Abs. 1 TKG)
- **Datenschutz in der TK** (§§ 91 – 107 TKG)

Rechtliche Anforderungen an die IT Sicherheit - TKG

Besonderheit:

Speicherung von Verbindungsdaten und die Verwendung dieser gespeicherten Daten (§§ 113a, 113b TKG)

Gesetz zur Speicherung von Telekommunikationsdaten (Richtlinie 2006/24/EG vom 15. März 2006)

⇒

Nichtigkeitsurteil des BVerfG 2010, Urteil vom 02. März 2010 (https://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html)

*Mit Entscheidung des EuGH jetzt auch **EU-Recht!***

Rechtliche Anforderungen an die IT Sicherheit - TMG

Telemediengesetz (TMG)

Telemedien (§ 1 TMG)

alle elektronischen Informations- und Kommunikationsdienste mit Ausnahme der Telekommunikationsdienste und des Rundfunks. Dazu zählen

- Internetangeboten
- Webshops, Webportale
- Online-Banking
- Informationsdienste
- Chatrooms, Websites und Blogs.

Diensteanbieter (§ 2 TMG)

„jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“

Auskunftsrecht (§ 14 Abs. 2 TMG)

Erhebung und Verwendung personenbezogener Daten (§ 12 Abs. 1 und 3 TMG)

Rechtliche Anforderungen an die IT Sicherheit - StGB

Strafgesetzbuch (StGB)

Aufbewahrungspflichten von Handelsbriefen (§ 283b StGB)

Datenveränderung (§ 303a StGB)

Rechtliche Anforderungen an die IT Sicherheit - KonTraG

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Das KonTraG legt dem Vorstand einer Aktiengesellschaft und der Geschäftsführung einer GmbH die Verpflichtung auf, geeignete Sicherungsmaßnahmen zur frühzeitigen Erkennung von Entwicklungen zu treffen, die den Fortbestand der Gesellschaft gefährden können.

Beruht auf dem Aktiengesetz (AktG)…

Rechtliche Anforderungen an die IT Sicherheit – EG

EU Richtlinien

Gesetz zur Speicherung von Telekommunikationsdaten (Richtlinie 2006/24/EG vom 15. März 2006) [bisher in D nicht umgesetzt!]

Regeln für die Eigenkapitalanforderungen des Basler Ausschusses für Bankenaufsicht (Basel II) (Richtlinien 2006/48/EG und 2006/49/EG)
⇒
Mindestanforderungen an das Risikomanagement – MaRisk [umgesetzt in dt. Recht]

EuroSOX (Richtlinie 2006/43/EG)
⇒
Bilanzrechtsmodernisierungsgesetz (BilMoG) [umgesetzt in dt. Recht]

Rechtliche Anforderungen an die IT Sicherheit – US

Sarbanes-Oxley Act (SOX)

Definition und Festlegung von Unternehmensprozessen und Kontrollverfahren, sowie wirksamer interner Kontrollsysteme für Datensicherheit und Backup.
[Betrifft zunächst nur US-amerikanische Unternehmen bzw. Unternehmen, die (auch) in den USA registriert sind]

Rechtliche Anforderungen an die IT Sicherheit - AktG

Aktiengesetz (AktG)

- Einrichtung eines *Überwachungssystems* (§ 91 Abs. 2 AktG i. V. m. § 317 Abs. 4 HGB)
- Haftung und Schadensersatz (§ 93 Abs. 2 AktG)

Archivierungspflichten

Rechtliche Anforderungen an die IT Sicherheit - Handelsrecht

Handelsgesetzbuch (HGB)

- Kaufmannseigenschaft (§§ 1ff. HGB)
- Revisionssicherheit (§ 239 Abs. 3 HGB i .V. m. § 146 Abs. 4 AO)
- Archivierungspflichten (§ 257 Abs. 1 HGB)
- Einrichtung eines *Risikofrüherkennungssystems* (bei börsennotierten Aktiengesellschaften) (§ 317 Abs. 4 HGB)

Rechtliche Anforderungen an die IT Sicherheit - Steuerrecht

Abgabenordnung (AO)

- Archivierungspflicht
  - handelsrechtlich aufzubewahrenden Unterlagen (§ 147 Abs. 1 AO)
  - Unterlagen, die für die Besteuerung von Bedeutung sind (§ 147 Abs. 1 Nr. 5 AO)
- Verstoß erzwingt
- Schätzung der Besteuerungsgrundlagen (§ 162 AO)
- Revisionssicherheit (§ 146 Abs. 4 AO i .V. m. § 239 Abs. 3 HGB)

Rechtliche Anforderungen an die IT Sicherheit - Buchführung

Grundsätze ordnungsgemäßer Datenverarbeitungs (DV)-gestützter Buchführungssysteme (GoBS)

⇒ nicht rechtlich bindend, aber Handelsbrauch

Anpassen des Datensicherheitskonzepts an die technische Entwicklung und den Stand der EDV-Technik des Unternehmens (Nr. 5 GoBS)

internes Kontrollsystem (IKS) (Nr. 4 der GoBS)

Rechtliche Anforderungen an die IT Sicherheit – Betriebsprüfung

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)

Erlass der Finanzverwaltung, beinhaltet u. a. die Verfügbar- und unverzüglich Lesbarmachung von steuerrelevanten Unterlagen gemäß §§ 146 Abs. 5, 147 Abs. 6 AO

Rechtliche Anforderungen an die IT Sicherheit - BGB

Bürgerliches Gesetzbuch (BGB)

- Aufbewahrungspflichten, die bei der Aufrechterhaltung der IT-Sicherheit zu beachten sind (§§ 259, 666, 667 BGB)
- Rechtsgüterabwägung (§ 241 Abs. 2 BGB)

Rechtliche Anforderungen an die IT Sicherheit - ZPO

Zivilprozessordnung (ZPO)

funktionstüchtiges Archivierungssystem für Beweissicherungszwecke (§§ 415 ff. ZPO) [um bei gerichtlichen Streitigkeiten den Vorlegungspflichten und der Beweislast Genüge tun zu können]

Verkehrssicherungspflichten

Rechtliche Anforderungen an die IT Sicherheit - StGB

Strafgesetzbuch (StGB)

- **Verschwiegenheitspflicht bes. Berufe** (§ 13 StGB)
  - Ärzte, Zahnärzte, Apotheker und Angehörige anderer Heilberufe
  - Berufspsychologen
  - Rechtsanwälte, Notare, Wirtschaftsprüfer und Steuerberater
  - staatlich anerkannte Sozialarbeiter und Sozialpädagogen
  - Amtsträger (z.B. Beamte, Richter)
  - Datenschutzbeauftragte
- **Datenverarbeitung zum Schutz vertraulicher Informationen** (§ 203 StGB)
- **Datenveränderung** (§ 303a StGB)

Rechtliche Anforderungen an die IT Sicherheit - UWG

Gesetzes gegen den unlauteren Wettbewerb (UWG)

Verrat von Geschäfts- und Betriebsgeheimnissen (§ 17 UWG)

Rechtliche Anforderungen an die IT Sicherheit - KWG

Gesetzes über das Kreditwesen (KWG)

Kredit- und Finanzdienstleistungsinstitute haben besondere **organisatorische Pflichten**, im Speziellen eine **angemessene personelle und technisch-organisatorische Ausstattung** des Instituts im Rahmen eines **angemessenen und wirksamen Risikomanagements** (§ 25a Abs. 1 Nr. 2 KWG)

Rechtliche Anforderungen an die IT Sicherheit - Verträge

Einhaltung vertragliche Vereinbarungen

- **Geheimhaltungsverträge** (non-disclosure agreement, NDA)
- **Softwarehinterlegungsvereinbarungen** (Escrow Agreement)
- **IT-Outsourcing**

Haftungsrisiken und strafrechtliche Verantwortung

Rechtliche Anforderungen an die IT Sicherheit - Haftungsfragen

Urheberrechtsgesetz (UrhG)

- Anspruch auf Beseitigung der Beeinträchtigung, bei Wiederholungsgefahr auf Unterlassung, sowie auf Schadensersatz (§ 97 UrhG)
- Ansprüche gegen den Inhaber oder die Inhaberin eines Unternehmens, wenn ein Arbeitnehmer oder Beauftragter des Unternehmens das Urheberrecht verletzt hat (§ 99 UrhG)
- Urheberrechtverletzungen, z.B. durch Kopieren der Software des Unternehmens, Nutzung von nicht lizensierter Software und Filesharingprogrammen seitens des Arbeitnehmers (§ 106 UrhG)

⇒ Schutz des Telekommunikationsanschlusses durch angemessene Sicherungsmaßnahmen durch die Begehung von Rechtsverletzungen von außenstehenden Dritten (WLAN-Urteil des BGH vom 12. Mai 2010 – I ZR 121/08)

Rechtliche Anforderungen an die IT Sicherheit – Haftungsfragen

Bürgerliches Gesetzbuch (BGB)

- Anspruch auf Schadensersatz bei Verletzung des allgemeinen Persönlichkeitsrechts aufgrund unzulässiger Behandlung personenbezogener Daten (§ 823 Abs. 1 BGB)
- Haftung für den Verrichtungsgehilfen (§ 831, Exkulpationsmöglichkeit gem. § 831 Abs. 1 S. 2 BGB)

Rechtliche Anforderungen an die IT Sicherheit – Strafrechtsfragen

Strafgesetzbuch (StGB)

- Ausspähen von Daten, § 202a StGB
- Verletzung von Privatgeheimnissen § 203 StGB
- Datenveränderung, § 303a StGB
- Computersabotage, § 303b StGB
- Fälschung beweiserheblicher Daten, § 269 StGB
- Unterdrückung beweiserheblicher Daten, § 274 Abs. 1 Nr. 2 StGB
- Fälschung technischer Aufzeichnungen, § 268 StGB
- Unterdrückung technischer Aufzeichnungen, § 274 Abs. 1 Nr. 1 2. Alt. StGB
- Verletzung des Fernmeldegeheimnisses, § 206 StGB
- Schutz der Vertraulichkeit personenbezogener Daten, § 44 Abs. 1 i. V. m. § 43 Abs. 2 BDSG
- Computerbetrug, § 263a StGB
- Störung von Telekommunikationsanlagen, § 317 StGB

Rechtliche Anforderungen an die IT Sicherheit – Strafrechtsfragen

Jugendmedienschutz-Staatsvertrag (JMStV)

- Verbot, Angebote mit Inhalten kriegsverherrlichender, menschenverachtender, nationalsozialistischer und pornographischer Art anzubieten
- Sanktion: Bußgeld von €500.000 § 24 Abs. 3 JMStV

Arbeitsrechtliche Aspekte

Rechtliche Anforderungen an die IT Sicherheit – Arbeitsrecht

Betriebsverfassungsgesetz (BetrVG)

- Befugnis zur privaten Nutzung des Internets muss ausdrücklich erlaubt sein, sonst verboten. Der Betriebsrat (BR) hat ein Mitspracherecht (§ 87 Abs. 1 Nr. 1 BetrVG)!
- Verstoß kann zur Kündigung führen, BR ist anzuhören (§ 102 Abs. 1 BetrVG)!
- Überwachung der nicht öffentlich zugänglichen Arbeitsbereiche mit optisch-elektronischen Einrichtungen ⇒ Neuregelung des Beschäftigtendatenschutzes (§ 32f BDSG-E i. V. m. § 87 Abs. 1 Nr. 6 BetrVG)

anlassunabhängige Internetrecherche

1. Ermächtigungsgrundlage für die anlassunabhängige Internetrecherche ist die Gefahrenabwehr zur Verhinderung von Gefahren für die öffentliche Sicherheit und Ordnung.
   - Generalklausel in den Polizeigesetzen der Länder
   - Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) des BKA gem. § 2 Abs. 2 Nr. 1 i. V. m. § 2 Abs. 1 BKAG

2. Werden die Ermittler fündig und haben einen konkreten Anfangsverdacht, richten sich die Voraussetzungen für Ermittlungen und für eine Beweiserhebung als Grundlage zur Erhebung von Verkehrsdaten nach dem Telekommunikationsgesetz (TKG) und der Strafprozessordnung (StPO). Insbesondere sind hier die Vorschriften § 100g StPO und § 113 TKG zu nennen.

anlassunabhängige Internetrecherche

§ 100a

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als **Täter** oder **Teilnehmer** eine in Absatz 2 bezeichnete **schwere Straftat** begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

…

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

anlassunabhängige Internetrecherche

Nach § 100b Abs. 1 StPO dürfen Maßnahmen nach § 100a **nur auf Antrag** der Staatsanwaltschaft **durch das Gericht** angeordnet werden. Bei **Gefahr im Verzug** kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft.

Sehr interessant und zum Lesen empfehlenswert: BVerfG-Urteil vom 27. Februar 2008, aus welchem sich auch das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität** informationstechnischer Systeme entwickelt hat;
(http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html).

Rechtsquellenverzeichnis 1

AktG Aktiengesetz
http://www.gesetze-im-internet.de/bundesrecht/aktg/gesamt.pdf

AO Abgabenordnung
http://www.gesetze-im-internet.de/bundesrecht/ao_1977/gesamt.pdf

BDSG Bundesdatenschutzgesetz
http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf

BDSG-E Bundesdatenschutzgesetz Entwurf
http://www.bmi.bund.de/cae/servlet/contentblob/1286172/publicationFile/95297/Entwurf_Beschaeftigtendatenschutz.pdf

BetrVG Betriebsverfassungsgesetz
http://www.gesetze.juris.de/bundesrecht/betrvg/gesamt.pdf

BGB Bürgerliches Gesetzbuch
http://www.gesetze-im-internet.de/bundesrecht/bgb/gesamt.pdf

BilMoG Bilanzrechtsmodernisierungsgesetz
http://www.buzer.de/gesetz/8755/l.htm

GS-DVO Europäische Datenschutz-Grundverordnung

GDPdU Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
http://www.bundesfinanzministerium.de/DE/Wirtschaft__und__Verwaltung/Steuern/Veroeffentlichungen__zu__Steuerarten/Abgabenordnung/Datenzugriff__GDPdU/002,templateId=raw,property=publicationFile.pdf

Rechtsquellenverzeichnis 2

GG Grundgesetz
http://www.gesetze-im-internet.de/bundesrecht/gg/gesamt.pdf

GoBS Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
http://www.bundesfinanzministerium.de/nn_314/DE/BMF__Startseite/Service/Downloads/Abt__IV/BMF__Schreiben/015,templateId=raw,property=publicationFile.pdf

HGB Handelsgesetzbuch
http://www.gesetze.juris.de/bundesrecht/hgb/gesamt.pdf
JMStV Jugendmedienschutz-Staatsvertrag
http://www.landesrecht-bw.de/jportal/?quelle=jlink&query=JMedienSchStVtrG+BW&psml=bsbawueprod.psml&max=true&aiz=true

KonTraG Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
Bundesgesetzblatt I Nr. 24 vom 30.04.1998, S. 786

KWG Gesetz über das Kreditwesen
http://www.gesetze.juris.de/bundesrecht/kredwg/gesamt.pdf

Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF

Rechtsquellenverzeichnis 3

Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0087:0087:DE:PDF

Richtlinie 2006/48/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (Neufassung)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:177:0001:0001:DE:PDF

Richtlinie 2006/49/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten (Neufassung)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:177:0201:0201:DE:PDF

SigG Signaturgesetz
http://www.gesetze-im-internet.de/bundesrecht/sigg_2001/gesamt.pdf

SigV Signaturverordnung
http://www.gesetze-im-internet.de/bundesrecht/sigv_2001/gesamt.pdf

StGB Strafgesetzbuch
http://www.gesetze-im-internet.de/bundesrecht/stgb/gesamt.pdf