Prof. Dr. Marc Strittmatter

HTWG Konstanz, Of-Counsel Vogel & Partner, Stuttgart

Sicherheit im Cloud Computing

- Rechtsbegriff
- Zugriffsbefugnisse von (US-) Behörden

Bird&Bird LawCamp 2013, Frankfurt am Main, 20.04.2013

Datensicherheit - Realität und Wahrnehmung

*“Das Bedürfnis nach **Datensicherheit** bringt Cloud Anbietern ein hübsches Verkaufsargument und Juristen lukrative Beratungsarbeit. Ob all der Schutz nötig ist, weiß keiner.”*

Zitiert nach ?

- ☑ BITKOM Leitfaden Cloud Computing
- ☑ Parteiprogramm der Piratenpartei
- ☑ FAZ vom 06.03.2012
- ☑ taz vom 16.03.2012

Fragen

- Was leistet der rechtliche Begriff der *Sicherheit*, insbesondere in Cloud Verträgen, Gesetzen und VOen ?
- Ist die verbreitete Einschätzung, Cloud-Anbieter mit US Bezug wegen mangelnder *Sicherheit* vor behördlichen Zugriffen zu meiden, rechtlich gut begründet ?

Thesen

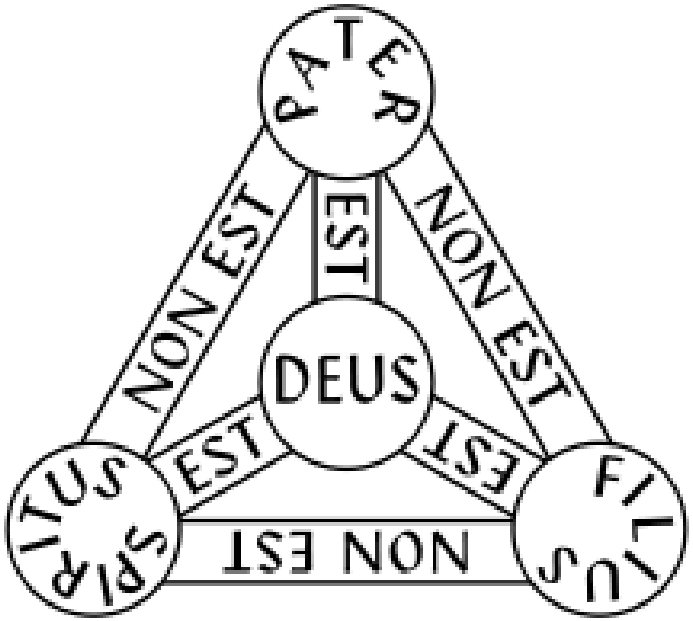
1. Es gibt keinen einheitlichen rechtlichen Sicherheitsbegriff. Sicherheitsbegriffe im Recht sind abstrakt-normativ statt objektiv oder risiko-/ schutzgutabhängig

2. Was als „sicher“ gilt, sollte ökonomisch-empirischen Rationalen wie der Relation von Gefahr und Schadenspotential (Risiko) folgen

3. Die Entscheidung für oder gegen einen bestimmten Cloud Provider sollte nicht primär auf Rechtsargumenten beruhen („USA“)

4. Der Anspruch auf Schutz durch Gesetzgeber und Datenverarbeiter steht in keinem ausgewogenen Verhältnis zur freiwilligen Selbstgefährdung der Datensubjekte und IT-Nutzer

Sicherheit - Ontologie



(Christliche Dreifaltigkeitslehre)

***äußerer Text*: Der Vater ist nicht der Sohn, der Sohn ist nicht der Heilige Geist, der Heilige Geist ist nicht der Vater;**

***innerer Text*: Der Vater ist Gott; der Sohn ist Gott; der Heilige Geist ist Gott**

Quelle: http://de.wikipedia.org/wiki/Ontologie

Verständnis von Sicherheit: „Ontologische Differenz“ zwischen Zustand und kategorisierender Einordnung

Sicherheitsbegriff - Rechtsquellen

1. Datenschutz RL 1995
2. BDSG
3. DS-GrundschutzVO 2012
4. GenTG
5. AtomG
6. LuftVG
7. GPSG 2004
8. MPG
9. BSI Standards
10. EU Paper z. Cloud Computing
11. ..[uvam]

Technikklauseln:

- Anerkannte Regeln der Technik
- Stand der Technik
- Stand von Wissenschaft und Technik

Sicherheit als ökonomisches Optimierungsproblem

Ziel: Optimale volkswirtschaftliche Ressourcenallokation

Aufwand für Schutz-maßnah-men	Erwarteter Schaden (Scha-denshöhe * Wahr-scheinlichkeit)	Gesellschaftliche Gesamtkosten
0	+ 40	= 40
10	+ 25	= **35**
20	+ 20	= 40

Quelle: *Spindler*, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären, Göttingen/ BSI 2007

Stochastische Sicherheitstheorie (1)

- **Begriffe:**
  1. Wertobjekte
  2. Gefahr, Bedrohung, Gefährdung [„Gefahr“]
  3. Schaden
  4. Risiko

Wertobjekte in der IT: Persönlichkeitsrechte, Geschäftsgeheimnisse, Ausfallsicherheit/ betriebliche Funktionalität, Spionageabwehr, Wettbewerbsfähigkeit, Attraktivität als Wirtschaftsstandort, etc.

Gefahr: abhängig von Sensitivität der Information, Infrastruktur und Nutzerverhalten

Schaden: abhängig vom Schadpotential: Materielle und immaterielle Schäden

Risiko: → **Relevante Größe**

Stochastische Sicherheitstheorie (2)

„Als Risiko ℜ (R Fraktur) bezeichnen wir den mittleren relativen Schaden an einem Wertobjekt über einem definierten Zeitraum, wobei der relative Schaden durch das Verhältnis von Schaden zu Anfangswert definiert ist.“

Sei $\mathbf{V}$: $t \mapsto \mathbf{V}(t)$ mit $t \in \mathbb{R}_0$ ein Wertänderungsprozess. Dann lässt sich das Risiko $\mathfrak{R}_V$: $\mathbb{R}^2 \rightarrow \mathbb{R}$ über einem Zeitraum $[t_1,t_2] \subset \mathbb{R}_0$ definieren als Erwartungswert der Änderung des Wertänderungsprozesses

$$\mathfrak{R}_V(t_1,t_2) \equiv \mathbf{E}\{\mathbf{V}(t_2) - \mathbf{V}(t_1)\} = \mathbf{E}\{\mathbf{V}(t_2)\} - \mathbf{E}\{\mathbf{V}(t_1)\}$$

wenn die Bedingung $\mathbf{V}(t) \rightarrow 1$ $(t > 0)$ einem vollständigen Wertverlust relativ zum Zeitpunkt 0 entspricht.

Quelle: Bromba, Stochastische Sicherheitstheorie, http://www.bromba.com/knowhow/Was_ist_Sicherheit.htm

Stochastische Sicherheitstheorie (3)

"Das Risiko einer Anlage oder Tätigkeit ist die Summe über alle (gefährlichen) Ereignisse der Produkte von Eintrittswahrscheinlichkeit und Schadensausmaß und eventuell (subjektiven) Gewichtungsfaktoren."

- **Eintrittswahrscheinlichkeit:** empirisch zu betrachten:
  - vertragliche Zusagen
  - providerabhängig
- **Schadensausmaß:**
  - geringe materielle Schadenshöhe bei einfachen pers.bez. Daten (z.B. Email Adresse),
  - große materielle Schadenshöhe bei Unternehmensdaten (z.B. kursrelevante Tatsachen)
- **Subjektive Gewichtungsfaktoren** (Rechtspolitische Erwägungen):
  - Gesellschaftspolitische Ziele
  - Ordnungs-/ wirtschaftspolitische Ziele
  - Verhältnis zu sonstigen (akzeptierten) Bedrohungen (freiw. Selbstgefährdung)
  - Sonstige ?

Stochastische Sicherheitstheorie (4)

"Das Risiko einer Anlage oder Tätigkeit ist die Summe über alle (gefährlichen) Ereignisse der Produkte von Eintrittswahrscheinlichkeit und Schadensausmaß und eventuell (subjektiven) Gewichtungsfaktoren."

- **Fragen bei der Normierung von Sicherheitsbegriffen im IT Recht:**
  - Welche Wertobjekte sind betroffen ?
  - Welche (mittleren) Schadenshöhen sind zu beobachten ?
  - Wie häufig treten diese Schäden ein ?
  - Welche subjektiven Gewichtungsfaktoren sollen Gesetzgeber sinnvollerweise einbeziehen ?

Sicherheitsbegriffe im Recht (1)

1. Spezialgesetzliche Regelungen: AtomG, LuftVG, ProdSG, GenTG
2. Datenschutzrecht (Anl. zu § 9 BDSG bei Auftragsdatenverarbeitung)
3. Strafrecht (z.B. § 203 I Nr. 6 StGB - Schutz von Privatgeheimnissen)
4. Quasi-Regulatorische Ansätze

→ Sicherheitsanforderungen werden im Recht anhand von Techniklauseln generalklauselartig beschrieben

→ Unterschiedlichste Schutzzwecke und Risikolagen

→ Keine “Einheit der Rechtsordnung” bei Sicherheitsbegriffen

Sicherheitsbegriffe im Recht – Luftfahrt (2)

1. **Unterscheidung von „Safety“ and „Security“**

2. **Safety Definition ICAO (International Civil Aviation Organisation) Doc. 9859:**

   “Safety is the state in which the risk of harm to persons or property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management”.

3. **Safety Definition IS-BAO (International Standard for Business Aviation Operators) :**

   “The state in which the risk of harm or damage is limited to an acceptable level as low as reasonably practicable („ALARP“) ”.

4. **LuftverkehrsG:** nennt Sicherheit ohne Definition zu geben.

Kategorien: Akzeptanz, vernünftige Praktikabilität, Risikomanagement

Sicherheitsbegriffe im Recht – Luftfahrt (3)

4.0 Global Accident Rate Data

4.1 Accident Rate by Aircraft Type

The accident rate per 100,000 flight hours for each year over a five year period, as well as for the total, is as follows:

Accident Rate per 100,000 hours by Aircraft Type												
	2006		2007		2008		2009		2010		5 Year Total	
	Acc Rate	Fatal Rate	Acc Rate	Fatal Rate	Acc Rate	Fatal Rate	Acc Rate	Fatal Rate	Acc Rate	Fatal Rate	**Acc Rate**	**Fatal Rate**
Business Jets	0.69	0.13	0.63	0.13	0.69	0.14	0.37	0.08	0.48	0.10	**0.64**	**0.14**
Turbo props	1.39	0.41	1.6	0.56	2.11	0.78	0.70	0.46	1.64	0.29	**1.70**	**0.50**
All Bus A/C	1.01	0.26	1.05	0.32	1.29	0.38	0.90	0.24	0.99	0.18	**1.13**	**0.30**

Table 4.1a

Quelle: http://www.ibac.org/wp-content/uploads/2010/07/businessaviationsafetybriefissue9.pdf

Sicherheitsbegriffe im Recht - Gentechnik (4)

§ 7 Sicherheitsstufen, Sicherheitsmaßnahmen

(1) Gentechnische Arbeiten werden in **vier Sicherheitsstufen** eingeteilt:

1. Der Sicherheitsstufe 1 sind gentechnische Arbeiten zuzuordnen, bei denen nach dem Stand der Wissenschaft nicht von einem Risiko für die menschliche Gesundheit und die Umwelt auszugehen ist.

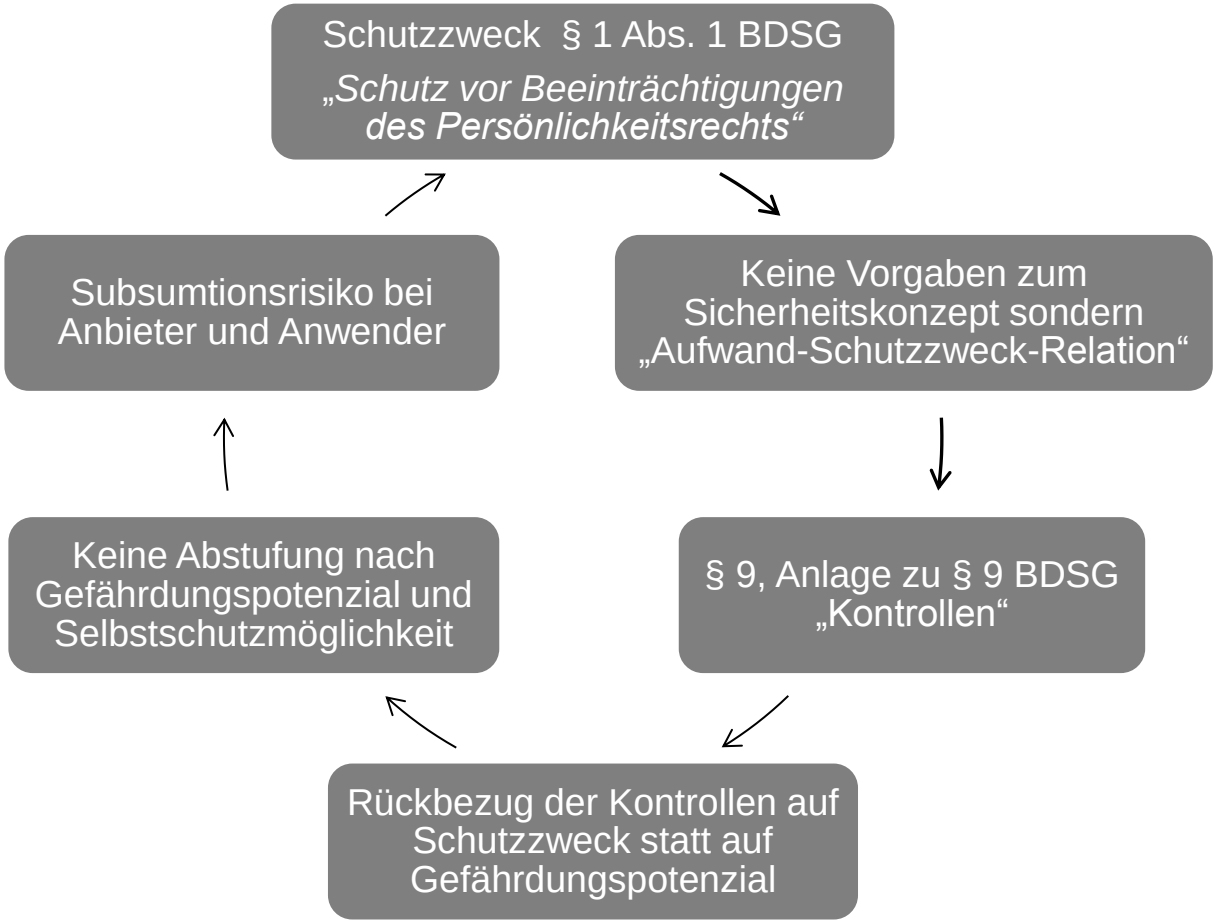
2. Der Sicherheitsstufe 2 sind gentechnische Arbeiten zuzuordnen, bei denen nach dem Stand der Wissenschaft von einem geringen Risiko für die menschliche Gesundheit oder die Umwelt auszugehen ist.

3. Der Sicherheitsstufe 3 sind gentechnische Arbeiten zuzuordnen, bei denen nach dem Stand der Wissenschaft von einem mäßigen Risiko für die menschliche Gesundheit oder die Umwelt auszugehen ist.

4. Der Sicherheitsstufe 4 sind gentechnische Arbeiten zuzuordnen, bei denen nach dem Stand der Wissenschaft von einem hohen Risiko oder dem begründeten Verdacht eines solchen Risikos für die menschliche Gesundheit oder die Umwelt auszugehen ist.

Kategorien: Risikopotential der gentechnischen Arbeit, Verfügbarkeit von Gegenmaßnahmen (§ 7 Abs. 1 GenTG (Forts.),
Anforderung: Stand von Wissenschaft und Technik) (§ 7 Abs. 2 GenTG)

Datensicherheit bei ADV (§§ 1, 9, 11, Anl. §9 BDSG)



→ „The missing link“ : Integration der Risikobetrachtung

Art. 30 Entwurf Datenschutz GVO

- **Artikel 30 Sicherheit der Verarbeitung**
- **1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter**
- **Berücksichtigung des Stands der Technik und der Implementierungskosten technische und organisatorische Maßnahmen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.**
- **Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen im Anschluss an eine Risikobewertung die in Absatz 1 genannten Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder widerrechtlichen Zerstörung oder vor unbeabsichtigtem Verlust sowie zur Vermeidung jedweder unrechtmäßigen Verarbeitung, insbesondere jeder unbefugten Offenlegung, Verbreitung beziehungsweise Einsichtnahme oder Veränderung.**
- **3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen für die in den Absätzen 1 und 2 genannten technischen und organisatorischen Maßnahmen festzulegen und den aktuellen Stand der Technik für bestimmte Sektoren und Datenverarbeitungssituationen zu bestimmen, wobei sie die technologische Entwicklung sowie Lösungen für einen Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen berücksichtigt, sofern nicht Artikel 4 gilt.**

Zwischenfazit

- Risikobezug ist der richtige Ansatz, der mit dem Konzept der Technikklauseln kombiniert werden kann (vgl. Art. 30 DS GVO Entwurf)
- *Diligentia quam in suis* als Regulativ ? *(„.. jedoch keine höheren Anforderungen als der Auftraggeber durch seine eigenen nachgewiesenen Sicherheitsmaßnahmen praktiziert*“).
- Technische Realität entfernt sich schneller vom Regulierungsansatz als das DS Recht fortentwickelt („entrümpelt“) wird Vollzugsdefizit
- Markt löst das Problem durch Ignorieren oder Selbst-/ Drittzertifizierung

Die Diskussion um den US Patriot Act 2001

- **Foreign Intelligence Surveillance Act (FISA) datiert von 1978**
- **Verschärfung durch „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act („US Patriot Act“) 2001, insb. durch:**
  - Herausgabe von Unterlagen und Informationen aller Art („all tangible things“) von Anbietern
  - Ausreichend, dass Daten „in Verbindung mit einer Untersuchung über Terrorismus oder Spionage in Verbindung“ stehen.
  - National Security Letters können Herausgabe von Daten ohne Vorschaltung eines Gerichtsbeschlusses anordnen
  - „gag orders“ -> Vertraulichkeitsverfügung, dass eine NSL erhalten wurde (vgl. Google Fall aus März 2013 -> Transparenzbericht)
  - Microsoft Law Enforcement Report 2012

Die Diskussion um den US Patriot Act 2001

Problem 1: Datensubjekt/ Cloud Nutzer

- Bedeuten die Zugriffsmöglichkeiten nach FISA eine Verschärfung der Sicherheitslage bei der Cloud Speicherung von Daten ?
- Haftet der Nutzer (AG) nach § 11 Abs. 2 S. 4, 7 BDSG weiß, dass seinem Provider das Dilemma der NSL/ FISA orders droht oder dieser gar kundgetan hat, dass er sich US-rechtskonform verhalten wird ?

Die Diskussion um FISA/ US Patriot Act 2001 (2)

Hogan Lovells White Paper 20. Juli 2012 (S. 13),
Fragen und Länder:

May government require a Cloud provider to disclose customer data in the course of a government investigation?	May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?	If a Cloud provider must disclose customer data to the government, must the customer be notified?	May government monitor electronic communications sent through the systems of a Cloud provider?	Are government orders to disclose customer data subject to review by a judge?*	If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose the data?

- Untersuchte Länder: Australien, Kanada, Dänemark, Frankreich, Deutschland, Irland, Japan, Spanien, UK, USA

- Zugriffsbefugnisse relativ ähnlich ausgestaltet

Die Diskussion um den US Patriot Act 2001 (3)

Problem 2: Cloud Provider mit US Bezug: Dilemma rechtskonformen Verhaltens bei NSL/ FISA order – wirklich ein neues Problem ?

- Problem: Datenübermittlung ins Ausland und an Behörde nach Herausgabeverlangen z.B. des FBI an US Mutter oder US Tochter mit Konzerngesellschaften oder Serverstandorten in Europa
- Eckpunkte: §§ 4, 4a, 4b, 4c, 28 BDSG
- Übertragung ins Ausland: § 4b Abs. 2 BDSG angemessenes DS Niveau (-)
- Ausnahmetatbestand § 4c I Nr. 4 : öffentliches Interesse, Gerichtsverfahren (-)
- Einwilligung oder Erlaubnistatbestände nach § 28 BDSG ?
  - § 28 II Nr. 2 lit. a BDSG: Wahrung berechtigter Interessen eines Dritten ?
  - § 28 II Nr. 2 lit. b: Gefahrenabwehr: str.

→ Bruch einer der beiden Vorgaben: FISA/ NSL oder §§ 4, 28 BDSG, → „Compliance Problem“, Aber was war seit 2002 (insb. global Outsourcing) ?

Schluß

- Das positive Recht bietet derzeit zum Begriff der Sicherheit technologieneutrale, risikounabhängige Generalklauseln an. Eine zusätzlich am Risiko orientierte Begriffsbildung ist sinnvoll.
- Das Nutzerverhalten und die „Sorgfalt in eigenen Angelegenheiten“ ist im Verhältnis zu den vermeintlichen externen Risiken bei Cloud Computing ein unterbewerteter Faktor (derzeit nur zivilrechtlich berücksichtigt)
- Die Diskussion um den US Patriot Act 2001 ist interessant, die Rechtslandschaft ist diesbezüglich indes seit 2001 weitgehend unverändert. Das Problem ist also nicht neu, es sollte auf durch die Juristen richtig eingeordnet werden („rightsizing“)
- Eine Anpassung des Datenschutzrechts an die Anforderungen einer globalisierten Datenwelt scheint mehr denn je erforderlich

Fragen

Antworten:
Rechtsanwalt Prof. Dr. Marc Strittmatter
Mail: ms@vogel-partner.eu
M: +49 173 3 111 333