Rechtsanwalt Dr. Falk Peters, Berlin

Bachelorseminar

„Technische Aspekte des Datenschutzes“

Ludwig-Maximilians-Universität München

Technische Universität München

Sommersemester 2015

Eine juristische und rechtsinformatische Einordnung des Seminarthemas

Gastvortrag von

Rechtsanwalt Dr. Falk Peters, Berlin

21. Mai 2015

Rechtsanwalt Dr. Falk Peters, Berlin

I. Zur rechtlichen Einordnung

Datenschutz und Datensicherheit: Die Begriffe

Datenschutz ist eine rechtliche Regelungsmaterie mit dem Normzweck, die missbräuchliche bzw. rechtswidrige Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch dazu grundsätzlich Befugte zu verhindern. Er ist Ausdruck der verfassungsrechtlich garantierten informationellen Selbstbestimmung des Menschen.[1]

Datensicherheit wird grundsätzlich als technisch-organisatorische Aufgabe mit dem Ziel verstanden, Unbefugten den Zugang, die Verarbeitung und die Nutzung jeglicher Daten unmöglich zu machen. Kurz gesagt: Sie bezweckt die Bekämpfung der Datenkriminalität.

[1] vgl. 1BvR 209/83 u.a. – Urteil vom 15. Dezember 1983

Rechtsanwalt Dr. Falk Peters, Berlin

Datenschutz durch Datensicherung !

Merke:

Es gibt eine Schnittstelle zwischen Datenschutz und Datensicherheit; denn Datenschutz durch Maßnahmen der Datensicherung, also technisch-organisatorischer Datenschutz, ist von Anfang an durch das Bundesdatenschutzgesetz gefordert, s. § 9 BDSG mit Anlage.

Denselben Ansatz verfolgt Art. 23 des Entwurfs der EU-Datenschutzgrundverordnung.

Rechtsanwalt Dr. Falk Peters, Berlin

§ 9 BDSG Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der **Anlage** zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anlage (zu § 9 Satz 1 BDSG)
Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren **(Zutrittskontrolle**),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können **(Zugangskontrolle)**,

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Zugriffskontrolle)**,

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass

überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist **(Weitergabekontrolle)**,

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(Eingabekontrolle)**,

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können **(Auftragskontrolle)**,

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind **(Verfügbarkeitskontrolle),**

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können **(Zwecktrennungskontrolle).**

Kritik

Es handelt sich um rein **finales Recht.** Das heißt: Der Gesetzgeber begnügt sich mit politischer Zeichensetzung, also mit der mehr oder weniger abstrakten Formulierung von Zwecken, die erfüllt werden müssen. Über die Art und Weise, wie diese Zwecke zu erfüllen sind, sagt er nichts.

Im Übrigen:

Daten, die vom Gesetz oder von datenverarbeitenden Stellen als schutzwürdig oder gar als geheimhaltungsbedürftig eingestuft werden – personenbezogene Daten gehören dazu –, fallen in den diesbezüglichen Sicherheitskonzepten unter das **Sicherheitsziel der Vertraulichkeit**, das indes immer durch technische oder menschliche Schwachstellen bedroht ist. Den damit verbundenen Risiken begegnet man üblicherweise mit einer **Access Control**, i.e. eine Zugriffs- bzw. Zugangskontrolle, die im Sicherheitskonzept detailliert geplant und sodann technisch umgesetzt wird. Abgesehen einmal von der Binsenweisheit, dass es 100%ige

Sicherheit nicht gibt, ist das Problem bei diesem Vorgehen, dass dabei immer nur der Devise gefolgt wird, Befugten etwas zu gestatten, Unbefugten dagegen etwas zu verwehren. Damit sind Aktionen von Befugten eigentlich gar nicht kontrollierbar, d. h. die gesamte Insider-Problematik fällt aus dieser Form der Sicherheitsmaßnahme heraus. Gerade hier ist aber ein hohes Potenzial für den unerwünschten Abfluss von Daten (Data Leakage) vorhanden. Um also Data Leakage zum Zweck des Datenschutzes möglichst perfekt zu entdecken bzw. zu vermeiden, muss daher neben dem Zugang zu Daten auch der Umgang mit Daten kontrolliert werden, was selbstverständlich rechtlich legitimiert sein muss.

(aus: Peters, Falk: Data Leakage Prevention zum Zweck des Datenschutzes – Eine vergleichende Betrachtung zweier Bedrohungsszenarien. LIFIS ONLINE(20.11.13) S.15 ; www.leibnitz-institut/archiv/peters_20_11_13.pdf)

Rechtsanwalt Dr. Falk Peters, Berlin

Art. 23 der EU-Datenschutzgrundverordnung

Die aktuelle Fassung des Art.23 der EU-Datenschutzgrundverordnung lautet:

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

1. Der für die Verarbeitung Verantwortliche führt unter Berücksichtigung des Stands der Technik und der Implementierungskosten sowohl zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung technische und organisatorische Maßnahmen und Verfahren durch, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und die Rechte der betroffenen Person gewahrt werden.

2. Der für die Verarbeitung Verantwortliche setzt Verfahren ein, die sicherstellen, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, die für die spezifischen Zwecke der Verarbeitung benötigt werden, und dass vor allem nicht mehr personenbezogene Daten zusammengetragen oder vorgehalten werden als für diese Zwecke unbedingt nötig ist und diese Daten auch nicht länger als für diese Zwecke unbedingt erforderlich gespeichert werden. Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um etwaige weitere Kriterien und Anforderungen in Bezug auf die in den Absätzen 1 und 2 genannten Maßnahmen und Verfahren festzulegen, speziell was die Anforderungen an den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen für ganze Sektoren und bestimmte Erzeugnisse und Dienstleistungen betrifft.

4. Die Kommission kann technische Standards für die in den Absätzen 1 und 2 genannten Anforderungen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Abs. 2 genannten Prüfverfahren erlassen.

Kritik

Art. 23 ist ein eklatantes Beispiel für die Flucht des Gesetzgebers in **symbolisches Recht**. Schon das Sprachgefühl verrät jedem Gebildeten und gerade auch dem Nichtjuristen, dass der Wortlaut von Art. 23 geeignet ist, einer "Wolkenschieberei" Vorschub zu leisten, wie sie im Datenschutz leider seit eh und je Usus ist. Der Normadressat ist zu nichts Konkretem gezwungen; denn

- in Abs. 1 ist nur erkennbar, dass der Datenschutz zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung durch technische und organisatorische Maßnahmen und Verfahren gewahrt werden soll, wie das aber geschehen soll, ist mit keinem Wort erwähnt. Die Maßnahmen zur Sicherstellung des Datenschutzes bleiben völlig dem Gutdünken des Normadressaten überlassen.

- in Abs. 2 werden die Grundsätze der Zweckbindung, der Datensparsamkeit und der Datenvermeidung zwar angesprochen; aber wiederum bleiben die Maßnahmen zur Implementierung dieser Grundsätze völlig dem Gutdünken des Normadressaten überlassen. Formulierungen wie "die für die spezifischen Zwecke der Verarbeitung benötigt werden" und "als für diese Zwecke unbedingt nötig" sowie "für diese Zwecke unbedingt erforderlich" zeigen, dass dem Normadressaten ein unbegrenzter Spielraum bei der Auslegung dieser wertausfüllungsbedürftigen Formulierungen bleibt.

- in Abs. 3 findet sich eine fragwürdige Ermächtigungsgrundlage für die Kommission, per delegierte Rechtsakte "etwaige weitere Kriterien und Anforderungen in Bezug auf die in den Abs.1 und 2 genannten Maßnahmen und Verfahren festzulegen". In den Abs. 1 und 2 sind aber gar keine Kriterien, Maßnahmen und Verfahren genannt.

- in Abs. 4 endlich findet sich die Ermächtigungsgrundlage zur Festlegung technischer Standards. Dieser Absatz, als Muss-Vorschrift mit verbindlicher Frist zur Erledigung formuliert, hätte als Legitimationsgrundlage für das Tätigwerden in Sachen technischen Datenschutzes gereicht.

Fazit: Art. 23 der EU-Datenschutzgrundverordnung enthält nahezu rein finales Recht, welches dem Normadressaten keinerlei technische oder organisatorische Maßnahmen vorschreibt bzw. zur Mittelwahl vorgibt, sondern es völlig seinem Belieben überlässt, welche Maßnahmen er de facto zur Sicherstellung des Datenschutzes trifft.

Rechtsanwalt Dr. Falk Peters, Berlin

Zulässigkeit personenbezogener Datenerhebung, -verarbeitung und -nutzung

§ 4 BDSG Zulässigkeit der Datenerhebung, -verarbeitung und –nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Entsprechende Rechtsvorschriften finden sich z.B. im
Beamtenrecht, Arbeitsrecht, Sozialrecht, Allg. Versicherungsrecht, Steuerrecht, Medizin- bzw. Arztrecht, Telekommunikationsrecht, Bankenrecht, Strafrecht, IT-Sicherheitsrecht usw. usf.

Ein Beispiel aus dem IT- Sicherheitsrecht, und zwar aus dem
Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14. August 2009, BGBl. I 2009, S. 2821 – kurz: BSI-Gesetz

§ 1 Bundesamt für Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik als Bundesoberbehörde. Es untersteht dem Bundesministerium des Innern.

§ 3 Aufgaben des Bundesamtes

(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr:

1. Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes;

2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;

3. Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik (IT- Sicherheitsprodukte), soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist, einschließlich der Forschung im Rahmen seiner gesetzlichen Aufgaben;

4. Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von in formationstechnischen Systemen oder Komponenten und für die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit;

5. Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und Erteilung von Sicherheitszertifikaten;

6. Prüfung und Bestätigung der Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen und Komponenten mit technischen Richtlinien des Bundesamtes;

7. Prüfung, Bewertung und Zulassung von informationstechnischen Systemen oder Komponenten, die für die Verarbeitung oder Übertragung amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes im Bereich des

Bundes oder bei Unternehmen im Rahmen von Aufträgen des Bundes eingesetzt werden sollen;

8. Herstellung von Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen für informationssichernde Systeme des Bundes, die im Bereich des staatlichen Geheimschutzes oder auf Anforderung der betroffenen Behörde auch in anderen Bereichen eingesetzt werden;

9. Unterstützung und Beratung bei organisatorischen und technischen Sicherheitsmaßnahmen sowie Durchführung von technischen Prüfungen zum Schutz amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes gegen die Kenntnisnahme durch Unbefugte;

10. Entwicklung von sicherheitstechnischen Anforderungen an die einzusetzende Informationstechnik des Bundes und an die Eignung von Auftragnehmern im Bereich von Informationstechnik mit besonderem Schutzbedarf;

11. Bereitstellung von IT-Sicherheitsprodukten für Stellen des Bundes;

12. Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen; dies gilt vorrangig für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihm bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz zusteht;

13. **Unterstützung**

a) der **Polizeien und Strafverfolgungsbehörden** bei der Wahrnehmung ihrer gesetzlichen Aufgaben,
b) der **Verfassungsschutzbehörden** bei der Auswertung und Bewertung von Informationen, die bei der Beobachtung terroristischer Bestrebungen oder nachrichtendienstlicher Tätigkeiten im Rahmen der gesetzlichen

Befugnisse nach den Verfassungsschutzgesetzen des Bundes und der Länder anfallen,

c) des **Bundesnachrichtendienstes** bei der Wahrnehmung seiner gesetzlichen Aufgaben.

Die Unterstützung darf nur gewährt werden, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen. Die Unterstützungsersuchen sind durch das Bundesamt aktenkundig zu machen;

14. Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;

15. Aufbau geeigneter Kommunikationsstrukturen zur **Krisenfrüherkennung**, **Krisenreaktion und Krisenbewältigung** sowie Koordinierung der Zusammenarbeit zum Schutz der kritischen Informationsinfrastrukturen **im Verbund mit der Privatwirtschaft.**

(2) Das Bundesamt kann die Länder auf Ersuchen bei der Sicherung ihrer Informationstechnik unterstützen.

§ 8 Vorgaben des Bundesamtes

(1) Das Bundesamt kann Mindeststandards für die Sicherung der Informationstechnik des Bundes festlegen. Das Bundesministerium des Innern kann nach Zustimmung des Rats der IT-Beauftragten der Bundesregierung die nach Satz 1 festgelegten Anforderungen ganz oder teilweise als **allgemeine Verwaltungsvorschriften für alle Stellen des Bundes** erlassen. Soweit in einer allgemeinen Verwaltungsvorschrift Sicherheitsvorgaben des Bundesamtes für ressortübergreifende Netze sowie die für den Schutzbedarf des jeweiligen

Netzesnotwendigen und von den Nutzern des Netzes umzusetzenden Sicherheitsanforderungen enthalten sind, werden diese Inhalte im Benehmen mit dem Rat der IT-Beauftragten der Bundesregierung festgelegt. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter.

(2) Das Bundesamt stellt im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 **technische Richtlinien** bereit, die von den Stellen des Bundes als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer (Eignung) und IT-Produkte (Spezifikation) für die Durchführung von Vergabeverfahren berücksichtigt werden. Die Vorschriften des Vergaberechts und des Geheimschutzes bleiben unberührt.

(3) Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 11 erfolgt durch **Eigenentwicklung oder nach Durchführung von Vergabeverfahren** aufgrund einer entsprechenden Bedarfsfeststellung. Die Vorschriften des Vergaberechts bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Bundesbehörden diese Produkte beim Bundesamt abrufen. Durch Beschluss des Rats der IT-Beauftragten der Bundesregierung kann festgelegt wer den, dass die Bundesbehörden verpflichtet sind, diese Produkte beim Bundesamt abzurufen. Eigenbeschaffungen anderer Bundesbehörden sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Die Sätze 4 und 5 gelten nicht für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane.

Rechtsanwalt Dr. Falk Peters, Berlin

Prominente Beispiele verfassungsrechtswidriger Gesetze der jüngeren Vergangenheit

Von geradezu rechtshistorischer Bedeutung sind diejenigen verfassungsgerichtlichen Entscheidungen, durch die eklatante Vorstöße des Staates, die Privatsphäre seiner Bürger per Gesetz zu kassieren, korrigiert, ja regelrecht gestoppt werden mussten.

1. Das Volkszählungsurteil 1983

Angefangen hat alles mit dem Verfahren über die Verfassungsbeschwerden gegen das Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983) vom 25. März 1982 (BGBl. I S. 369)[1]. Durch das Volkszählungsurteil wurde die Volkszählung verhindert. Mit dieser „Jahrhundertentscheidung“ erhielt der Datenschutz, verstanden als Grundrecht auf **informationelle Selbstbestimmung** gemäß Art. 2 Abs.1 GG (Persönliches Freiheitsrecht) i.V.m. Art. 1 Abs. 1 GG (Menschenwürde), Verfassungsrang. Seither müssen alle Gesetze, die eine Beschränkung der informationellen Selbstbestimmung zur Folge haben (können), sich an der Reichweite dieses Grundrechts orientieren.

Prominente Beispiele verfassungsrechtswidriger Gesetze der jüngeren Vergangenheit

Beachtlich häufig haben vor allem die sog. Sicherheitsgesetze in den letzten 25 Jahren wegen befürchteter Freiheitsbedrohung Aufsehen erregt und der bundesverfassungsgerichtlichen Prüfung nicht bzw. nicht in vollem Umfang standgehalten, so z.B.:

§ 31 NWPolG 1990 in der Fassung vom 24. Februar 1990 betr. die **Rasterfahndung**[2],

[1] vgl. dazu 1 BvR 209/83 u.a. – Urteil vom 15. Dezember 1983
[2] vgl. dazu 1 BvR 518/02 – Beschluss vom 04. April 2006

Gesetz zur Änderung des Grundgesetzes (Artikel 13) vom 26. März 1998 (BGBl. I S. 610) und Gesetz zur Verbesserung der Bekämpfung der organisierten Kriminalität vom 04. Mai 1998 (BGBl. I S. 845) betr. die **akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung (Großer Lauschangriff)**[3],

HessSOG in der Fassung vom 14. Januar 2005 und SchlHLVwG in der Fassung vom 13. April 2007 betr. die **automatisierte Erfassung von Autokennzeichen**[4],

Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 betr. **heimliche Online- Durchsuchungen von Computern**[5],

Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007 betr. die **Vorratsdatenspeicherung**[6],

Gesetze zur Änderung des Bayerischen Polizeiaufgabengesetzes (Art. 34 Abs.2 und 3 BayPAG) und des Bayerischen Verfassungsschutzgesetzes (Art. 6c Abs.2 BayVSG) vom 8. Juli 2008 betr. die **Nutzung der Vorratsdatenspeicherung** nach §113a TKG[7].

Aber Achtung:

1. Im Bundesministerium des Innern sind gegenwärtig Überlegungen im Gange, wie man die Erhebung der Maut-Gebühr zur Kontrolle des Verkehrsverhaltens von Autofahrern und zur Erstellung von Migrationsprofilen verwenden kann.
2. Die Bundesministerien des Innern und der Justiz sind gegenwärtig dabei, ein neues Gesetz betreffend die Vorratsdatenspeicherung zu entwerfen.
3. Das Bundeskriminalamt (BKA) will im Herbst 2015 den so genannten Bundestrojaner einsatzbereit haben. Als Bundestrojaner wird eine Software bezeichnet, die Bundesbehörden für online-Durchsuchungen auf Heimcomputern, PDAs, Smartphones und BlackBerrys einsetzen können.

---

[3] vgl. dazu 1 BvR 2378/98 und 1 BvR 1084/99 – Urteil vom 3. März 2004
[4] vgl. dazu 1 BvR 2074/05 und 1 BvR 1254/07 – Urteil vom 11. März 2008
[5] vgl. dazu 1BvR 370/07 und 1BvR 595/07 - Urteil vom 27. Februar 2008
[6] vgl. dazu 1BvR 256/08, 1BvR 263/08 und 1 BvR 586/08 – Urteil vom 2.März 2010
[7] vgl. dazu 1 BvR 256/08 – Beschluss vom 28. Oktober 2008

Rechtsanwalt Dr. Falk Peters, Berlin

Datenschutzskandale in der Wirtschaft – kleine Lese 2009

Von den allein im Jahre 2009 bekannt gewordenen Datenskandalen haben die im Folgenden genannten besonderes Aufsehen erregt:

bei der **Handelskette Lidl** das Ausforschen von Krankheitsursachen bei krankgeschriebenen Arbeitnehmern[1],

bei der **Deutschen Bahn** die systematische Filterung von emails bei bis zu 80.000 Mitarbeitern zwecks Boykotts eines gewerkschaftlichen Streikaufrufs[2],

bei der **Deutschen Telekom** die jahrelange Bespitzelung von Aufsichtsratsmitgliedern, Journalisten, Mitarbeitern und deren Angehörigen sowie von firmenfremden Personen durch Ausforschen ihrer Bankkonten[3],

bei der **Innungskrankenkasse Weser-Ems** die Weitergabe von Sozialdaten ihrer Versicherten mit den vermarktbaren Vermerken „krebskrank“, „keine Zähne“ usw. an die Signal Iduna Versicherung[4],

bei der **Bundesagentur für Arbeit** der Einsatz eines Computersystems, über das gut 100 000 Mitarbeiter u.a. Suchtkrankheiten, Verschuldung, Familienprobleme von Hartz IV- Empfängern abrufen konnten[5],

bei der **Bundesagentur für Arbeit** die Zulassung eine Berliner Firma zur Schaltung von mehr als 2500 unterschiedlichen Stellenangeboten in der Online-Jobbörse der Arbeitsagentur, um die Daten von Bewerbern abgreifen zu können[6].

Zitat (2009) „Es gibt, und ich habe das in diesem Maße nicht für möglich gehalten, Mängel in der Datenschutzkultur der Unternehmen. Und – das gebe ich zu – die

---

[1] vgl. Berliner Morgenpost v. 07. 04. 2009
[2] vgl. DIE WELT v. 31. 03. 2009
[3] vgl. Berliner Morgenpost v. 18. 05. 2009
[4] vgl. Berliner Morgenpost v. 15. 05. 2009
[5] vgl. Spiegel Online v. 30. 10.2009
[6] vgl. AFP v. 10.11.2009

Datenschutzaufsicht ist doch über weite Strecken ein zahnloser oder zumindest ein zahnarmer Tiger.“[7]

Deutscher Bundestag Drucksache 18/4631

18. Wahlperiode 15.04.2015

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts

A. Problem und Ziel

Die Entwicklungen in der Informationstechnik ermöglichen es Unternehmern, personenbezogene Daten von Verbrauchern in immer größerem Umfang zu erheben, zu verarbeiten und zu nutzen. Unternehmer, die mit Verbrauchern über Verträge verhandeln oder mit Verbrauchern Verträge schließen, erheben, verarbeiten und nutzen in immer größerem Umfang personenbezogene Daten der Verbraucher. Diese Daten werden nicht nur für die Abwicklung des Schuldverhältnisses zwischen dem Unternehmer und dem Verbraucher erhoben, verarbeitet und genutzt, sondern immer häufiger auch vom Unternehmer zu anderen Zwecken verarbeitet und genutzt, um die Daten für das Unternehmen zu kommerzialisieren. Dies geschieht vor allem, wenn solche Daten dann zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens von Auskunfteien, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels verarbeitet und genutzt werden. Viele Leistungen, die Verbrauchern insbesondere im Internet unentgeltlich angeboten werden, wie z. B. die Nutzung von sozialen Netzwerken, Internetsuchmaschinen, Apps für mobile Endgeräte oder Kundenkarten, lassen sich die Anbieter durch die Daten der Verbraucher bezahlen, die sie dann für das Unternehmen kommerzialisieren, insbesondere immer öfter auch durch eine gewinnbringende Weitergabe an andere Unternehmer. Aufgrund des stetigen Fortschritts in der Informationstechnik ist es möglich, immer mehr personenbezogene Daten immer schneller zu sammeln, zu systematisieren

[7] So der Bundesbeauftragte für den Datenschutz, vgl. Innenausschuss des 16. Deutschen Bundestages, 88. Sitzung am 23.03.2009, Protokoll Nr. 16/88, S. 17

und auszuwerten, insbesondere auch für Profilbildungen zu nutzen. Deshalb können Verstöße gegen Datenschutzgesetze beim Erheben, Verarbeiten und Nutzen von personenbezogenen Daten eines Verbrauchers zu erheblichen Persönlichkeitsrechtsverletzungen bei den betroffenen Verbrauchern führen. Dies gilt insbesondere, wenn Daten von Unternehmern zu Zwecken der Werbung, der Markt und Meinungsforschung, des Betreibens von Auskunfteien, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden. Davon sind nämlich in der Regel nicht nur einzelne Verbraucher, sondern eine Vielzahl von Verbrauchern in gleicher Weise betroffen.

Nach dem Unterlassungsklagengesetz (UKlaG) haben die anspruchsberechtigten Stellen nach § 3 Absatz 1 Satz 1 UKlaG einen Unterlassungsanspruch nach § 1 UKlaG gegen einen Unternehmer, dessen Allgemeine Geschäftsbedingungen, die er gegenüber Verbrauchern verwendet, gegen datenschutzrechtliche Vorschriften ver stoßen. Die anspruchsberechtigten Stellen können dadurch z. B. auch die Verwendung von vorformulierten datenschutzrechtlichen Einwilligungen verhindern, die nicht den Anforderungen des § 4a des Bundesdatenschutzgesetzes (BDSG) entsprechen.

Wenn ein Unternehmer allerdings datenschutzrechtliche Vorschriften gegenüber Verbrauchern in anderer Weise verletzt, ist strittig, ob die anspruchsberechtigten Stellen einen Unterlassungsanspruch nach § 2 Absatz 1 UKlaG haben.

Ein Unterlassungsanspruch nach § 2 Absatz 1 UKlaG besteht in diesen Fällen nur, wenn die verletzten datenschutzrechtlichen Vorschriften Verbraucherschutz-gesetze sind. Die zuständigen Zivilgerichte haben datenschutzrechtliche Vorschriften überwiegend nicht als Verbraucherschutzgesetze angesehen.

In Allgemeinen Geschäftsbedingungen für Verträge, die im Internet geschlossen werden, finden sich immer wieder Klauseln, die für Kündigungen und andere Erklärungen des Verbrauchers die Schriftform vorsehen. Verbraucher meinen dann meist, dass die Erklärung nur auf Papier mit eigenhändiger Unterschrift abgegeben werden kann. Sie wissen nicht, dass nach § 127 Absatz 1 und 2 des Bürgerlichen Gesetzbuchs (BGB) regelmäßig auch eine E-Mail oder ein Telefax ausreicht, um die vereinbarte Schriftform einzuhalten.

B. Lösung

Durch die Ergänzung des § 2 Absatz 2 UKlaG-E soll ausdrücklich geregelt werden, dass datenschutzrechtliche Vorschriften, welche die Zulässigkeit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten eines Verbrauchers durch einen Unternehmer zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens von Auskunfteien, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken regeln, Verbraucherschutzgesetze im Sinne des § 2 Absatz 1 UKlaG sind. Daneben sind weitere Änderungen vorgesehen, die die Durchsetzung der Ansprüche nach dem Unterlassungsklagengesetz erleichtern, aber ihre missbräuchliche Geltendmachung verhindern sollen. § 309 Nummer 13 BGB soll so geändert werden, dass durch Bestimmungen in Allgemeinen Geschäftsbedingungen künftig keine strengere Form als die Textform für Erklärungen und Anzeigen, die gegenüber dem Verwender der Allgemeinen Geschäftsbedingungen oder einem Dritten abzugeben sind, vereinbart werden kann.

Damit wird sichergestellt, dass insbesondere auch die Beendigung von Verträgen für Verbraucher nicht unnötig erschwert wird und sie einfach feststellen können, wie die vereinbarte Form zu erfüllen ist.

Rechtsanwalt Dr. Falk Peters, Berlin

1975: Gesellschaftspolitische und datenschutzrechtliche Prognosen der informationstechnischen Evolution

Die Quo-vadis-Computer? - Frage in Zusammenhang mit der informations-technischen Entwicklung wurde erstmals Mitte der 70er Jahre des vorigen Jahrhunderts gestellt, als sich insbesondere bei mit Computerthemen befassten Juristen, aber auch bei anderen diesbezüglich engagierten Intellektuellen die Befürchtung zu regen begann, durch den Einsatz von Computern könnte die an den verfassungsrechtlich garantierten Grundwerten der individuellen Würde und Freiheit orientierte Gesellschaft künftig zu einem Kollektiv von numerierten Bürgern pervertieren.[1] Als signifikant für die damalige Skepsis soll hier ein Aufsatz des damaligen Rechts- und Rechtsinformatikprofessors *Wilhelm Steinmüller* mit dem Titel „Quo vadis, Computer?“ in Erinnerung gebracht werden, dessen 8 (Hypo)Thesen wegen ihrer Weitsicht damals und ihrer Aktualität heute im Folgenden zitiert werden: [2]

These I: Datenschutz ist weniger ein Problem einer zu schützenden „Privatsphäre“ (was immer das auch heißen möge), als vielmehr eine Teilfrage aus dem übergreifenden Problem gesellschaftlicher Informationskontrolle angesichts einer im Gefolge der Automationsunterstützten Datenverarbeitung (ADV) sich zunehmend verändernden Informationsverteilung in der Gesellschaft.

These II: ADV kann interpretiert werden als eine erstmals gelungene Maschinisierung bestimmter intellektueller Prozesse.

These III: Die sozialen Auswirkungen der ADV entstehen weniger durch die ADV selber (also durch den sogenannten „Computer“), als vielmehr durch die mit ihr neu und zusätzlich entstehende Informationsorganisation und durch die sich ihrer bedienenden gesellschaftlichen Kräfte.

---

[1] vgl. Hoffmann/Tietze/Podlech, Numerierte Bürger, Peter Hammer Verlag, Wuppertal 1975
[2] vgl. Steinmüller aaO, Seite 139 ff

These IV: Die Bedeutung bzw. Leistung von Informationssystemen besteht in der Erzeugung und Optimierung dynamischer kybernetischer „Modelle“ über gesellschaftliche Objekte zu deren Beherrschung.

These V: Der Auf- und Ausbau von Informationssystemen in Wirtschaft und Staat erzeugt eine globale Verschiebung bisheriger Informationsverteilungen und dadurch mittelbar der Machtstruktur.

These VI: Im wirtschaftlichen Bereich sind allmähliche, aber tiefgreifende und weittragende Gewichtsverlagerungen und Neuentwicklungen im Gefolge der Automation der Information zu erwarten.

These VII: Im staatlichen Bereich einschließlich seiner Wechselwirkung zur übrigen Gesellschaft wird die Tendenz zur Ausweitung des staatlich-exekutiven Sektors bei gleichzeitiger Zurückdrängung partizipatorischer Strukturen und zunehmender ökonomisch-administrativer Verflechtung verstärkt.

These VIII: Gegenläufige Tendenzen sind vorhanden und erweiterungsfähig.

Rechtsanwalt Dr. Falk Peters, Berlin

2015 : Zur perfekten Objektstellung des Menschen

Der Autor Rudi Klausnitzer (Kommunikationsagentur DMC) hat in seinem Buch *Das Ende des Zufalls* (erschienen 2013) gezeigt, *Wie Big Data uns und unser Leben vorhersagbar macht*, und die Autoren Viktor Mayer-Schönberger (Oxford Internet Institut) und Kenneth Cukier (Data Editor of the Economist) schätzen in ihrem Buch *Big Data: A Revolution That Will Transform How We Live, Work and Think* (erschienen 2013) den Betrag der weltweit gesammelten Daten auf (selbstverständlich nur vorläufige) 1, 2 **Zettabyt**. 1 Zettabyte entspricht 1 Milliarde **Terabytes**. Mittlerweile verfügt die NSA in dem neuen Spionagezentrum in Bluffdale im Mormonenstaat Utah über einen Yottabyte-Speicher. Ein **Yottabyte** entspricht 1000 Zettabytes.[1]

Spätestens durch die 2013 erfolgten Enthüllungen des Edward Snowden zu PRISM und TEMPORA und dem daraufhin mehr oder weniger systematischen Entdecken oder gar nur zufälligen Bekanntwerden von Art und Ausmaß der Datenspionage wurde dem kritischen Bürger vollends klar, dass bei rechtlich unkontrolliertem Einsatz derartiger IT-gestützter Überwachungssysteme alles und alle einer Ausforschung ausgesetzt sind, die von sich aus vor keiner rechtlichen Schranke halt macht und die sich schon jetzt auf dem Weg in einen sinnlich nicht wahrnehmbaren und dafür umso gefährlicheren globalen Totalitarismus befindet.

Aus: (aus: Peters, Falk: Data Leakage Prevention zum Zweck des Datenschutzes – Eine vergleichende Betrachtung zweier Bedrohungsszenarien. LIFIS ONLINE(20.11.13) S.2; www.leibnitz-institut/archiv/peters_20_11_13.pdf)

[1] vgl. http://www.conspirare.net/w2/nsa-yottabyte-speicher-bluffdale-kein-bluff-sondern-...

Rechtsanwalt Dr. Falk Peters, Berlin

Das Datenschutzproblem am Beispiel des De-Mail-Betriebs,

siehe Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften vom 28. April 2011 (BGBl. 2011 Teil I S. 666 vom 2. Mai 2011) - kurz: De-Mail-Gesetz

§ 2 des De-Mail-Gesetzes lautet:

Zuständige Behörde nach diesem Gesetz und der Rechtsverordnung nach § 24 ist das Bundesamt für Sicherheit in der Informationstechnik.

Die Koppelung von BSI-Gesetz und De-Mail-Gesetz wirft die Frage auf:

Wann ist die Überwachung des De-Mail-Verkehrs (bis hin zur Kenntnisnahme des Klartextes) durch das Bundesamt für Sicherheit in der Informationstechnik rechtmäßig bzw. wann nicht?

Rechtsanwalt Dr. Falk Peters, Berlin

De-Mail: Startschuss für Ende-zu-Ende Verschlüsselung

(BS) Die De-Mail-Anbieter Deutsche Telekom, Francotyp-Postalia sowie United Internet mit 1&1, WEB.DE und GMX haben heute ihr neues, stark vereinfachtes Verschlüsselungsverfahren auf Basis des weltweit anerkannten Standards “Pretty Good Privacy” (PGP) live geschaltet. Damit sollen De-Mail Nutzer in die Lage versetzt werden, ganz einfach ohne Vorkenntnisse, vertrauliche Nachrichten und Dokumente durchgängig vor Zugriffen Dritter zu schützen.

Der Einsatz von PGP war bisher so komplex, dass lediglich Internet-Experten davon Gebrauch machten. Die De-Mail-Anbieter haben den Prozess nun so stark vereinfacht, dass der Anwender im Rahmen seiner gewohnten Browser-Umgebung durch den Prozess geführt wird. Dazu steht den Nutzern ab heute kostenlos eine Browsererweiterung für Chrome und Firefox auf Basis des Open-Source-Projekts Mailvelope zur Verfügung. Die Schlüssel liegen ausschließlich bei Sender und Empfänger, nicht beim Anbieter.

1&1, GMX und WEB.DE stellen zudem ein De-Mail-PlugIn zur Verfügung, so dass der Nutzer mit einer geeigneten Software Ende-zu-Ende verschlüsselte De-Mails mit Outlook senden und empfangen kann.

Für professionelle Anwender mit hohem Kommunikationsvolumen hat Francotyp-Postalia zudem das komfortable AddIn für Microsoft Exchange/Outlook Umgebungen um die PGP-Funktionalität erweitert. De-Mails können somit einfach mit PGP ver- und entschlüsselt werden. Als Basis dient die Open-Source-Software Gpg4win.

Die De-Mail Anbieter haben sich für PGP entschieden, da De-Mail auf offenen E-Mail-Standards basiert und auch für die Kommunikation mit anderen zertifizierten europäischen Diensten anschlussfähig sein soll. Für beide Anforderungen sei PGP ohne Alternative, so die De-Mail-Anbieter.

Aus: Behördenspiegel - Newsletter E-Government Nr. 715 vom 23. April 2015, S. 5

Aber Achtung: Die De-Mail-Anbieter, die dem BSI und damit dem BMI unterstehen, sind als Erzeuger/Hersteller der Schlüssel jederzeit zur Entschlüsselung der verschlüsselten Texte, also zur Kenntnisnahme des Klartextes in der Lage.

Rechtsanwalt Dr. Falk Peters, Berlin

II. Rechtsinformatische Einordnung

Das Ziel der Rechtsinformatik ist die Adaption des Rechts auf die Digitale Welt.

Eine Mahnung aus dem Jahre 1960

Vor mehr als einem halben Jahrhundert hat der Staatsrechtler *Forsthoff* in seinem berühmten Vortrag "Der Jurist in der industriellen Gesellschaft" ausgeführt : " Mit den Augen des Technikers gesehen ist der Jurist ein Funktionär, der für sich in Anspruch nimmt, alles zu können,…. obgleich er in technisch-fachlichem Sinne nichts gelernt hat. Aber die Entwicklung erreicht einmal einen Punkt, an dem die Technik vermöge ihres gewachsenen Eigengewichts die Funktionsweisen des Juristen überwältigt."[1] Der von Forsthoff prophezeite " Punkt in der Entwicklung" wurde spätestens mit Beginn des digitalen Zeitalters erreicht.

Klassisches Recht vs. Technisches Organisationsrecht

Im Unterschied zum klassischen Datenschutzrecht, welches – wie fast das gesamte klassische Recht – aus Zulässigkeitsvorschriften (Geboten und Verboten), Anspruchsgrundlagen und Legaldefinitionen besteht und demzufolge ein System aus **Verhaltensappellen** darstellt, betrifft das technische Organisationsrecht die **Reglementierung der Technik** durch den Gesetzgeber selbst und stellt ein IT-gestütztes System der **Normbefolgungs-** bzw. der **Normkonkretisierungs-kontrolle** dar.

Charakteristika des klassischen Rechts sind: präskriptiv-normativ gefasst, auslegbar, beliebig befolgbar, sanktionierend.

Charakteristika des technischen Organisationsrechts sind: empirisch-deskriptiv gefasst, eindeutig, Befolgung zwingend, präventiv.

---

[1] NJW 1960, S. 1275

Rechtsanwalt Dr. Falk Peters, Berlin

Ein Appell an die Politik

Zu einem aussichtslosen Unterfangen wird der Datenschutz bald geraten, wenn wir einfach im alten Stil weitermachen und meinen, mit dem Erlass von Rechtsvorschriften sei ihm Genüge getan. Das ist ganz bestimmt ein Fehlschluss, wie die zahllosen und nicht enden wollenden Datenskandale seit Bestehen des Datenschutzrechts zeigen.

Was wir daher dringend brauchen, sind **technische Lösungen** für den Datenschutz, gesichert gegen Manipulationen und selbstverständlich produktneutral. Paragraphen sind im Rechtsstaat als Legitimationsgrundlagen zwar unverzichtbar, aber sie allein – und das gilt überall in der digitalen Welt und wird am Datenschutz besonders deutlich - machen nichts und niemanden lebendig; soll z.B. der von der Rechtspolitik bei jeder sich bietenden Gelegenheit propagierte Satz „Das Internet ist kein rechtsfreier Raum“ keine hohle Phrase bleiben, so müssen auf die Paragraphen draufgesattelt werden – und zwar vorgeschrieben vom Gesetzgeber bzw. vom Verordnungsgeber selbst mittels **technischen Organisationsrechts** - formalwissenschaftlich, also mathematisch-informatisch konzipierte und ingenieurtechnisch umsetzbare Verfahren der **Zweckbindung** und damit der **Informationskontrolle**, möglichst so allgemeingültig beschrieben, dass nicht bei jeder informationstechnischen Neuerung gleich auch eine Gesetzesnovellierung nötig wird. Kurzum: Der Datenschutz muss – wie das bereits seit Langem schon für die Datensicherheit angestrebt wird – **Konstruktionselement** einer jeden Informationstechnik werden, vom Supercomputer bis zum Smartphone, vom Internet bis zur Cloud. Nur so hat der Datenschutz als Quintessenz unserer höchsten Verfassungswerte, der Menschenwürde und der persönlichen Freiheit, in der digitalen Welt eine Zukunft.

Aus der unveröffentlichten Rede von RA Dr. Falk Peters anlässlich der Überreichung des Buches „Innovativer Datenschutz“ an die Bundesministerin der Justiz am 20. 02. 2013

Rechtsanwalt Dr. Falk Peters, Berlin

Die Folgen rein präskriptiv-normativer Datenschutzregelungen

- Unmöglichkeit präventiven Datenschutzes
- Unmöglichkeit der Vollstreckung gerichtlicher Datenschutzurteile
- Unmöglichkeit eines compliance managements im Datenschutz
- Unmöglichkeit der Reduzierung von Übermaßbürokratie im Datenschutz

Das konsequente Postulat

Ein schwerfälliges System aus rechtlichen Wertungen und Begriffen wie der Datenschutz ist mit der Rasanz der informationstechnischen Entwicklung und ihrer beliebigen Nutzung nicht zu synchronisieren. Soll der Datenschutz präventive Wirkungen entfalten, worin im Zeitalter des ubiquitous Computing allein sein Zweck bestehen kann, so darf er nicht der zweifelhaften Normtreue datenverarbeitender Stellen (Normadressaten) anheim gegeben werden bzw. allein überlassen bleiben. Vielmehr müssen bereits Organisation und Funktionsweisen der personenbezogenen Datenverarbeitung selbst Ausdruck der formal artikulierten und schließlich programmierten Datenschutzbelange der Betroffenen sein. In der formalen Artikulierung der Datenschutzbelange liegt die Kernaufgabe des technischen Organisationsrechts im Datenschutz.

Rechtsanwalt Dr. Falk Peters, Berlin

Schritte zur Automatisierung von rechtstextlich gefasster Zweckbindung bei personenbezogener Datenverarbeitung

1. **Logifizierung:** eine Aufgabe der Jurisprudenz

2. **Formalisierung:** eine Aufgabe der Kooperation von Jurisprudenz, Informatik und evtl. Mathematik

3. **Programmierung:** eine Aufgabe der Informatik

Rechtsanwalt Dr. Falk Peters, Berlin

1. Logifizierung – auf dem Weg zur Automatisierung von rechtstextlich gefassten Zwecken

Es gibt einen aus dem positiven Recht stammenden Grund, der den Juristen zur Beschäftigung mit der Logik zwingt: Es handelt sich um den **Revisionsgrund des Verstoßes gegen die Denkgesetze.**

Quelle: Herberger/Simon, Wissenschaftstheorie für Juristen, Juristische Lernbücher, Band 15, Alfred Metzner Verlag 1980

Begriffe der Logik

Assoziatives Schlussfolgern, i.e. teleologisch–induktives Vorgehen (Entelechie, Erkenntnisinteresse → nicht logifizierbar, nicht formalisierbar, nicht automatisierbar).

Logisches Schlussfolgern, i.e. logisch–deduktives Vorgehen

- **Klassische Logik** (Aristoteles → der Mittelbegriff, Syllogismus)
- **Moderne Logik** (Babbage, Boole → formale Logik) , i.e.

Formale Logik

→ **Prädikatenlogik:** i.e. Verwendung empirisch bewährter Begriffe (z.B. Namen statt Indikatoren, Symbole bzw. Bilder statt Text, hierarchische statt relationale Ordnung der Begriffe) und Quantoren in Aussagen; beachte aber: semantische Barriere.

→ **Aussagenlogik:** i.e. eindeutige Verknüpfung von Aussagen mittels der Boole'schen Operatoren.

→ **Relationslogik:** i.e. Ermöglichung einer Mehrstelligkeit des Prädikats und dadurch einer logische Behandlung von Beziehungen (Relationen). Der moderne Prädikats-begriff macht den Weg dafür frei, auch Relationen sowie Existenzaussagen logisch adäquat zu erfassen.

Achtung!

Deontische Logik: i.e. Unterfall der formalen Logik für ethische, insbesondere rechtsnormative Systeme. Merke: rechtliche Normen sind nicht wahr (w) oder falsch(f), sondern gültig oder ungültig; daher sind besondere deontische Operatoren erforderlich.

2. Formalisierung – auf dem Weg zur Automatisierung von rechtstextlich gefassten Zwecken

Informationstheorie: 4 semiotische Aspekte der natürlichsprachlichen Information

1. **Syntaktischer Aspekt:** betrifft das, was an der Information zähl- und messbar und somit in die Rechnersprache übersetzbar ist. Die syntaktische Komponente ist der Funktionsgrund des Computers. Der Binärcode ist eindeutig.

2. Semantischer Aspekt: betrifft die Bedeutung der Information. Sie ist hier gleich Nachricht. Z.B. bedeute die Zeichenfolge 100101 „Herr X ist geschäftsunfähig."

3. Pragmatischer Aspekt: betrifft den Zweck der Information, d.h. die Beziehung der Information zu ihrem „ Sender" (Absender, Erzeuger, Hersteller) und /oder ihrem „Empfänger"(Adressat, Benutzer).

4. Sigmatischer Aspekt: betrifft die Beziehung der Information zu dem, worüber sie informiert, also zur Realität.

Quelle: Steinmüller, Gegenstand, Grundbegriffe und Systematik der Rechtsinformatik. Ansätze künftiger Theoriebildung. in: Datenverarbeitung im Recht (DVR), Band 1, Heft 2/3, September 1972, S. 113 - 148

Rechtsmodellierung: Linguistische Stufen zur formalen Legistik

Präzision und Allgemeinverständlichkeit der juristischen Sprache stehen in reziprokem Verhältnis. Dieser Konflikt ist zugunsten der Präzision aufzulösen[1], wobei hinsichtlich der Qualität der Sprache der Kreis der Normadressaten als maßgeblich zu berücksichtigen ist.[2] Das geschieht durch **Rechtsmodellierung**. Darunter versteht man eine Methode zur Verbesserung der formalen Qualität von Rechtsnormen

[1] Vgl. BMJ, Handbuch der Rechtsförmlichkeit, 2. Aufl., Teil B: Formulieren, Randnote 49.

[2] Vgl. Karpen u. a., Die Gesetzgebung der Großen Koalition in der ersten Hälfte der Legislaturperiode des 16. Deutschen Bundestages, 2005 -2007, Studie Oktober 2007 S. 72 f. (Formale Qualität der Sprache)

zwecks erhöhter Kalkulierbarkeit der Rechtsauslegung bei der Rechtsanwendung sowie zwecks erleichterter IT-Unterstützung der Rechtsanwendung und mithin zur Verbesserung des Compliance Managements als des frühestmöglichen Ansatzes zur Reduzierung der Übermaßbürokratie.

Außerdem darf der Normzweck einer rechtlichen Regelung (ihre Systemrationalität) nicht der Spekulation von Einzelfallbeteiligten überlassen bleiben, sondern muss ihr selbst eindeutig zu entnehmen sein. Heute gilt die – von manchem Juristen indes nur verschämt bestätigte – Auffassung als allgemein unbestritten, dass das Recht in weiten Teilen vor Inkonsistenz strotzt und dass die von ihm zu fordernde Erwartungssicherheit eher ein frommes ethisches Postulat als zuverlässige Realität ist. Eine linguistische Stufung lässt sich von (1) bis (4) folgendermaßen darstellen:

Linguistische Stufungen zur Schärfung der Bedeutung:

Auf dem Weg zur IT- gestützten Prozesssprache

Linguistik,

i.e. moderne Sprachwissenschaft, die Theorien über die Struktur der (verbalen) Sprache erarbeitet und in weitgehend deskriptiven (d.h. formalen) Verfahren kontrollierbare, empirisch nachweisbare Ergebnisse anstrebt.

Quelle: Duden, Fremdwörterbuch

Computerlinguistik

In der Computerlinguistik wird untersucht, wie natürliche Sprache mit Hilfe des Computers algorithmisch verarbeitet werden kann. Sie ist **Teilbereich der künstlichen Intelligenz** und gleichzeitig Schnittstelle zwischen Sprachwissenschaft und Informatik, zwischen Leben und Technik. Dabei will man im Prinzip zweierlei Ziele erreichen:

1. Die Unterstützung der sprachwissenschaftlichen Forschung durch den Einsatz von Computern.

2. Die Entwicklung sprachverarbeitender Systeme, z.B. für die maschinelle Übersetzung, automatische Textzusammenfassung, Extraktion von Informationen aus Texten, **Reduzierung der Vieldeutigkeit der natürlichen Sprache zwecks natürlichsprachlicher Interaktion mit Automaten** usw.

Die **praktische Aufgabe** der Computerlinguistik besteht folglich darin, Computerprogramme zu entwickeln, die bestimmte, an natürliche Sprache geknüpfte Leistungen erbringen wie z.B. die Überprüfung der grammatikalischen Richtigkeit oder auch (noch weitergehend) die Unterstützung bei der Textverarbeitung oder gar bei der Formulierung in stringenten Kontexten.

Quelle: KON TE XIS 22_2007

(4) Formale Spezifikation:

mathematische Version,

bewiesene mathematische Version

(3) Semiformale Spezifikation:

strukturs prachliche Version, i.e.
graphenorientierte Sprache (z.B. Petrinetz),

logikorientierte Sprache (z.B. Entscheidungstabelle)

(2) Verbale Spezifikation:

prädikaten-, aussagen- und relationslogisch geprüfte Version

(1) Natürlichsprachliche Fassung:

Umgangssprache, Fachsprache

Erläuterung

(1) Entwurf in **natürlicher Sprache**: Der Mensch drückt alles, was er mitteilen will, wegen der allgemeinen Verständlichkeit zunächst in natürlicher Sprache aus. Auch Vorschriften, die z.B. Arbeitsabläufe beschreiben, werden zunächst in natürlicher Sprache formuliert. Diese Fassung bietet naturgemäß aber noch viele Auslegungsmöglichkeiten. Doch genau deren Eliminierung muss erfolgen, um die Vorschriften IT- gestützten Arbeitsabläufen zuordnen zu können (BPM).

(2) Erstellung der **verbalen Spezifikation**: die Vorschriften werden durch

prädikaten-, aussagen- und relationslogische Prüfung des Textes von den Unexaktheiten der natürlichen Sprache so weit befreit, dass Zweck gefährdende Missverständnisse oder gar rabulistische Sophismen ausgeschlossen sind.

(3) Erstellung der **semiformalen Spezifikation**: Die Vorschriften werden – wie das z.B. in den exakten Wissenschaften der Fall ist - mit einem genormten Vokabular, also in einer Kunstsprache formuliert. Diese muss von einer solch formalen Qualität sein, dass im nächsten Schritt die Programmierung erfolgen kann. In Frage kommen graphenorientierte Strukturspra chen (z.B. Petri-Netz) oder logikorientierte Strukturspra chen (z.B. Entscheidungstabelle).

(4) Erstellung der **formalen Spezifikation**: Die Vorschriften werden in einen Algorithmus gepackt. Dabei ist ein iteratives Vorgehen zwischen den linguistischen Stufungen, wenn nicht zwingend, so doch nützlich.

13.3 Programmierung - auf dem Weg zur Automatisierung von rechtstextlich gefassten Zwecken

Programmierung findet in der Regel aufgrund der semiformalen Spezifikation statt, in brisanten Fällen aufgrund der formalen Spezifikation. Bei unkomplexen Vorschriften bietet sich die Übersetzung in eine der sog. prozeduralen Programmiersprachen an (Sprachen der 3. Generation, z. B. Pascal oder C), da diese Sprachen einerseits noch maschinennah genug, andererseits aber schon genügend abstrakt bzw. symbolisch sind, um Verfahren präzise und doch relativ leicht modellieren zu können. Bei komplexen Vorschriften jedoch kann durch Anwendung prozeduraler Programmiersprachen Spaghetti-Code entstehen. Dann empfehlen sich objektorientierte Sprachen (Sprachen der 4. Generation, z. B. Smalltalk, Java) oder KI-Sprachen (Sprachen der 5. Generation, z.B. Prolog, die Ontologie-Sprache OWL[1]).

[1] vgl. Siegfried Knöpfler, Computationel Law und Datenschutz, in: Peters, Falk /Kersten, Heinrich /Wolfenstetter, Klaus-Dieter, Innovativer Datenschutz, Duncker&Humblot, Berlin 2012 .

Rechtsanwalt Dr. Falk Peters, Berlin

Datenschutz- Engineering beim De-Mail-Betrieb – eine Projektidee

Die **ENISA** empfiehlt **Privacy by design** (vgl. Behörden Spiegel, Februar 2015, S. 37)

Eine Möglichkeit: **Das Opt-in-Verfahren**. Es basiert auf dem Datenschutzziel der **Intervenierbarkeit** und ist problemlos einsetzbar beim datenschutzrechtlichen Erlaubnistatbestand der Einwilligung des Betroffenen. Soll das Verfahren im massenhaften De-Mail-Verkehr eingesetzt werden und dabei praktikabel sein, so muss es automatisiert werden. Dahin geht der folgende Vorschlag:[1]

- Eine Person P, die Kunde des De-Mail-Dienstleisters X ist, soll im Sinne der neuen Datenschutzziele der Transparenz, Nichtverkettbarkeit und Intervenierbarkeit die Möglichkeit erhalten, sich zu beliebiger Zeit davon zu überzeugen, was mit ihrer De-Mail samt den Verbindungsdaten geschieht, und gegebenenfalls einzuschreiten.
- Eine autorisierende Stelle A (am besten der für X zuständige Datenschutzbeauftragte) legt die Zweckbindung, also den Verwendungszeck Z bzw. die Verwendungszwecke Z1 – Zn, beim Umgang mit der De-Mail fest. Dazu modelliert A die Aufgaben, also die Befugnisse und Pflichten von X nach dem De-Mail-Gesetz sowie des BSI nach dem De-Mail-Gesetz und dem BSI-Gesetz, bis zur Eindeutigkeit, also mindestens zu semiformalen Spezifikationen, sodass diese sodann programmiert werden können.
- A stellt für X eine Chipkarte zur Verfügung mit

  a) einem üblichen Zertifikat zum Identitätsnachweis (mit einem öffentlichen und einem privaten Schlüssel zum Signieren und Verschlüsseln),

  b) einem Autorisierungszertifikat. Dieses enthält einen an den Zweck Z gebundenen öffentlichen Schlüssel.

---

[1] Entnommen aus dem Beitrag von Falk Peters in: Peters, Falk/Kersten, Heinrich/ Wolfenstetter, Klaus-Dieter, Innovativer Datenschutz, Verlag Duncker & Humblot, Berlin 2012, S. 166 ff.

- A führt eine öffentlich zugängliche Liste, die zu jedem erlaubten Zweck den zugehörigen öffentlichen Autorisierungsschlüssel enthält.
- X sendet an P, mit deren De-Mail Dp gesetzeskonform umgegangen werden soll, unter Nennung der programmierten Z und der Autorisierung von Z durch A, die Nachricht, jegliche De-Mail Dp unter den genannten Voraussetzungen über X versenden zu können. X signiert diese Nachricht elektronisch.
- P besitzt ebenfalls eine Chipkarte, die seine Identität bestätigt und ihm die Möglichkeit zum elektronischen Signieren und Verschlüsseln gibt. P ist anhand der elektronischen Unterschrift von X in der Lage, die Identität von X zu verifizieren und anhand des Autorisierungszertifikats i.V.m. der von A bereitgestellten Liste (siehe 4. Aufzählungszeichen) die Autorisierung von X für den Verwendungszweck Z zu überprüfen und – entweder positiv oder negativ – zu bestätigen.
- Bei positiver Bestätigung verschlüsselt P nun zunächst die De-Mail Dp mit dem öffentlichen Autorisierungsschlüssel für den Verwendungszweck Z (das Ergebnis ist Dp') und mit dem öffentlichen Schlüssel von X (das Ergebnis ist Dp''). Er signiert anschließend Dp'' elektronisch und übermittelt diese De-Mail mit seinem Zertifikat an X.
- X kann durch Überprüfung der elektronischen Unterschrift feststellen, ob die De-Mail von P stammt und auf dem Transportweg nicht verändert wurde.
- Ist das der Fall, so kann X durch Anwendung seines privaten Schlüssels anschließend die DeMail Dp' zurückgewinnen. Niemand anders ist dazu in der Lage.
- X hat nun die Wahl zwischen zulässiger Verwendung (nämlich Z) und nicht zulässiger Verwendung (-Z). Dabei wird Z durch eine Software SWz repräsentiert (siehe 2. Aufzählungszeichen).
- Die De-Mail Dp' wird nun der Software SWz zur Verfügung gestellt. Zwischen der Software SWz und der Chipkarte von X läuft ein Authentisierungsprotokoll ab, sodass „beide Seiten" erkennen können, dass die jeweils andere Seite die entsprechende Berechtigung besitzt. Der Einfachheit halber soll angenommen werden, dass das geheime Gegenstück zum öffentlichen Autorisierungsschlüssel (nämlich der private Autorisierungsschlüssel) für den Verarbeitungszweck Z in zwei Teile zerlegt worden ist: Eine Hälfte ist auf der Chipkarte von X mit dem Attribut Z gespeichert, die andere ist in der Software SWz integriert. Nur durch Zusammenwirken beider Hälften ist es möglich, die unverschlüsselte De-Mail Dp zu gewinnen.

- Die De-Mail Dp wird nunmehr durch SWz zulässigerweise verarbeitet.
- Vor irgendeiner Speicherung oder Übertragung muss die De-Mail Dp wieder verschlüsselt werden und zwar stets mit

  1) dem öffentlichen Autorisierungsschlüssel (hierfür benötigt die SWz die Chipkarte von X nicht) und

  2) dem öffentlichen Identitätsschlüssel von X (hierfür wird das entsprechende Zertifikat auf der Chipkarte benötigt).

Durch das Authentisierungsprotokoll ist damit sichergestellt, dass

1) die De-Mail Dp nur von X gelesen werden kann,

2) X sicher sein kann, dass die De-Mail tatsächlich von P kommt,

3) X keine Chance hat, von dem Verwendungszweck Z bzw. von den Verwendungszwecken Z1 – Zn abzuweichen,

4) Dritte keine Möglichkeit zu irgendeiner Verwendung von Dp haben.

Ergebnis: Die zweckgerechte Verwendung der De-Mail ist damit gegeben.

Erläuterung:

Das vorstehend vorgeschlagene technisch-organisatorische Verfahren basiert auf einer sog. *Public Key Infrastructure* (PKI). Die autorisierende Stelle A hat die Funktion eines Trustcenters. Da es um die datenschutzgerechte Zweckbindung des Umgangs mit der De-Mail geht, muss der Datenschutzbeauftragte diese Trustcenter-Funktion übernehmen. Das BSI kommt dafür nicht infrage, weil es zu den zu kontrollierenden Akteuren gehört. Ebenso wenig die BNetzA, weil sie nur für Netzregulierungen am Markt zuständig ist. Allerdings muss der Datenschutzbeauftragte technisch, personell und finanziell weitaus besser ausgerüstet werden, um die interdisziplinären Aufgaben zwischen den beiden staatstragenden Säulen Recht und Informationstechnik wissenschaftlich optimal wahrnehmen zu können.

Selbstverständlich funktioniert auch das vorstehend vorgeschlagene PKI-Verfahren nur dann einwandfrei, wenn es keinen Angriffen von außen, also z.B. keiner Datenspionage ausgesetzt ist.

Rechtsanwalt Dr. Falk Peters, Berlin

Ein Blick auf Gegenwart und Zukunft

Wir wollen den Rechtsstaat und wir brauchen ihn IT-gestützt !!

Zur Dynamik der Situation

Die Ubiquität des Rechts und die Ubiquität des Rechners

Die normative Ohnmacht des klassischen Rechts und die faktische Macht des Rechners

Die digital basierte Künstliche Intelligenz (KI) des Learning Computer und die analoge Intelligenz des Juristen

Notwendigkeiten in der Zukunft

Entwicklung interdisziplinärer Kompetenzen zwischen Computer und Recht von der Schulzeit an und die darauf basierende Kooperation von Juristen und Informatikern

Entwicklung einer juristischen Strukturspracheh zwecks Computational Law (CL)

Realisierung der Asimov'schen „Gesetze" durch Entwicklung einer Roboterethik

Rechtsanwalt Dr. Falk Peters, Berlin

Einschlägige Schriften des Autors zur Nacharbeit

Verfassungsgerechter Datenschutz in der digitalen Gesellschaft, LIFIS ONLINE (29.06.10) www.leibniz-institut.de/archiv/peters_29_06_10.pdf , ISSN 1864 - 6972

Datenschutz-Engineering am Beispiel der De-Mail, in: Falk Peters, Heinrich Kersten, Klaus-Dieter Wolfenstetter (Hrsg.), Innovativer Datenschutz, Verlag Duncker & Humblot, Berlin 2012, S.147 ff (ISBN 978-3-428-13860-9 (Print))

Data Leakage Prevention zum Zweck des Datenschutzes, LIFIS ONLINE (20.11.13) www.leibniz-institut.de/archiv/peters_20_11_13.pdf, ISSN 1864-6972