

# Datenschutz als Wettbewerbsvorteil\*

## Das ungarische Datenschutzgesetz unter der ökonomischen Lupe

Thomas Hoeren

### I. Mikroökonomische Analyse aus der Sicht der Unternehmen

#### 1. Regulierungsbedingt zu erwartende Kosten

- a) Definierungskosten
- b) Überwachungskosten
  - aa) Kosten der Überwachung nach dem ungarischen Datenschutzgesetz
  - bb) Änderungen durch die Datenschutzrichtlinie
- c) Durchsetzungskosten
  - aa) Kosten der Durchsetzung des ungarischen Datenschutzgesetzes
  - bb) Änderungen durch die Datenschutzrichtlinie

#### 2. Einfluß der Regulierung auf den Umsatz

- a) Vorteile einer innerbetrieblichen Kontrolle
- b) Datenschutz bei „Vertrauensgütern“

### II. Datenschutz und Wettbewerbsvorteil – die Sicht der Staaten

#### 1. Datenschutz als Spiel

#### 2. Spielstrategien

- a) Free Rider
- b) Tit for Tat
- c) n-Personen-Gefangenen-Dilemma

„Datenschutz als Wettbewerbsvorteil“ – dies scheint auf den ersten Blick ein Paradoxon zu sein. Datenschutz wird regelmäßig als verfassungsrechtlich relevantes Schutzgut bestimmt. Stellt man überhaupt einmal auf die wirtschaftliche Betrachtung ab, erscheint Datenschutz nie als Wettbewerbsvorteil, sondern eher als Hemmschuh für einen freien Informationsmarkt. Bei dieser Sicht handelt es sich jedoch nur um eine unreflektierte, diffuse Vorstellung. Denn eine ökonomische Analyse des Datenschutzrechts steht bis heute aus. Auch im folgenden kann eine solche Analyse nicht geliefert werden. Vielmehr soll in (zwangsweise fragmentarischer) Form der Nutzen einer solchen Analyse für die Bewertung des europäischen Datenschutzrechts verdeutlicht werden.

Dieser Blickwinkel ist gerade für das Gastgeberland dieses Symposiums von großer Bedeutung. Ende 1993 schlossen die Europäischen Gemeinschaften und deren Mitgliedstaaten mit der Republik Ungarn ein Assoziierungsabkommen.<sup>2</sup> Nach Art. 67 S. 1 des Vertrages erkennen die Vertragsparteien an, daß die Angleichung der bestehenden und künftigen Rechts-

vorschriften Ungarns an das Gemeinschaftsrecht eine wesentliche Voraussetzung für die wirtschaftliche Integration Ungarns in die Gemeinschaft darstellt. Ungarn wird dafür sorgen, daß die künftigen Rechtsvorschriften möglichst weitgehend mit dem Gemeinschaftsrecht vereinbar sind (Art. 67 S. 2). Von dieser Angleichungspflicht ist auch das Datenschutzrecht umfaßt. Zwar ist das Datenschutzrecht nicht in den Katalog der anzuleichenden Rechtsvorschriften aufgeführt; Art. 68 enthält jedoch lediglich einen nicht abschließenden Beispielskatalog („insbesondere“). Daher gehört auch die Umsetzung der neuen Europäischen Datenschutzrichtlinie<sup>3</sup> zu den Vertragspflichten der Republik Ungarn. Bis 1992 verfügte Ungarn nur über rudimentäre Datenschutzbestimmungen.<sup>4</sup> Durch die Einführung des Datenschutzgesetzes<sup>5</sup> verfügt Ungarn nunmehr über ein sehr modernes Datenschutzrecht, das Elemente des deutschen<sup>6</sup>, französischen<sup>7</sup> und englischen Systems<sup>8</sup> miteinander verbindet. Ohne die Bedeutung dieses Gesetzes für die Wirtschaftspraxis zu kennen, sollen im weiteren die Erfolgsfaktoren für die Implementierung dieses Gesetzes ermittelt und mit den ökonomischen Folgen der neuen EU-Datenschutzrichtlinie verglichen werden.

### I. Mikroökonomische Analyse aus der Sicht der Unternehmen

Damit Datenschutz ökonomisch begründet werden kann, ist eine Integration der Staatstheorie in die Betriebswirtschaftslehre erforderlich, wie dies u.a. in der „Neuen Institutionenökonomie“ erfolgt ist.<sup>9</sup> Staatliche Gesetzgebung erscheint hiernach als Wirtschaftsgut, das der Befriedigung wirtschaftlicher Bedürfnisse dient.<sup>10</sup> Eine ökonomische Theorie des Datenschutzes muß beim Gewinninteresse des einzelnen Unternehmens ansetzen. Ein Unternehmen wird Datenschutzmaßnahmen nur einführen und unterstützen, wenn dies in seinem eigenen Gewinninteresse ist.<sup>11</sup> Der Begriff des erwarteten Gewinns ist definiert als der erwartete Umsatz abzüglich der Kosten.<sup>12</sup> Folglich geht das Interesse eines Unternehmens dahin, den eigenen Umsatz zu maximieren und dabei die Kosten gering zu halten.<sup>13</sup> Zu prüfen ist daher, welchen Einfluß staatliche Regulierungen auf dem Gebiet des Datenschutzes auf die Kosten (1.) und den Umsatz (2.) eines Unternehmens haben.

\* Der Text gibt einen um Fußnoten erweiterten Vortrag wieder, den der Verfasser am 8. Juni 1996 bei einer Tagung der Friedrich-Naumann-Stiftung in Budapest gehalten hat.

## 1. Regulierungsbedingt zu erwartende Kosten

Das Interesse eines Unternehmens an Datenschutz hört auf, sobald die Grenzkosten der datenschutzrechtlichen Regulierung die Grenzkosten einer Nichtbefolgung übersteigen.<sup>14</sup> Hinsichtlich der Kosten ist vor allem auf die sog. Transaktionskosten abzustellen. Hierunter versteht man alle „Ressourcenaufwendungen für die Koordinierung wirtschaftlicher Handlungen“.<sup>15</sup> Zu solchen Aufwendungen zählen insbesondere die Kosten für Schaffung, Kontrolle und Durchsetzung einer Verhaltensordnung.<sup>16</sup> Im einzelnen geht es folglich im weiteren um die Bestimmung dreier verschiedener Kostenarten, die Definierungs-, Überwachungs- und Durchsetzungskosten.

### a) Definierungskosten

Die Definierungskosten umfassen die Kosten für die Schaffung einzelner Normen. Im Fall staatlicher Rechtssetzung fallen hierunter vor allem die zur Finanzierung des Staatshaushaltes erhobenen Steuern und die Aufwendungen für verbandspolitische Arbeit, die von Verbandsmitgliedern über die Verbandsbeiträge mittelbar finanziert werden. Wie hoch die Definierungskosten in Ungarn liegen, ist für mich nicht zu ermitteln gewesen. Im Bereich des deutschen Datenschutzrechts sind die Kosten jedenfalls sehr hoch. Dies hängt mit der unklaren Verbandssituation in diesem Gebiet zusammen. Gerade im Vorfeld der Diskussion um die Europäische Datenschutzrichtlinie erwies sich Datenschutz als Querschnittsmaterie, die alle Bereiche der Wirtschaft erfaßt. Daher haben die verschiedensten Verbände, vom BDI über den Bundesverband deutscher Banken bis hin zu den Markenverbänden, Stellungnahmen zur Richtlinie verfaßt. Eine deutsche oder gar europäische Zentralorganisation für den Bereich Datenschutz fehlt. Statt dessen sind die wenigen Datenschutzverbände, wie die Gesellschaft für Datenschutz und Datenverarbeitung (GDD), die Deutsche Vereinigung für Datenschutz (DVD), die Bundesvereinigung der Datenschutzbeauftragten (BvD) untereinander heillos zerstritten. Hinzu treten weitere Verbände, wie die Deutsche Gesellschaft für Recht und Informatik (DGRI), der Hamburger Arbeitskreis für Datenschutz oder die Gesellschaft für Informatik. Im ganzen werden durch dieses Verbandskonglomerat die Definierungskosten immens erhöht. Man kann nur hoffen, daß in Ungarn dieser Fehler nicht wiederholt, sondern auf die Einführung einer effizienten Lobbystruktur geachtet wird.

### b) Überwachungskosten

Die Überwachungskosten umfassen die Aufwendungen für die Kontrolle der Einhaltung von Normen. Im Falle staatlicher Aufsicht werden diese Aufwendungen vom einzelnen Unternehmen mittelbar über Steuern finanziert. Bei einer Selbstkontrolle fallen unmittelbar Aufwendungen für die Einrichtung einer unternehmensinternen Kontrollstelle an.

#### aa) Das ungarische Datenschutzgesetz

Der ungarische Gesetzgeber hat sich – anders der deutsche – für ein System staatlicher Aufsicht entschieden. Nach Art. 23 ist ein parlamentarischer Beauftragter für Datenschutz, der sog. Datenschutz-Ombudsman, durch die Nationalversammlung zu bestellen. Dieser hat die Durchführung datenschutzrechtli-

cher Bestimmungen zu „beobachten“ (Art. 24 lit. a). In der deutschen Übersetzung kaum verständlich ist die Regelung in Art. 25 Abs. 1, wonach der Ombudsman auch das „Vorhandensein von Voraussetzungen für den Schutz von persönlichen Daten (...) zu überwachen“ habe. Dem Ombudsman obliegt auch die Führung eines Datenregisters, in dem zentrale Daten über Art und Umfang der Datenverarbeitung enthalten sind (Art. 28). Der Registrierungspflicht unterliegen eine Reihe von Daten nicht, insbesondere sofern sie sich auf Arbeitsverträge oder Geschäftsverbindungen beziehen (Art. 30 lit. a). Die ökonomische Effizienz des Registrierungsmodells ist fragwürdig. So gehen mit der Pflicht der Unternehmen zur Benachrichtigung des Ombudsmans hohe personelle und finanzielle Aufwendungen einher. Diesen Aufwendungen steht die Tatsache gegenüber, daß die Registrierung als solche weder aus der Sicht des Betroffenen noch aus der Sicht des Unternehmens vorteilhaft ist. Zwar ist das Register für jedermann einsehbar (Art. 11 Abs. 2). Doch das Register enthält nur allgemeine Mindestinformationen, die überdies schnell veralten.

#### bb) Änderungen durch die Datenschutzrichtlinie

Die Überwachungskosten werden sich für ungarische Unternehmen durch die Datenschutzrichtlinie nicht nennenswert erhöhen. Die Richtlinie setzt auf ein System staatlicher Aufsicht (Art. 28). Daneben findet sich auch das Modell des Datenschutzregisters (Art. 18 ff.). Lediglich der Umfang der zu registrierenden Daten geht über das ungarische System insoweit hinaus, als auch eine geplante Datenübermittlung in Drittländer und Hinweise zur Datensicherheit mitgeteilt werden müssen (Art. 19 Abs. 1 lit. e und f).

### c) Durchsetzungskosten

Die wichtigste Kostenart stellen die Durchsetzungskosten dar.<sup>17</sup> Hierzu zählen vor allem die Kosten, die infolge eines Normverstößes entstehen. Die Palette solcher Aufwendungen reicht von Schadensersatznormen, Gewinnabschöpfung, Kosten durch Anordnung der Nichtigkeit eines Vertrages bis hin zu Vertragsstrafen. Zu berücksichtigen ist dabei vor allem die Sanktionswahrscheinlichkeit und Sanktionshöhe in Relation zu den infolge der innerbetrieblichen Umsetzung der Regelungen entstehenden „Time and Trouble“-Kosten.<sup>18</sup>

#### aa) Kosten der Durchsetzung des ungarischen Datenschutzgesetzes

Das ungarische Datenschutzgesetz sieht kaum Sanktionen für Normverstöße vor. Straf- und Bußgeldvorschriften finden sich im Gesetz nicht. Statt dessen kann der Datenschutz-Ombudsman bei Feststellung einer unzulässigen Datenverarbeitung den Verwalter der Daten auffordern, die Verarbeitung einzustellen (Art. 25 Abs. 2). Reagiert die speichernde Stelle darauf nicht, hat der Ombudsman die Öffentlichkeit über das Bestehen der unzulässigen Datenverarbeitung, die Identität des Verwalters der Daten und die Kategorien der verarbeiteten Daten zu unterrichten (Art. 25 Abs. 3). Diese Regelung ist ein Novum; nach meinem Wissensstand findet sich in Datenschutzgesetzen anderer Staaten keine vergleichbare Regelung. Offensichtlich geht es hier um die moderne Variante des mittelalterlichen Prangers. Allerdings übernimmt sie von dieser Strafmethode nicht deren Effizienz. Im Mittelalter konnte man sich aufgrund eines einheitlichen Sittenkodices darauf verlassen, daß der öffentlich vorgeführte Delinquent der so-

zialen Mißachtung anheimfiel. An einem solchen Common Sense fehlt es jedoch in der Moderne, zumindest was den Datenschutz geht. Große Teil der deutschen Bevölkerung sind nach meinem Eindruck an Fragen des Datenschutzes nicht interessiert. Ich könnte mir vorstellen, daß die Situation in Ungarn ähnlich ist. Damit erweist sich das Mittel des „going public“ im Datenschutzrecht als relativ ineffizient. Dieser Eindruck wird auch noch dadurch verstärkt, daß dem Datenschutz-Ombudsman weitergehende Sanktionsmöglichkeiten nicht zugebilligt werden. Insbesondere kann er die speichernde Stelle nicht dazu zwingen, die Verarbeitung einzustellen. Für den Verantwortlichen ist es daher nur eine Kostenfrage, ob er trotz des öffentlichen Drucks weiterhin unzulässige Verarbeitungen vornimmt.

Damit verbleibt es dem Betroffenen, über die Geltendmachung von Schadensersatzansprüchen Regelverletzungen zu sanktionieren (Art. 18). Allerdings kommt in der Praxis ein solcher Anspruch nur wegen Persönlichkeitsrechtsverletzungen in Betracht. Diese liegen allenfalls dann vor, wenn Daten unrichtig gespeichert oder übermittelt werden. Im übrigen sieht das Gesetz zwar Lösungs- und Berichtigungsansprüche im Falle unzulässiger Speicherungen vor (Art. 14 Abs. 1 und 2); der Betroffene dürfte aber mangels allgemeiner Informationspflicht in den seltensten Fällen vom Umfang der Speicherung Kenntnis haben. Daher ist der Betroffene in der Praxis das schwächste Glied für die Sanktionierung von Gesetzesverstößen. Die Sanktionswahrscheinlichkeit ist daher äußerst gering.

Die Durchsetzungskosten würden sich erhöhen, wenn Wettbewerber die Einhaltung datenschutzrechtlicher Bestimmungen mitkontrollieren könnten. In Deutschland ist eine solche Möglichkeit infolge der Entscheidungen in Sachen „D-Info 2.0“ eröffnet.<sup>19</sup> Das Landgericht Mannheim hat in seiner Entscheidung vom 29. März 1996 einen Verstoß gegen das BDSG als Rechtfertigung für einen Unterlassungsanspruch nach § 1 UWG angesehen. Das BDSG ziele „auf die Sicherung und Erhaltung eines durch die Verfassung (Art. 2 Abs. 1 GG) geschützten Rechts, dessen Bedeutung das Bundesverfassungsgericht betont hat (BVerfGE 65, 1)“. Der „Verstoß gegen das BDSG zu Zwecken des Wettbewerbs“ sei daher „unlauter im Sinne des § 1 UWG, ohne daß es dafür noch auf das Vorliegen weiterer Umstände ankäme“. Die Argumentation des Gerichts ist insoweit sehr knapp, was für allem deshalb verwundert, als es sich hier um die erste Entscheidung zur Verbindung von Datenschutz- und Wettbewerbsrecht handelt. Im Ergebnis könnte nach dieser Entscheidung jeder Verstoß gegen geltendes Datenschutzrecht vom Konkurrenten über § 1 UWG gerügt werden. Dies erscheint mir eine pauschale, undifferenzierte Sichtweise. Man wird das Urteil des Landgerichts auch dahingehend interpretieren können, daß jede einzelne Regelung des Datenschutzrechts auf ihren wettbewerbsrechtlichen Gehalt hin überprüft wird. Dabei wäre auch der Wertbezug jeder einzelnen Norm zu prüfen, der sich insbesondere auch aus der Tatsache des Grundrechtsbezug ableiten läßt.<sup>20</sup>

#### bb) Änderungen durch die Datenschutzrichtlinie

Die Kostenstruktur wird sich mit der Umsetzung der Datenschutzrichtlinie ändern. Künftig stehen der Aufsichtsbehörde nunmehr weitreichende Eingriffsbefugnisse zu (Art. 28 Abs. 3, 2. Spiegelstrich), etwa hinsichtlich

- einer Sperrung, Löschung oder Vernichtung von Daten,
- einem Verbot der Verarbeitung oder

- einer Verwarnung des Verantwortlichen (etwa im Rahmen eines Bußgeldverfahrens).

Im übrigen haben sie die Befugnis, die Justizbehörden bei Feststellung von Datenschutzverstößen einzuschalten. Hier bleibt allerdings unklar, ob die Aufsichtsbehörden damit Strafverfolgungsmaßnahmen unabhängig davon einleiten können, ob es sich um ein Antragsdelikt handelt (vgl. § 43 Abs. 4 des deutschen BDSG).

Erhöhte Durchsetzungskosten dürfte auch das neu eingeführte Widerspruchsrecht mit sich bringen. Aus dem französischen Recht wurde ein umfassendes Recht des Betroffenen auf Widerspruch gegen die Verarbeitung seiner Daten entnommen und europäisch verbindlich gemacht (Art. 14 lit. a). Dies gilt auch, wenn Daten rechtmäßig verarbeitet werden. Allerdings muß der Betroffene darlegen, daß er überwiegende und schutzwürdige Gründe geltend machen kann. Im übrigen bedarf die Regelung noch der Zustimmung des Einzelstaates; die Frage ist, ob in Ungarn ein solch diffuses und unkonkretes Widerspruchsrecht von den Gesetzgebungsgremien akzeptiert wird.

Insgesamt wird sich zeigen, ob die Anhebung der Sanktionshöhe und -wahrscheinlichkeit zu einer stärkeren Beachtung des Datenschutzes aus der Sicht der Unternehmen führen wird. Frappierend sind allerdings die allgemeinen betriebswirtschaftlichen Forschungsergebnisse zur Befolgung von staatlich sanktionierten Regeln. Hiernach stellt der Regelverstoß bis zur Sanktionierung die kostenoptimale Handlungsweise eines Unternehmens dar.<sup>21</sup> Insbesondere bei der Verhängung von Geldstrafen gilt der Auflagenverstoß als stets optimal.<sup>22</sup> Diese Berechnungen gehen allerdings einseitig von den Durchsetzungskosten staatlicher Regelungen aus. Auf die - im weiter zu klärende - Frage der damit verbundenen Umsatzerhöhungen geht die bisherige Forschung nicht ein.<sup>23</sup>

## 2. Einfluß der Regulierung auf den Umsatz

Die ökonomische Analyse des Datenschutzrechts wäre unvollständig, würde sie nur die komparativen Kostenvor- und -nachteile der verschiedenen Regulierungsformen berücksichtigen. Der Gewinn eines Unternehmens ist jedoch auch vom Umsatz bestimmt. Seitens der Wirtschaft wird der Marketingeffekt des Datenschutzes noch nicht hinreichend in den Blick genommen. Wie bereits einleitend bemerkt, wird Datenschutz weitgehend immer nur als Stör- und Kostenfaktor begriffen. Die umsatzsteigernde Wirkung insbesondere bei Unternehmen, die sensible Daten verarbeiten<sup>24</sup>, wird demgegenüber vernachlässigt. Hier besteht echter Nachholbedarf.

So dürfte der Datenschutz einen nachweisbaren Einfluß auf den Umsatz von sog. Vertrauensgütern haben.<sup>25</sup> Es handelt sich hierbei um Güter, deren Qualität nicht vom Kunden abschließend beurteilt werden kann.<sup>26</sup> Was zu diesen Gütern zählt, dürfte soziokulturell bedingt unterschiedlich sein; in Ungarn denkt man darüber anders als in Deutschland. Vertrauensgüter finden sich insbesondere bei Banken und Versicherungen, wenn man z.B. an die Kapitallebensversicherung oder den Bereich der Bankeinlagen denkt. In beiden Beispielfällen muß der Kunde darauf vertrauen können, daß seine medizinische Daten bzw. die Informationen zu seinen Vermögensverhältnissen im Rahmen gesetzlicher und vertraglicher Vorgaben vertraulich behandelt werden. Würde er dieses Vertrauen verlieren, würde sich dies unmittelbar auf den Umsatz auswirken. Der Kunde würde etwa seine Konten auf-

lösen und nach geeigneteren Kreditinstituten, z. B. in der Schweiz oder in Luxemburg, Ausschau halten. In solchen Fällen können unternehmensinterne Datenschutzmaßnahmen dazu führen, das Vertrauen der Kunden und damit auch den Umsatz des Unternehmens zu stärken.

Nicht nachweisbar war bislang jedoch ein positiver Einfluß des Datenschutzes auf den Vertrieb von Produktionsgütern. Hier spielt anscheinend Datenschutz keinen Einfluß auf den Umsatz. Allenfalls über Sanktionshöhe und Sanktionswahrscheinlichkeit läßt sich in diesem Sektor die Einhaltung von Datenschutznormen sichern.

### 3. Datenschutz und Wettbewerbsvorteil – Ein erstes Resümee

Im Ergebnis fällt es schwer, die Beziehung zwischen unternehmerischem Gewinn und Regulierung zu quantifizieren. Nach den bisherigen Ausführungen wird ein Unternehmen von sich aus einen innerbetrieblichen Datenschutzbeauftragten bestellen, wenn die ex ante erwarteten Kosten unter den Kosten staatlicher Normsetzung liegen und dieser Kostenvorteil nicht durch Umsatzeinbußen infolge des Fehlens staatlicher Regelungen kompensiert wird.

Umgekehrt wird ein Unternehmen kein Interesse an der Einführung von Datenschutzbeauftragten haben, wenn die damit ex ante verbundenen Kosten höher als die Kosten staatlicher Aufsicht sind oder der Verzicht auf staatliche Regelungen mit zu hohen Umsatzeinbußen verbunden ist.

---

## II. Datenschutz und Wettbewerbsvorteil – die Sicht der Staaten

---

Die Transaktionskostenanalyse ist in ihrer Wurzel ausschließlich an dem Verhalten eines einzelnen Unternehmens orientiert.<sup>27</sup> Sie geht von der Prämisse aus, daß der seitens des Unternehmens ex ante erwartete Gewinn mit dem tatsächlich ex post zu erwartenden Gewinn übereinstimmt. Damit setzt die Analyse voraus, daß das einzelne Unternehmen die Umwelt, insbesondere das Verhalten anderer Unternehmen vollständig kontrollieren kann.<sup>28</sup>

Diese Prämisse ist bereits für die Analyse des Verhaltens von Unternehmen fragwürdig. Sie gilt vor allem aber nicht für die Betrachtung von Staaten, die miteinander um die Setzung internationaler Datenschutzstandards ringen.<sup>29</sup> Stellt sich Datenschutz auch auf internationaler Ebene als Wettbewerbsvorteil dar? Wieso sollten sich eigentlich Staaten für ein international vereinheitlichtes Datenschutzniveau entscheiden, das ihrer nationalen Industrie zusätzliche Beschränkungen auferlegt? Oder – wie Axelrod, der Altmeister der Spieltheorie – fragt: „Unter welchen Bedingungen entsteht Kooperation in einer Welt von Egoisten ohne zentralen Herrschaftsstab?“<sup>30</sup>

### 1. Datenschutz als Spiel

Zu diesem Problemkreis liegen empirische Ergebnisse aus der spieltheoretischen Forschung<sup>31</sup> vor, die das Verhalten von Unternehmen und Staaten als strategische Spiele betrachten

und die taktisch günstigsten Spielstrategien<sup>32</sup> mathematisch errechnen will. Dazu wird im Sinne der obigen Überlegungen eine Kosten-Nutzen-Analyse für die verschiedenen strategischen Alternativen erstellt und auf dieser Grundlage Vor- und Nachteile einzelner Varianten ermittelt.<sup>33</sup>

Der Datenschutz weist hier gerade im internationalen Kontext ein besonderes Problem auf. Gesetzt ein Staat A würde für alle Unternehmen schärfere Datenschutzbestimmungen einführen. Aufgrund der oben beschriebenen Kosten-Nutzen-Erwägungen könnte es für die Unternehmen nunmehr sinnvoll sein, seine Datenverarbeitung im Staat A aufzugeben und durch ein Rechenzentrum in dem Land B durchführen zu lassen. Staat A mag nunmehr den Staat B um Anhebung des Datenschutzes auf ein gemeinsames Niveau bitten. Staat B wird dies ablehnen, weil er durch das niedrigere Datenschutzniveau eine Reihe volkswirtschaftlicher Vorteile genießt. Würde aber nunmehr auch der Staat A sein Datenschutzniveau aufgeben, würde das Vertrauen der Kunden in die Seriosität des Unternehmens verloren gehen. Es drohen heftige Umsatzeinbußen bis hin zum Konkurs, der auch die Verarbeitung der Daten im Staat B in Frage zieht.

Es handelt sich demnach um eine Situation, in denen Nichtkooperation für den einzelnen Spieler am gewinnträchtigsten, doch für alle Spieler am ungünstigsten ist<sup>34</sup>:

„Such dilemmas are defined by two simple properties: (a) each individual receives a higher payoff for a socially defecting choice (...) than for a socially cooperative choice, no matter what the other individuals in society do, but (b) all individuals are better off if all cooperate than if all defect.“<sup>35</sup>

Kurzzeitig hat jeder Staat durch Nichtkooperation einen Vorteil zu Lasten anderer (kooperierender) Staaten. Wenn allerdings alle Staaten nicht-kooperieren, fällt das System des Datenschutzes zu Lasten der einzelnen Unternehmen zusammen. Je nach Höhe der anfallenden Transaktionskosten kann diese schwierige Situation in ein Dilemma münden, das von der Forschung als sog. Gefangenendilemma<sup>36</sup> aufgefaßt wird. Dieses Dilemma setzt eine bestimmte Situation mit zwei Spielern voraus, in der jeder Spieler mit dem anderen kooperieren oder eine solche Kooperation verweigern kann.<sup>37</sup> Kooperieren beide, erhalten sie eine hohe Belohnung. Lehnen beide die Kooperation ab, werden sie beide bestraft. Will der eine kooperieren und der andere lehnt dies ab, erhält der Kooperationswillige nichts; der andere bekommt eine noch höhere Belohnung als bei beiderseitiger Kooperation.

### 2. Spielstrategien

Derzeit werden verschiedene Strategien zur Bewältigung dieses Dilemmas diskutiert. Diese reichen von der Taktik des Free Riding (a) über das sog. „Tit for Tat“ (b) bis hin zu komplexen Strategien für das n-Personen-Gefangenendilemma (c).

#### a) Free Rider

Olson vertrat die Ansicht, daß das Gefangenendilemma letztendlich nicht lösbar sei. Statt dessen sei es die rationalste Strategie, als Trittbrettfahrer das Vertrauen anderer zu mißbrauchen: „Rational, self-interested individuals will not act to achieve their common or group interests.“<sup>38</sup> Nach dieser Ansicht muß die Einführung internationaler Kontrollsysteme an

den sog. Free-Ridern, d.h. den Außenseitern, die sich nicht an dem System beteiligen, per se scheitern.<sup>39</sup>

Diese Free-Rider-Situation prägte lange Zeit die Situation innerhalb Europas. Jeder Staat schuf sein eigenes Datenschutzrecht ohne Rücksicht auf andere.<sup>40</sup> So besaßen bis 1995 nur sieben EU-Mitgliedstaaten Rechtsvorschriften zum Datenschutz (Deutschland, Dänemark, Frankreich, Irland, Luxemburg, Niederlande und Großbritannien). Alle anderen Staaten kannten keine speziellen Datenschutzgesetze. Insofern war innerhalb Europas ein starkes Nord-Süd-Gefälle entstanden: Im Süden Europas (und zusätzlich in Belgien) war jegliche Verarbeitung von personenbezogenen Daten (noch) fast ohne jede rechtliche Beschränkung möglich, während im Norden Europas detaillierte Kontrollmechanismen geschaffen wurden. Damit entstand aber die Gefahr, daß sich besondere „Daten-oasen“ herausbilden: Unternehmen könnten gefahrlos ihre Daten in Italien oder Spanien verarbeiten lassen, um dem rigiden Datenschutz deutscher oder englischer Provenienz zu entgehen. Die Herabsetzung des Datenschutzniveaus führte folglich zu einem volkswirtschaftlichen Wachstum, einem Ertrag, der sich für die einzelnen Staaten bezahlt machte.

Die düstere Free-Rider-Prognose geht allerdings davon aus, daß das „Spiel“ nur einmal durchgeführt wird. Tatsächlich erscheint es bei einmalig auftretenden Situationen nicht rational, Kooperationen einzugehen. Statt dessen kann Kooperation rational nur bei Wiederholung des „Spiels“ begründbar sein, bei dem sich ein Spieler auf die Strategien der anderen Mitspieler einstellen kann. Von daher fragt sich, ob der Aufbau von Daten-oasen auch langfristig für die nationale Wirtschaft vorteilhaft ist.

#### b) Tit for Tat

Mit iterativen „Spielen“ hat sich Robert Axelrod beschäftigt. Axelrod ist der Nachweis gelungen, daß es in einem Zwei-Personen-Spiel nur eine Strategie gibt, die am effektivsten funktioniert: „Tit for Tat“ (Wie Du mir, so ich Dir).<sup>41</sup> Diese Taktik beinhaltet, „im ersten Zug zu kooperieren und dann zu tun, was der andere Spieler im vorangegangenen Zug gemacht hat“<sup>42</sup>. In der Zwischenzeit ist diese Strategie durch andere Forscher noch erweitert und verfeinert worden. So wird teilweise ein „generous tit for tat“<sup>43</sup> vorgeschlagen, bei dem ein Spieler auf jede Kooperation mit Kooperation und auf Nichtkooperation in regelmäßigen Abständen ebenfalls mit Kooperation reagiert. Neuerdings wird auch eine Strategie mit der Bezeichnung „pavlov“ oder „Win-stay/Lose-shift“ diskutiert<sup>44</sup>, bei der ein Spieler nur kooperiert, wenn beide Spieler sich im vorherigen Zug für die gleiche Strategie entschieden haben.

Allen Strategien ist gemeinsam, daß sie kooperationsfreundlich sind. Kooperation kann demnach durchaus die strategisch effektivste Strategie auch von datenschutzreglementierenden Staaten sein. Umgekehrt sind sich alle Spieltheoretiker darin einig, daß langfristig eine Strategie der Kooperationsverweigerung ökonomisch nachteilig und damit irrational ist.

Allerdings setzen die Strategien voraus, daß die Spiele wiederholt werden und die Spieler nicht nur aus Kooperations-unwilligen bestehen<sup>45</sup>:

„Eine Welt ‚Böswilliger‘ kann einer Invasion durch jeden widerstehen, der irgendeine andere Strategie verwendet, vorausgesetzt, die Fremden kommen einzeln an. (...) Wenn die

Neulinge jedoch in kleinen Gruppen ankommen, haben sie durchaus eine Chance, Kooperation in Gang zu setzen.“<sup>46</sup>

Axelrod zieht hieraus die weitere Konsequenz, daß Kooperation durch Vermittlung von Gruppen die erfolgreichste Spielstrategie ist:

„Also kann wechselseitige Kooperation in einer Welt von Egoisten ohne zentrale Kontrollinstanz entstehen, wenn sie mit einer Gruppierung von Individuen beginnt, die sich auf Gegenseitigkeit verlassen.“<sup>47</sup>

Nach Axelrod ist demnach Kooperation durchaus in einer Welt von Egoisten begründbar. Allerdings sind dabei langfristige Beziehungen und das Vorhandensein einer kooperativ eingestellten Gruppe notwendige und hinreichende Bedingungen.

Was ergibt sich hieraus für die Harmonisierung des Datenschutzrechts? „Tit for Tat“ – dies ist aus meiner Sicht das Modell für den innereuropäischen Datenschutz. Hier haben sich die Staaten erstmals auf eine Kooperation, auf ein einheitliches Datenschutzniveau geeinigt. Durch die engen Bindungen der europäischen Staaten untereinander würde die Bildung von Daten-oasen auch für den jeweiligen „Oasen“-Staat empfindliche Nachteile mit sich bringen. Die anderen Staaten sähen sich gezwungen, den Datenexport in den datenschutzfreien Staat zu reglementieren. Dadurch wäre die erhoffte Abwanderung von Unternehmen oder Auslagerung von Unternehmensfunktionen ins Ausland ineffizient geworden. Nur bei langfristiger Kooperation läßt sich diese Entwicklung von Datenschutzfestungen umgehen.

Daher sieht die Datenschutzrichtlinie die freie Zirkulierung von Daten innerhalb der Europäischen Union bei gleichzeitiger Harmonisierung des Datenschutzniveaus vor. Nach Art. 1 Abs. 2 dürfen die Mitgliedstaaten den freien Verkehr personenbezogener Daten untereinander nicht aus Gründen des Datenschutzes beschränken. Man entnimmt aus dieser Regelung, daß der Datenschutzstandard innerhalb der EU mit Umsetzung der Richtlinie einheitlich sein wird und soll. Innerhalb dieses europäischen Datenraums soll dann jede nationale Beschränkung des Datenverkehrs unzulässig sein. Beschränkungen dürfen nur noch auf die EG-Richtlinie, nicht aber auf nationale Sonderregeln gestützt sein<sup>48</sup>. Ob dieses Ideal wirklich erreicht wird, ist aber nach der Neukonzeption des Richtlinienartikels äußerst fraglich. Der Text der Richtlinie enthält zahlreiche nationale Vorbehalte<sup>49</sup>; insoweit werden die Mitgliedstaaten weiterhin eigene Wege gehen können. Die Kooperation steht auf wackeligen Füßen; es bleibt abzuwarten, wie die Richtlinie in den verschiedenen Mitgliedstaaten umgesetzt werden wird.

#### c) n-Personen-Gefangenen-Dilemma

Die Überlegungen Axelrods gelten zunächst einmal nur für das Verhalten zweier Personen zueinander. Situationen, in denen mehr als zwei Personen agieren, bedürfen daher einer erweiterten Modellierung. Hierbei wird in der spieltheoretischen Forschung mit dem n-Personen-Gefangenen-Dilemma argumentiert. Die Ergebnisse in diesem Bereich sind derzeit noch uneinheitlich und widersprüchlich.<sup>50</sup> Allerdings schälen sich allmählich bestimmte Kriterien für eine Anwendung des Tit-for-Tat-Prinzips in sozialen Dilemmata ab. Hiernach ist bei Entscheidungen, an der mehr als zwei Personen beteiligt sind, neben der Langfristigkeit der Beziehungen<sup>51</sup> die Überschaubarkeit der Gruppe<sup>52</sup> und das darin vorhande-

ne Kommunikationsgefüge über die Berechenbarkeit des Verhaltens<sup>53</sup> wichtig.

Innerhalb der Europäischen Union ist ein solches Kommunikationsgefüge in der Zwischenzeit vorhanden. Daher war es nur konsequent, daß die Richtlinie den Europäischen Datenraum datenschutzrechtlich freigegeben hat (s.o.). Abzuwarten bleibt, wie die neuen, der EU assoziierten Staaten das komplexe Kooperationsgefüge beeinflussen.

Die europäischen Mitgliedstaaten hatten aber große Probleme damit, die Freiheit des innereuropäischen Datenverkehrs auf andere Staaten auszuweiten. Statt dessen hat man sich für den Export von Daten in Drittstaaten, d.h. in Staaten, die nicht der EU angehören, für eine prinzipielle Kooperationsverweigerung entschieden. Ein Datentransfer in einen Drittstaat ist nach dem Wortlaut von Art. 25 Abs. 1 grundsätzlich unzulässig. Ausnahmsweise ist er im Einzelfall erlaubt, sofern der Drittstaat ein angemessenes Schutzniveau gewährleisten kann. Ein dauerhaftes Kooperationsangebot besteht nur, sofern der andere Staat nach Feststellung der Kommission seine eigene dauerhafte Kooperationswilligkeit durch Nachweis eines angemessenen Datenschutzniveaus gewährleistet (Art. 25 Abs. 6). Wann ein solches Schutzniveau vorliegt, bleibt aber auch im neuen Entwurf unklar. Offen ist z.B., ob das EU-Recht oder das nationale Datenschutzrecht als Maßstab dienen soll. Beides ist nach dem zweiten Entwurf nicht identisch, da dieser Entwurf weitreichende nationale Vorbehalte enthält (s.o.). Nach Erwägungsgrund 60 sind Übermittlungen in Drittstaaten „auf jeden Fall nur unter voller Einhaltung der Rechtsvorschriften zulässig, die die Mitgliedstaaten gemäß dieser Richtlinie, insbesondere gemäß Artikel 8, erlassen haben“. Dies bedeutet, daß für die Beurteilung der Angemessenheit das infolge der Datenschutzrichtlinie geschaffene, nationale Recht zählt. Damit konterkariert sich die Richtlinie aber selbst. Es könnte künftig der Fall auftreten, daß Italien die Datenübermittlung in die USA zuläßt, während Deutschland diese aufgrund anderer Umsetzung der Datenschutzrichtlinie verbietet. Unternehmen mit Sitz in Deutschland werden dann überlegen müssen, ihr Rechenzentrum nach Italien zu verlagern. Damit ist das in Art. 1 Abs. 2 verankerte europäische Kooperationsmodell durch Art. 25 ad absurdum geführt. An dieser Schwierigkeit ändert auch das Feststellungsverfahren nach Art. 25 Abs. 4 und 6 nichts. Zwar kann die Kommission hier nach die Angemessenheit des Datenschutzniveaus für alle Mitgliedstaaten feststellen; sie ist dabei aber an die Richtlinie selbst gebunden, die für die Angemessenheit offensichtlich auf den Vergleich mit innerstaatlichen Schutzvorschriften abstellt.

Im übrigen kann das Recht des ausländischen Staates nicht nur an der Meßlatte seiner Gesetze gemessen werden; vielmehr ist die Umsetzung dieser gesetzlichen Regelungen in der Praxis erforderlich. Neben dem geschriebenen Recht sind Rechtsprechung und die Tätigkeit der Aufsichtsorgane zu beachten; dabei sind auch zeitliche Veränderungen zu berücksichtigen. All dies läßt eine Prüfung der Angemessenheit fast aussichtslos erscheinen. Schließlich ist nicht klar, wer die Angemessenheit feststellt. Daß die Europäische Kommission autoritativ Feststellungen zum Datenschutzrecht in allen Staaten der Welt trifft, klingt utopisch. Wenn aber nicht die Europäische Kommission die Angemessenheit prüft, bleibt die Entscheidung dem einzelnen Mitgliedsstaat oder gar dem privaten DV-Anwender überlassen. Angesichts der damit verbundenen unterschiedlichen Prüfungsergebnisse bleibt die Idee einer Vereinheitlichung des internationalen Datentransfers auf der Strecke.

Allerdings nimmt auch der ungarische Staat für sich eine Kontrolle der Datenströme ins Ausland in Anspruch. Nach Art. 9 dürfen personenbezogene Daten nur an speichernde Stellen im Ausland übermittelt werden, wenn der Betroffene einwilligt oder es durch Gesetz erlaubt ist. Beide Erlaubnistatbestände<sup>54</sup> stehen unter der Voraussetzung, daß die gleichen Grundsätze des Datenschutzes durch die ausländische speichernde Stelle gewährleistet werden. Dieser Zusatz verwundert, müssen doch Daten bei Einwilligung des Betroffenen auch ohne Vorhandensein eines angemessenen Datenschutzniveaus transferiert werden dürfen<sup>55</sup>. Im übrigen finden sich gesetzliche Bestimmungen zum Datentransfer nicht. Auch ist der Verweis auf das Datenschutzniveau fatal, da damit eine Datenübermittlung zwischen Deutschland und Ungarn aufgrund der Unterschiede in der Datenschutzgesetzgebung unmöglich wäre. Von daher ist Ungarn auch im Verhältnis zur Europäischen Union noch eine datenschutzrechtliche Festung. Man kann nur hoffen, daß sich auf lange Sicht auch Ungarn dem Kooperationsgedanken öffnet und die Freiheit des europäischen Datenverkehrs unterstützt.

## Literaturverzeichnis

### I. Kommentare und Monographien

- von Arnim, Hans Herbert, Gemeinwohl und Gruppeninteressen, 1977 (zit.: von Arnim, Gemeinwohl).
- Axelrod, Robert, The Evolution of Cooperation, New York 1984 (zit.: Axelrod, Evolution).
- Bergmann/Möhrle/Herb, Datenschutzrecht, Loseblattausgabe, Stuttgart Stand: Oktober 1995 (zit.: Bergmann/Möhrle/Herb, § Rdnr.).
- Hardin, Russell, Collective Action, Baltimore 1982 (zit.: Hardin, Action).
- Krebs, David M., Game Theory and Economic Modelling, Oxford 1990 (zit.: Krebs, Theory).
- Krouse, Clement G., Theory of Industrial Economics, Cambridge 1990 (zit.: Krouse, Theory).
- Neumann, Helmut, Staatliche Regulierung betrieblicher Beschäftigungspolitik. Ein Vergleich zentraler und dezentraler Arbeitsmarktinstitutionen, Frankfurt 1991 (zit.: H. Neumann, Regulierung).
- North, Douglas C., Institutionen, institutioneller Wandel und Wirtschaftsleistung, Tübingen 1992 (zit.: North, Institutionen).
- Olson, Mancur, The Logic of Collective Action, Cambridge 1962 (zit.: Olson, Logic).
- ders., Die Logik des kollektiven Handelns, Tübingen 1968 (zit.: Olson, Logik).
- Posner, Richard A., Economic Analysis of Law, 2. Aufl., Boston 1977 (zit.: Posner, Analysis).
- Ridder-Aap, Christa-Maria, Die moderne Aktiengesellschaft, Frankfurt 1980 (zit.: Ridder-Aap, Aktiengesellschaft).
- Schäfer, Hans-Bernd/Ott, Claus, Lehrbuch der ökonomischen Analyse des Zivilrechts, Berlin 1986 (zit.: Schäfer/Ott, Lehrbuch).
- Spiros Simitis/Ulrich Dammann u.a., Kommentar zum Bundesdatenschutzgesetz, Loseblatt, 4. Aufl. Baden-Baden ab 1992 (zit.: Simitis/Dammann, BDSG § Rdnr.).
- diess., Kommentar zum Bundesdatenschutzgesetz, 3. Aufl. Baden-Baden 1978 (zit.: Simitis/Dammann, BDSG, 3. Aufl., § Rdnr.).
- Taylor, Michael, The possibility of cooperation, Cambridge 1987 (zit.: Taylor, Possibility).
- Terhart, Klaus, Die Befolgung von Umweltschutzmaßnahmen als betriebswirtschaftliches Entscheidungsproblem, Berlin 1986 (zit.: Terhart, Befolgung).

## II. Aufsätze

- Akerlof, George, The Market for „Lemons“: Quality, Uncertainty and the Market Mechanism, in: Quarterly Journal of Economics 84 (1970), 488–500.
- Bergh, Roger van den/Faure, Michael, Self-regulation of the professions in Belgium, in: IRLE 1991, 165–182.
- Bossmann, Eva, Volkswirtschaftliche Probleme der Transaktionskosten, in: ZgesStW 138 (1982), 664–679.
- Dahlmann, Carl J., The Problem of Externality, in: Journal of Law and Economics 22 (1979), 141–161.
- Dawes, Robyn M., Social Dilemmas, in: Annual Review of Psychology 31 (1980), 169–193.
- Enderle, Georges, Artikel Selbstregulierung, in: ders. (Hg.), Lexikon der Wirtschaftsethik, Freiburg 1993, Sp. 945–951.
- Edwards, L.N./Edwards, F.R., Measuring the Effectiveness of Regulation: The Case of Bank Entry Regulation, in: Journal of Law and Economics 17 (1974), 445–483.
- Fastenrath, Ulrich, Die Struktur der erweiterten Europäischen Union, in: Ulrich Everling (Hg.), Von der Europäischen Gemeinschaft zur Europäischen Union, Europarecht Beiheft 1/1994, 101–137.
- Finkelstein, Claire, Financial Distress as a Noncooperative Game: A Proposal for Overcoming Obstacles to Private Workouts, in: Yale LJ 102 (1993), 2205–2230.
- Frey, Bruno S./Ramser, Hans-Jürgen, Where are the Limits of Regulation?, in: ZgesStW 142 (1986), 571–580.
- Garvin, David A., Can Industry Self-Regulation Work?, in: California Management Review 25 (1983), Heft 4, 37–52.
- ders., Deregulation and Self-Regulating, in: The Wharton Magazine, Spring 1981, 57–63.
- Gupta, A.K./Lad, L.J., Industry Self-Regulation: An economic, organisational and political analysis, in: Academy of Management Review 8 (1983), 416–425.
- Hamburger, Henry, N-person Prisoner's Dilemma, in: Journal of Mathematical Sociology 3 (1973), 27–48.
- Hardin, Russell, Collective Action as an Agreeable n-Prisoner's Dilemma, in: Behavioral Science 46 (1984), 154–181.
- ders., The tragedy of the commons, in: Science 162 (1968), 1243–1248.
- Jordan, W.A., Producer Protection, Prior Market Structure and the Effects of Government Regulation, in: Journal of Law and Economics 15 (1972), 151–186.
- Kaiser, Joseph H., Industrielle Absprachen im öffentlichen Interesse, in: NJW 1971, 585–588.
- Leipold, Helmut, Ordnungspolitische Implikationen der Transaktionskostenökonomie, in: Ordo 36 (1985), 31–50.
- Marwell, G./Ames, R.E., Experiments on the provision of public goods I: resources, interest, group size, and the free-rider problem, in: American Journal of Sociology 84 (1979), 1335–1360.
- Milinski, Manfred, Cooperation wins and stays, in: Nature 1993, heft 364, 12–13.
- Möschel, Wernhard, Privatisierung, Deregulierung und Wettbewerbsordnung, in: JZ 1988, 885–893.
- Nelson, Philipp, Information and Consumer Behavior, in: Journal of Political Economy 78 (1970), 311–329.
- Nowak, Martin/Sigmund, Karl, New strategies, in: Nature 1992, Heft 355, 250–253.
- diess., A strategy of win-stay, lose-shift that outperforms tit for tat in the Prisoner's Dilemma game, in: Nature 1993, Heft 364, 56–58.
- Orbell, J.M./Rutherford, B., Can Leviathan make the life of man less solitary, poor, nasty, brutish, and short?, in: British Journal of Political Science 3 (1973), 383–407.
- Peltzman, S., Entry in Commercial Banking, in: Journal of Law and Economics 8 (1965), 11–29.
- Philippis, Lothar, Artificial Morality and Artificial Law, in: Artificial Intelligence and Law 2 (1993), 51–63.

- Posner, R.A., Theories of Economic Regulation, in: The Bell Journal of Economics and Management Science 5 (1974), 335–349.
- Schofield, Norman, Anarchy, Altruism and Cooperation: A Review, in: Social Choice and Welfare 2 (1985), 207–219.
- Tietzel, M., Die Rationalitätsannahme in den Wirtschaftswissenschaften, in: Jahrbuch für Sozialwissenschaften 1981, 115–133.
- Ulmer, Peter, Die freiwillige Selbstkontrolle in Wirtschaft und Presse, in: WRP 1975, 549–561.

## Anmerkungen

- 2 ABl. EG L 347 vom 31. Dezember 1993, in Kraft seit 1. Februar 1994. Siehe auch BGBl. II 1473 und das entsprechende bundesdeutsche Zustimmungsgesetz vom 26. August 1993, BGBl. II 1472.
- 3 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG L 281 vom 23. November 1995, 31.
- 4 § 59 (1) der ungarischen Verfassung enthält das Recht des Betroffenen auf vollständige Kenntnis der gespeicherten und verarbeiteten Daten; ähnlich die Entscheidung des Ungarischen Verfassungsgerichts 15/1991. § 83 des Ungarischen Zivilgesetzbuch aus dem Jahre 1977 enthielt kurze Bestimmungen zu Berichtigungsansprüchen des Betroffenen (Simitis/Dammann u.a., BDSG-Dokumentation, D 15.1).
- 5 Ungarisches Datenschutzgesetz Nr. LXIII von 1992 über den Schutz von personenbezogenen Daten und die Offenlegung von Daten im öffentlichen Interesse. Dem Text liegt die deutsche Übersetzung von Thomas Mühlelein und Désirée Zolotas, datiert am 11. Januar 1994, zugrunde; mein besonderer Dank gilt PD Dr. Herbert Burkert für die Übersendung der Übersetzung.
- 6 So etwa Art. 3 (1) mit dem Prinzip des Verbots mit Erlaubnisvorbehalt.
- 7 So etwa die Einführung eines besonderen Schutzes spezieller Datenarten (Art. 2 Nr. 2, Art. 3 Abs. 2).
- 8 Dies gilt vor allem für die Regeln zur Qualität von Daten (Art. 7).
- 9 Der Begriff der „New Institutional Economics“ umfaßt die Theorie der Property Rights, die ökonomische Theorie des Rechts, die Transaktionskostenökonomie und andere Ansätze. Vgl. hierzu Schäfer/Ott, Lehrbuch, 67 ff.; Leipold, Ordo 36 (1985), 31 ff.; Posner, The Bell Journal of Economics and Management Science 5 (1974), 341 f.
- 10 Vgl. zu den im folgenden zugrunde liegenden Prämissen Posner, Analysis, 12 ff., 19 ff.
- 11 In der Forschung wird dies als sog. REM-Hypothese, d.h. als Hypothese des rationalen egoistischen Menschen, bezeichnet; vgl. Schäfer/Ott, Lehrbuch, 46 ff.; Tietzel, Jahrbuch für Sozialwissenschaften 1981, 115 ff. Diese Hypothese wird im folgenden nur als empirische Prämisse, nicht aber als normatives Postulat verwendet; ob ein Unternehmen rational-egoistisch und profitorientiert arbeiten soll, ist nicht Gegenstand dieser Untersuchung.
- 12 Vgl. Schäfer/Ott, Lehrbuch, 63.
- 13 Vgl. zu den verschiedenen Nutzen- und Kostentheorien Schäfer/Ott, Lehrbuch, 53 ff. und 61 ff.
- 14 Zu dieser Konstellation finden sich einige betriebswirtschaftliche Kostenrechnungen; siehe etwa Terhart, Befolgung, 131 ff. für die Befolgung von Umweltschutzaufgaben.
- 15 Leipold, Ordo 36 (1985), 33; ähnlich auch Dahlmann, Journal of Law and Economics 22 (1979), 141 ff.; Bossmann, ZgesStW 138 (1982), 664 ff.
- 16 Vgl. die Definition bei Ridder-Aap, Aktiengesellschaft, 44. Ähnlich auch North, Institutionen, 33.

- 17 In der spärlichen Literatur zu diesem Thema wird durchweg allein auf die Durchsetzungskosten abgestellt; vgl. Terhart, Befolgung, 122 ff.
- 18 Vgl. hierzu Dales, CJE 8 (1975), 488.
- 19 Zuletzt LG Mannheim, Urteil vom 29. März 1996 – 7 O 43/96 (unveröff.).
- 20 BGH, GRUR 1969, 287, 290; Baumbach/Hefermehl, § 1 UWG Rdnr. 544.
- 21 Vgl. Terhart, Befolgung, 161.
- 22 Terhart, Befolgung, 158.
- 23 Siehe Terhart, Befolgung, 45. Auf S. 40 geht Terhart kurz auf die „Komplementarität zwischen Gewinn- und Umweltschutzziel“ ein, erklärt diesen Fall jedoch für die Ausnahme (S. 41).
- 24 In der Tat hat die Sphärentheorie hier ökonomische Relevanz. Je geringer die Sensibilität der Daten, desto geringer dürften die Erwartungen des Kunden an das Datenschutzniveau des Unternehmens sein. Folglich hat Datenschutz als Marketinginstrument beim klassischen Adresshandel eine untergeordnete, wirtschaftliche Bedeutung.
- 25 Siehe hierzu allgemein Schäfer/Ott, Lehrbuch, 305 ff.; Akerlof, Quarterly Journal of Economics 84 (1970), 488 ff.; van den Bergh/Faure, IRL 1991, 165, 171 f.; Enderle, in: ders. u.a. (Hg.) Wirtschaftsethik, Sp. 945, 947 f.
- 26 Zur Differenzierung von Inspektions-, Erfahrungs- und Vertrauensgütern siehe Nelson, Journal of Political Economy 78 (1970), 311 ff.
- 27 So auch Möschel, JZ 1988, 885, 893.
- 28 Krouse, Theory, 290.
- 29 Höffe, Rechtsprinzipien, 301.
- 30 Axelrod, Evolution 4.
- 31 Die Literatur zu diesem Themenkreis ist nicht mehr überschaubar. Im folgenden wurde im wesentlichen herangezogen Axelrod, Evolution, insbes. 4 ff.; Krebs, Game Theory, 9 ff.; Krouse, Theory, 290 ff.; North, Institutionen, 13 ff.; Taylor, Cooperation, 34 ff. Im folgenden werden die mathematischen Grundlagen der Spieltheorie nicht referiert, um den Rahmen der Untersuchung nicht zu sprengen.
- 32 Zum Begriff der Strategie vgl. Krebs, Theory, 21 ff.
- 33 Vgl. Garvin, California Management Review 25 (1983), 37 ff.; Gupta/Lad, Academy of Management Review 8 (1983), 416 ff.; Marwell/Ames, American Journal of Sociology 84 (1979), 1335 ff. mit weit. Nachw. Siehe zur Anwendung zur Spieltheorie in der Rechtsinformatik grundlegend Philipps, Artificial Intelligence and Law 2 (1993), 51 ff.
- 34 Axelrod, Evolution, 8. Ähnlich Finkelstein, Yale LJ 102 (1993), 2205, 2209.
- 35 Dawes, Ann. Rev. Psychol. 31 (1980), 169.
- 36 Der Name stammt von einer Anekdote, in der zwei Straftäter nach einem gemeinsamen begangenen Verbrechen vom Staatsanwalt getrennt vernommen werden. Dieser verspricht jedem der beiden Täter, daß er im Falle eines Geständnisses freigelassen werde und sein nicht geständiger Kompagnon die Höchststrafe erhalte. Sofern beide gestehen, sollen beide eine milde Strafe bekommen; gesteht keiner, kann (aus Mangel an Beweisen) nur eine Mindeststrafe verhängt werden. Vgl. Krebs, Theory, 36 ff.; Dawes, Annual Review of Psychology 31 (1980), 169, 182.
- 37 Hinsichtlich der Definition des Gefangenendilemmas siehe Axelrod, Evolution, 7 und 186.
- 38 Olson, Logic, 2; ähnlich auch Hardin, Behavioral Science 16 (1971), 472 ff.
- 39 So auch das Ergebnis von Hardin, Science 162 (1968), 1243, 1247; Orbell/Rutherford, British Journal of Political Science 3 (1973), 383 ff.
- 40 Siehe hierzu Simitis, in: ders./Dammann, BDSG, § 1 Rdnr. 155.
- 41 Vgl. Axelrod, Evolution, 26 ff. Siehe hierzu auch die Darstellung von Höffe, Rechtsprinzipien, 285 ff.
- 42 Axelrod, Evolution, 12.
- 43 Nowak/Sigmund, Nature 355 (1992), 250 ff.
- 44 Vgl. Milinski, Nature 1993, Heft 364, 12 ff.; Nowak/Sigmund, Nature 1993, Heft 364, 56 ff.
- 45 Siehe hierzu Hardin, Action, 145 ff. Vgl. zur kollektiven Stabilität der IMMER D-Spieler das fünfte Theorem bei Axelrod, Evolution, 56 ff.
- 46 Axelrod, Evolution, 57.
- 47 Axelrod, Evolution, 62.
- 48 Vgl. hierzu ausführlich Ehmann, 'Vertragslösungen' auf der Basis der EG-Datenschutzrichtlinie, in: CR 1991, 234 ff.
- 49 Art. 8 IV, V; 13, 18 II, III, IV, V u.a.
- 50 Vgl. Hardin, Action, 153 f. und 188 ff.; Taylor, Cooperation, 82 ff.; Dawes, Ann. Rev. Psychol. 31 (1980), 169, 182 ff.; Hamburger, Journal of Mathematical Sociology 3 (1973), 27 ff.; Schelling, Journal of Conflict Resolution 17 (1973), 381 ff.
- 51 Zu weit geht North, der aus dem Erfordernis der Iterativität den Zwang ableitet, daß „das Spiel endlos fort dauert“. Vgl. ders., Institutionen, 68.
- 52 Vgl. auch Olson, Logik, 35: „Kurz, je größer eine Gruppe ist, um so weniger wird sie ihre gemeinsamen Interessen fördern.“ Ähnlich (trotz Kritik an den Olsonschen Prämissen) Taylor, Cooperation, 8 ff., insbes. 12 f.
- 53 So auch Schofield, Social Choice and Welfare 2 (1985), 212 f.
- 54 Die deutsche Übersetzung ist hier nicht ganz zweifelsfrei; es bleibt unklar, worauf sich der Hinweis auf das Datenschutzniveau bezieht.
- 55 So auch die Endfassung der Richtlinie (Art. 26 Abs. 1 lit. a) im Gegensatz zu den Vorentwürfen.

*Stichwörter:* Definierungskosten, Durchsetzungskosten, EG-Datenschutzrichtlinie, Free Rider, Gefangenendilemma, moderner Pranger, Registrierung, Spieltheorie, Tit for Tat, Überwachungskosten, ungarisches Datenschutzgesetz, Verbände, Vertrauensgüter, Wettbewerb, Widerspruchsrecht