

**Rechtsinformatik V**  
(Wintersemester 2007 / 2008)  
RA Prof. Dr. Jochen Schneider

**Seminararbeit**

Der Widerspruch von staatlich verordneter  
Datensicherung und staatlicher Datenspionage

Alessandro Fuschi  
XXXXXXXXXXXX XX  
XXXX München

Matrikel-Nr.: XXXXXX  
5. Fachsemester

# Gliederung

I. Einleitung.....	1
1.) Ziel der Arbeit.....	1
2.) Verwendete Begriffe.....	1
a.) „Datenschutz“.....	1
b.) „Datensicherheit“.....	1
II. Aktuelle Anforderungen.....	2
1. Nach BDSG.....	2
2. Nach TKG.....	2
a.) Fernmeldegeheimnis.....	2
b.) TK-Datenschutz.....	3
c.) Öffentliche Sicherheit.....	3
3. Nach BayDSG.....	4
III. Strafrecht und Datensicherheit.....	5
1. Vorschriften zum Schutz.....	5
a.) § 206 StGB.....	5
b.) § 202 a StGB.....	5
c.) § 202 b StGB.....	6
d.) §§ 89, 148 TKG.....	6
e.) § 202 c StGB.....	7
f.) §§ 303 a, 303 b StGB.....	8
2. Vorschriften gegen Schutz.....	9
a.) § 202 a StGB.....	9
b.) § 202 c StGB.....	10
c.) §§ 100 a ff. StPO.....	11
IV. Geplante Maßnahmen: Die Online-Durchsuchung.....	13
1. Aktuelle Gesetzeslage im Bund.....	13
2. Gesetze zur Online-Durchsuchung.....	14
3. Politische Positionen.....	14
aa.) CDU / CSU.....	14
bb.) SPD.....	14
cc.) FDP.....	15
dd.) Bündnis 90 / Die Grünen.....	16
ee.) Die Linke.....	16

4. Technische Grundlagen.....	16
a.) Funktionsweise.....	16
b.) Installation.....	17
5. Technische und sicherheitsbezogene Probleme.....	17
a.) Firewalls.....	17
b.) Router.....	18
c.) Anti-Viren-Software.....	18
d.) Betriebssystem.....	19
e.) Read-Only Systeme.....	20
f.) Steganographie.....	20
g.) Entdeckung und Fehlinformation.....	20
h.) Sicherheitslücken durch Disassembling.....	21
6. Rechtliche Probleme.....	21
a.) Internationalität.....	21
b.) Art. 13 GG.....	21
c.) Recht auf informationelle Selbstbestimmung.....	22
aa.) Kernbereich der Privatsphäre.....	22
bb.) Verhältnismäßigkeit.....	22
d.) Gefahr der Ausweitung.....	23
e.) Gefahr der Manipulation.....	23
f.) Gefahr kommerzieller Nutzung.....	24
g.) Schadensersatzforderungen gegen den Staat.....	24
V. Fazit.....	24

## Literaturverzeichnis

- *Cornelius, Kai*: „Zur Strafbarkeit des Anbietens von Hackertools“, CR 2007, 682.
- *Eckhardt, Jens*: „Die Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen im TKG“, CR 2007, 405.
- *Ernst, Stefan (Hrsg.)*: Hacker, Cracker & Computerviren, 2004.
- *ders.*: „Das neue Computerstrafrecht“, NJW 2007, 2661.
- *Gercke, Marco*: „Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit“, CR 2007, 245.
- *Gliss, Hans*: „Bundestrojaner" - die Schnapsidee des Jahres“, DSB 2007, 15.
- *Holznagel, Bernd / Enaux, Christoph / Nienhaus, Christian*: Telekommunikationsrecht, 2. Auflage 2006.
- *Koenig, Christian / Loetz, Sascha / Neumann, Andreas*: Telekommunikationsrecht, 2004.
- *Kutscha, Martin*: „Verdeckte 'Online-Durchsuchung' und Unverletzlichkeit der Wohnung“, NJW 2007, 1169.
- *Leipold, Klaus*: „Die Online-Durchsuchung“, NJW-Spezial 2007, 135.
- *Marberth-Kubicki, Annette*: „Neuregelungen des Computerstrafrechts: Veränderungen und Neuerungen durch das 41. StrÄndG zur Bekämpfung der Computerkriminalität“, ITBR 2008, 17.
- *Prantl, Heribert*: „Die Schranken des Rechtsstaats“, *Süddeutsche Zeitung* vom 07.09.2007.
- *Rieß, Peter (Hrsg.)*: Löwe-Rosenberg: Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 25. Auflage 2004.
- *Schönke, Adolf / Schröder Horst (Begr.)*: Strafgesetzbuch, 27. Auflage 2006.
- *Schulz, Alexander*: „Neue Strafbarkeiten und Probleme - Der Entwurf des Strafrechtsänderungsgesetzes (StrafÄndG) zur Bekämpfung der Computerkriminalität vom 20.09.2006“, MIR 2006, Dok. 180; online abrufbar unter: <http://miur.de/dok/398.html>.
- *Steckler, Brunhilde*: Grundzüge des IT-Rechts, 2. Auflage 2006.
- *Tinnefeld, Marie-Theres*: „Online-Durchsuchung – Menschenrechte vs. Virtueller Trojaner“, MMR 2007, 137.

## **I. Einleitung**

### **1.) Ziel der Arbeit**

Ziel dieser Arbeit soll es sein, den Widerspruch aufzuzeigen, den der Gesetzgeber vor allem im Zuge der Terrorabwehr plant oder bereits umgesetzt hat, nämlich jenen zwischen der Pflicht zur Datensicherung, wie es z.B. das *Telekommunikationsgesetz* und das *Bundesdatenschutzgesetz* vorsehen und der staatlichen Versuche, im Rahmen der Gefahrenabwehr (Stichwort „Bundestrojaner“), sich Zugang zu eben jenen Daten zu verschaffen.

### **2.) Verwendete Begriffe**

Unterschieden werden müssen die Begriffe „Datenschutz“ und „Datensicherung“. Beide werden oftmals synonym verwendet, ihre Bedeutung unterscheidet sich jedoch grundlegend:

#### **a.) „Datenschutz“**

Unter „Datenschutz“ versteht man das Recht jedes Einzelnen im Rahmen des ihm zustehenden informationellen Selbstbestimmungsrechts<sup>1</sup> zu entscheiden, was mit seinen Daten geschieht und sich gegebenenfalls gegen Missbrauch zu wehren.<sup>2</sup>

#### **b.) „Datensicherheit“**

Unter „Datensicherheit“ versteht man dagegen die Pflicht zum Schutz personenbezogener Daten von unbefugten Zugriff, Zerstörung oder Manipulation.<sup>3</sup>

## **II. Aktuelle Anforderungen**

### **1. Nach BDSG**

Nach § 9 BDSG haben die datenverarbeitenden Stellen alle Maßnahmen zu treffen, die erforderlich sind, um die Bestimmungen des BDSG einzuhalten. Die Erforderlichkeit ist durch die Verhältnismäßigkeit der Maßnahme zum angestrebten Schutzzweck begrenzt.<sup>4</sup> Für die automatisierte Datenverarbeitung im Besonderen gelten weitere Vorschriften, die in der Anlage zu § 9 Satz 1 BDSG zu finden sind, so unter anderem Zugangs- und Zugriffskontrollen, Zutrittsüberwachung, Weitergabe-, Eingabe- und

---

<sup>1</sup> Erstmals geprägt in BVerfGE 65, 1 ff. als Ausfluss von Art. 2 I GG i.V.m. Art. 1 I GG.

<sup>2</sup> Steckler, Grundzüge des IT-Recht, S. 61.

<sup>3</sup> Steckler, aaO (Fn. 2).

<sup>4</sup> Steckler, aaO (Fn. 2), S. 98.

Organisationskontrolle und Schutz vor Zerstörung oder Verlust.<sup>5</sup> § 11 BDSG regelt den (häufigen) Fall, dass die Datenverarbeitung durch ein externes Unternehmen vorgenommen wird. In diesem Fall besteht eine Pflicht zur Datensicherung sowohl bei Auftraggeber, der den Beauftragten sorgfältig und nach gewissen Formvorschriften auswählen muss, als auch beim Auftragnehmer.

## **2. Nach TKG**

### a.) Fernmeldegeheimnis

In § 88 TKG normiert das Gesetz das sog. einfachrechtliche Fernmeldegeheimnis als Ergänzung zu Art. 10 GG. Während das Grundgesetz dieses nur für den Staat bindend normiert, folgt aus § 88 TKG, dass auch alle privaten Dienstleister verpflichtet sind, dieses in identischer Weise zu gewähren.<sup>6</sup> Daraus folgt, dass der Dienstleister nur solche Daten speichern darf, inwieweit sie für die Erbringung der TK-Dienste erforderlich sind und auch nur solange dieser Zweck nicht erfüllt ist.<sup>7</sup>

Bereits das TKG normiert jedoch die Pflicht, Verbindungsdaten an staatliche Stellen auszuliefern, wenn der zugrunde liegende Paragraph das „kleine Zitiergebot“ in § 88 III 3 TKG erfüllt.<sup>8</sup>

Strafrechtlich flankiert wird § 88 TKG dabei von § 206 StGB, welcher die Weitergabe an Dritte bestraft.

### b.) TK-Datenschutz

Die §§ 91 ff. TKG regeln weiterhin das TK-Datenschutzrecht, dass neben den Regelungen des BDSG und der Länderdatenschutzgesetze steht und spezielle Regelungen für den Bereich der Telekommunikation trifft. Es schützt, anders als das allgemeine Datenschutzrecht, auch die Daten juristischer Personen.<sup>9</sup>

Die Art der zur Speicherung erlaubten Daten spezifiziert § 96 I TKG. In Abs. 2 wird klargestellt, dass diese nur für gesetzlich normierte Zwecke oder zum Aufbau weiterer Verbindungen verwendet werden dürfen, ansonsten sind sie nach Satz 2 nach Beendigung der Verbindung unverzüglich zu löschen.

---

<sup>5</sup> Steckler, aaO (Fn. 2), S. 99.

<sup>6</sup> Koenig/Loetz/Neumann, Telekommunikationsrecht, S. 197.

<sup>7</sup> Holznagel/Enaux/Nienhaus, Telekommunikationsrecht, Rn. 647.

<sup>8</sup> Koenig/Loetz/Neumann, aaO (Fn. 6), S. 198.

<sup>9</sup> Koenig/Loetz/Neumann, aaO (Fn. 6), S. 199.

Praktisch am bedeutendsten ist dabei die Speicherung zur Entgeldermittlung, in deren Rahmen auch zur Erstellung eines Einzelverbindungsachweises nach §§ 97, 99 TKG.<sup>10</sup>

### c.) Öffentliche Sicherheit

Ebenfalls im TKG geregelt sind, nach den §§ 91-107 zum TK-Datenschutz, in den §§ 108-115 TKG Normen zum Bereich öffentliche Sicherheit. Sie regeln, nach mancher Ansicht vollkommen misslungen,<sup>11</sup> u.a. die Bereitstellung von Notrufen, technische Schutzmaßnahmen, die technische Umsetzung von TK-Überwachung und zum Auskunftersuchen staatlicher Stellen.<sup>12</sup>

So sind Diensteanbieter z.B. nach § 109 TKG dazu verpflichtet, technische Schutzmaßnahmen zu treffen, die dem Schutz des Fernmeldegeheimnisses dienen sollen. Dies wird jedoch durch § 110 TKG konterkariert, der vorschreibt, dass Maßnahmen zur Überwachung eben jener Telekommunikation eingerichtet werden sollen.

Hier findet sich auch eine besonders einschneidende Regelung, die mit Wirkung vom 1.1.2008 in das Gesetz aufgenommen wurde: Die sog. Vorratsdatenspeicherung.<sup>13</sup> Die in den §§ 113 a und 113 b TKG normierten Vorschriften verpflichten jeden Diensteanbieter, Informationen über das Nutzungsverhalten all seiner Kunden für 6 Monate bereit zu halten. Dazu gehören u.a. Informationen über Rufnummer und Gesprächsdauer bzw. E-Mail-Adressen und Versandzeit und IP-Adressen und bei Zugang zum Internet, IP-Adresse und Verbindungszeit. Somit kann, entgegen der in §§ 91 ff. TKG getroffenen Regelungen, auch bis zu 6 Monate nach Beendigung aller Dienstleistungen, nachvollzogen werden, wer mit wem wie lang Kontakt hatte. Dies führt zu großen Bedenken, was die Verfassungsmäßigkeit dieser Protokollierung angeht, ist es doch mit Art. 10 GG und Art. 2 i.V.m. Art. 1 GG (Recht auf informelle Selbstbestimmung) eigentlich nicht vereinbar.<sup>14</sup> Außerdem höhlt es die vorher besprochenen Regelungen z.T. komplett aus, da eine Speicherung von Daten ohne Einverständnis und ohne konkreten Verdachtsmoment (wie bei einer Telefonüberwachung) stattfindet.

---

<sup>10</sup> Koenig/Loetz/Neumann, aaO (Fn. 6), S. 202 ff.

<sup>11</sup> Koenig/Loetz/Neumann, aaO (Fn. 6), S. 208.

<sup>12</sup> Holznagel/Enaux/Nienhaus, Telekommunikationsrecht, Rn. 688.

<sup>13</sup> Informationen hierzu finden sich z.B. auf [www.vorratsdatenspeicherung.de](http://www.vorratsdatenspeicherung.de).

<sup>14</sup> Eckhardt, CR 2007, 405 (406).

### **3. Nach BayDSG**

Ähnliche Vorschriften wie im BDSG finden sich auch in Art. 6 und 7 BayDSG, betreffen jedoch nach Art. 1 BayDSG nur die Datenverarbeitung durch öffentliche Stellen.

## **III. Strafrecht und Datensicherheit**

### **1. Vorschriften zum Schutz**

#### **a.) § 206 StGB**

Auffälligste Vorschrift in dieser Kategorie ist der § 206 StGB. Er soll denjenigen bestrafen, der Tatsachen, die dem Post- oder Fernmeldegeheimnis unterliegen, weiterverbreitet. Diese Vorschrift dient zur Absicherung des § 88 TKG (s.o.), hat jedoch mehrere Einschränkungen: Zum einen betrifft die Vorschrift nur die Weitergabe an Dritte, während § 88 TKG das Speichern an sich außerhalb seiner Rahmenbedingungen verbietet. Ein TK-Anbieter, der mehr speichert, als es § 88 TKG erlaubt, fällt also nicht unter § 206 StGB.

Auch beschränkt sich § 206 StGB auf geschäftsmäßige Erbringung der Dienste. Dies schließt zwar kostenlose Dienste ohne Gewinnerzielungsabsicht nicht aus, jedoch muss die Erbringung gewisse unternehmerische Züge tragen, d.h. auf eine gewisse Dauer angelegt sein und eine organisatorische Struktur aufweisen.<sup>15</sup> Damit steht es im Unterschied zu § 88 TKG, das alle privaten Dienstleister, ohne Rücksicht auf deren Status, verpflichtet.

Täter der Vorschrift des § 206 StGB kann nur Inhaber oder Beschäftigter des o.g. Unternehmens sein. Diese Einschränkung rechtfertigt sich dadurch, dass Personen, die solche Daten ausspionieren, ohne beruflich damit zu tun zu haben, sich bereits nach § 202 a StGB strafbar machen.

#### **b.) § 202 a StGB**

§ 202 a StGB schützt das „elektronische Hausrecht“, stellt also „elektronischen Hausfriedensbruch“ unter Strafe.<sup>16</sup> Nach der Neuregelung vom 11.08.2007 bestraft diese Norm nicht nur die bereits vorher strafbare Handlung des Verschaffens von Daten, sondern bereits das Verschaffens des Zugangs zu selbigen an sich. Damit ist

---

<sup>15</sup> Schönke/Schröder-Lenckner, § 206 Rn. 8.

<sup>16</sup> Ernst, Hacker, Cracker & Computerviren, Rn. 228.

auch das bloße „Hacking“, d.h. das Verschaffen des Zugangs ohne Absicht zur Datenauslese, strafbar.<sup>17</sup>

Eingeschränkt wird diese weite Auslegung allein durch Einfügen des Tatbestandsmerkmals der „Überwindung der Zugangssicherung“, was keine wirkliche Einschränkung bedeutet, da die wenigsten Systeme komplett ohne jegliche Zugangssicherungen auskommen werden. Dies ist insoweit problematisch, als es zur Kriminalisierung von Handlungen kommt, die keinerlei Rechtsgutsverletzungsabsicht umfassen. Insoweit wird § 202 a unten bei 2. nochmal zu behandeln sein.

#### c.) § 202 b StGB

§ 202 b StGB ergänzt den vorher genannten § 202 a StGB insoweit, dass es das Abfangen von nicht für den Täter bestimmten Daten für strafbar erklärt. Dazu muss keine Zugangssicherung vorhanden sein (sonst wäre § 202 a StGB einschlägig), es geht allen um die Widmung der Daten durch den Übermittler.<sup>18</sup>

Dieser neu eingeführte Straftatbestand hat hauptsächlich den Schutz von E-Mails im Sinn, deren Abfangen damit unter Strafe gestellt werden soll.

Nicht unter § 202 b StGB fallen die Fälle des sog. „Phishing“, d.h. das sich Verschaffen von Zugangsdaten mittels Erschleichen, da in diesem Fall das Opfer die Daten bewusst an den Täter abgibt, welcher nur über seine Eigenschaft (z.B. als Bankinstitut des Opfers) täuscht.<sup>19</sup>

#### d.) §§ 89, 148 TKG

Nach §§ 89, 148 TKG war bereits das Abhören von Funkverkehr, der nicht für einen selbst oder die Allgemeinheit bestimmt war, unter Strafe gestellt. Danach war also auch das Abhören unverschlüsselter WLAN-Verbindungen bereits unter Strafe gestellt, so dass § 202 b StGB in diesem Fall keine Änderung bewirkt. Jedoch ist anzunehmen, dass diese Strafvorschrift den meisten Ermittlungsbehörden nicht bekannt war.<sup>20</sup>

#### e.) § 202 c StGB

Der am meisten umstrittene Paragraph, der durch die Neuregelungen eingeführt wurde, ist wohl § 202 c StGB. Er stellt das „Vorbereiten des Ausspähens und Abfangens von Daten“ unter Strafe.

---

<sup>17</sup> Ernst, NJW 2007, 2661.

<sup>18</sup> Ernst, NJW 2007, 2662.

<sup>19</sup> Marberth-Kubicki, ITBR 2008, 17.

<sup>20</sup> Ernst, NJW 2007, 2662.

Was harmlos klingt, hat im Endeffekt gravierende Auswirkungen: § 202 c StGB nimmt Bezug auf die Handlungen der §§ 202 a und 202 b StGB. Keine der beiden Vorschriften kennt die Strafbarkeit des Versuchs, jedoch stellt § 202 c StGB die Vorbereitungshandlungen zu selbigen unter Strafe. Existiert keine Versuchsstrafbarkeit, kann es aber erst recht keine Strafbarkeit der Vorbereitung geben. Somit ist § 202 c StGB eigentlich ein abstraktes Gefährdungsdelikt.<sup>21</sup>

Ziel dieser neuen Norm soll es vor allem sein, das Herstellen und Sich-Verschaffen sog. „Hacker-Tools“ zu bestrafen.

Unter § 202 c I Nr. 1 StGB fällt wohl in erster Linie das sog. „Phishing“.<sup>22</sup> Damit ist ein Vorgehen gemeint, welches in erster Linie dazu dienen soll, Passwörter und Benutzernamen des Opfers zu erlangen, indem man es darüber täuscht, wem es die Daten anvertraut.

Nicht unter § 202 c I Nr. 1 fällt jedoch das Publizieren von Sicherheitslücken in fremden Systemen.<sup>23</sup> Dies wird jedoch von § 202 a StGB erfasst, da zur Erlangung dieser Informationen in der Regel eine Zugangsüberwindung begangen werden muss.

§ 202 c I Nr. 2 StGB bestraft das Herstellen oder Sich-Verschaffen sog. „Hacker-Tools“, also Programme, mit deren Hilfe sich Zugangsdaten oder andere Daten herausfinden lassen. Darunter fallen (wie unten unter 2. noch zu sehen) auch solche Programme, die sog. „Dual Use“ erlauben, also auch für legale Zwecke eingesetzt werden können.

Subjektiv muss der Vorsatz für § 202 c StGB auch umfassen, dass der Täter eine nach §§ 202 a, 202 b, 303 a oder 303 b StGB strafbare Tat vorbereiten will (unwichtig ist, ob er diese auch begehen wird).<sup>24</sup> Ein solcher Vorsatz dürfte in den meisten Fällen jedoch nicht zu beweisen sein, was eine Strafbarkeit nach § 202 c StGB schwer verwirklichen lässt.

#### f.) §§ 303 a, 303 b StGB

Wenn § 202 a StGB das digitale Äquivalent zum Hausfriedensbruch ist, dann ist § 303 a StGB das zur Sachbeschädigung. Die Norm bestraft all jene, die Daten nach § 202 a StGB löscht, unterdrückt, unbrauchbar macht oder verändert, also auch etwas hinzufügt. § 303 b StGB stellt eine Qualifikation zu § 303 a StGB bzw. eine Weiterführung des § 202 a StGB. So ist nach Abs. 1 derjenige zu bestrafen, der eine Datenverarbeitung von

---

<sup>21</sup> Schulz, MIR 2006, Dok. 180, Rz. 27; Ernst, NJW 2007, 2663.

<sup>22</sup> Schulz, MIR 2006, Dok. 180, Rz. 26.

<sup>23</sup> Ernst, NJW 2007, 2663.

<sup>24</sup> Ernst, NJW 2007, 2664.

erheblicher Bedeutung dadurch stört, dass er Daten verändert/zerstört nach § 303 a StGB oder solche aus § 202 a StGB eingibt oder sonst wie destruktiv eingreift. Unklar ist, was unter einer erheblichen Bedeutung zu verstehen sein. So wird die Dissertation eines Doktoranden auf dessen Laptop sicherlich darunter fallen, aber ob eine Arbeit wie die hier vorliegende Seminararbeit hierunter zu fassen ist, ist schon nicht mehr sicher. Desgleichen gilt für private Hobbies wie Private-E-Mail-Kommunikation oder Speicherstände eines Spielers. All das lässt sich als „zentrale Funktion für die Lebensgestaltung der Privatperson“<sup>25</sup> ansehen. Inwiefern in diesen Fällen die Datenverarbeitung durch § 303 b StGB geschützt ist, wird erst noch zu klären sein.<sup>26</sup>

Absatz 2 war vor der Neuregelung Absatz 1 der Norm und stellt nun eine Qualifizierung des Grundtatbestands dar. Sie betrifft solche Datenverarbeitungsvorgänge, bei denen das Opfer ein Unternehmen, ein Betrieb oder eine Behörde ist.

Absatz 4 regelt besonders schwere Fälle, wie z.B. großen Vermögensschaden oder bandenmäßige Begehung.

Anders als bei §§ 202 a ff. StGB, ist bei §§ 303 a und 303 b StGB der Versuch strafbar.

## **2. Vorschriften gegen Schutz**

### **a.) § 202 a StGB**

Ogleich § 202 a StGB eigentlich den Schutz privater Daten im Sinn hat, führt die aktuelle Fassung, basierend auf der Neuregelung vom 11.08.2007, auch dazu, dass der Schutz von Computersystemen indirekt verschlechtert wird.

In der Computergeschichte waren „Hacker“ (oder auch „White Hat“-Hacker) eigentlich eine Gruppe Individuen, die, anders als ihr Ruf, nicht den Schaden von anderen im Sinn hatten. Vielmehr sind es Personen, die sich, aus Zeitvertreib oder um ihre Fähigkeiten zu erweitern, bemüht haben, u.a. Fehler in Programmen und Computersystemen zu finden und die theoretische Ausnutzbarkeit zu dokumentieren. Anders als sog. „Cracker“ ist es ihr Ziel hierbei jedoch nicht, diese auszunutzen, sondern allein eine Art „sportlicher“ Beweis ihres Könnens.<sup>27</sup> Dieses „Hacking“ im traditionellen Sinn erfolgte fast immer mit der Bekanntmachung der Sicherheitslücke gegenüber dem Betreiber bzw. Hersteller oder, seltener, gegenüber der Öffentlichkeit z.B. im Usenet oder im World Wide Web.

---

<sup>25</sup> Begründung zu § 303 b StGB-E, BT-Drucksache 16/3656, sub 1 a.

<sup>26</sup> Ernst, NJW 2007, 2665.

<sup>27</sup> Ernst, (Fn. 16): Pierrot, Rn. 11.

Dadurch konnten Sicherheitslücken entdeckt werden, ohne dass Schaden entstehen musste. Dementsprechend war das bloße Zugangverschaffen ohne Absicht zur Datenauslese bisher auch absichtlich straflos gehalten gewesen.<sup>28</sup> Die aktuelle Fassung führt zu einer unnötigen Kriminalisierung jener, die keine schlechten Absichten hegten, während sog. „Cracker“ auch bisher sich nicht mit dem Eindringen in ein fremdes System zufrieden gegeben haben und daher durch ihre Absicht zur Manipulation bereits strafbar waren. Durch diese Kriminalisierung ist zu befürchten, dass deutsche „Hacker“ nach dem alten Hacker-Bild sich zurückziehen werden und das Feld jenen überlassen, die allein schlechte Absichten hegen, ihre Angriffe aber i.d.R. aus dem Ausland, d.h. außerhalb der Reichweite des § 202 a StGB, heraus ausführen werden.

#### b.) § 202 c StGB

Auch § 202 c StGB ist als janusköpfig anzusehen. Während in den meisten Fällen bereits eine Strafbarkeit mangels (beweisbaren) Vorsatz ausscheiden sollte, existiert bei § 202 c I Nr. 2 StGB immer noch das Problem der „Dual Use“-Software.<sup>29</sup> Darunter versteht man solche Programme, die sowohl positiv als auch negativ verwendet werden können. Dies ist besonders der Fall bei allen Programmen, die Systemadministratoren verwenden, um ihre Systeme angriffssicher zu machen.

Ebenfalls sehr problematisch ist diese Norm für die IT-Sicherheitsindustrie. Viele Firmen stellen Software her, die dem Schutz von Computersystemen dienen soll, aber im Endeffekt ebenfalls negativ verwendet werden kann.<sup>30</sup> Als einfachste Beispiele seien dabei nur sog. „Portscanner“ und „Passwort-Tools“ genannt:

Ein Portscanner ermöglicht das überprüfen eines Computersystems auf offene Ports, also Adresskomponenten, die zur Unterscheidung von Datenströmen dienen sollen, bei fehlerhafter Absicherung jedoch ungewollte Daten in das System eindringen lassen können. Klar verständlich ist also, dass Täter, die vorhaben, ein System zu knacken, solche Tools einsetzen, um potentielle Einfalltore zu finden. Leider müssen auch Systemadministratoren diese Tools verwenden, um genau solchen Angriffen zuvorkommen zu können und Sicherheitslücken zu entdecken.

Passwort-Tools sind solch Programme, die es erlauben, verlorene Passwörter trotz Verschlüsselung wieder zu finden. Auch diese können natürlich von Nicht-Befugten verwendet werden, um Passwörter herauszufinden, aber auch vom Systemadministrator

---

<sup>28</sup> Amtl. Begründung zu § 202 a StGB, BT-Drucksache 10/5858, S. 4, S. 28; dazu *Ernst*, (Fn. 16), Rn. 232.

<sup>29</sup> Ausführlich: *Cornelius*, CR 2007, 682 ff.

<sup>30</sup> *Cornelius*, CR 2007, 682 f.

zum selben Zweck oder zum Testen, wie sicher sein System gegenüber solchen Tools ist.

Dies führt dazu, dass jeder Systemadministrator durch das Downloaden solcher Tools für diesen (legalen!) Gebrauch bereits den objektiven Tatbestand der neuen Norm des § 202 c I Nr. 2 StGB erfüllt und nur über den subjektive Tatbestand noch vor Strafbarkeit geschützt wird. Diese Folge ist zu Recht als unerfreulich zu charakterisieren.<sup>31</sup>

Ebenfalls hat es zur Folge, dass IT-Firmen in Unsicherheit leben, ob und inwiefern, sie sich strafbar machen, wenn sie ihre Produkte anbieten. Dies kann zur Folge haben, dass diese Firmen sich entschließen, aus Deutschland aus zu wandern oder ihre Produkte hier nicht mehr zu verbreiten, was mittelbar wieder der Sicherheit der Computersysteme schaden kann.

#### c.) §§ 100 a ff. StPO

Die §§ 100 a ff. StPO regeln die Telekommunikationsüberwachung. Traditionell wird hierunter die Telefonüberwachung, d.h. das Mithören von Gesprächen Verdächtiger durch die Ermittlungsbehörden verstanden.<sup>32</sup> Die aktuelle Formulierung „Telekommunikation“ erlaubt jedoch das Heranziehen der Legaldefinition in § 3 Nr. 17 TKG. Danach ist Telekommunikation *der technische Vorgang des Aussendens, Übermittels und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen. Letztere sind technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können.*

Unter diese Definition lassen sich also auch leicht Daten fassen, die z.B. per E-Mail oder FTP an einen anderen übertragen werden. § 100 b III StPO bestimmt, dass jeder, der (nach § 88 TKG) geschäftsmäßig TK-Dienste anbietet, also zum Beispiel Internet Service Provider, E-Mail Provider, Web-Hoster etc., dem Richter, der Staatsanwaltschaft und der Polizei gegenüber im in § 88 TKG spezifizierten Umfang die Telekommunikation des Betroffenen überwachen und aufzeichnen muss. Dies führt dazu, dass ein Schutz der persönlichen Daten, die über die beschriebenen Wege vermittelt werden, nicht mehr gegeben ist. Zwar kann die Überwachung nur unter bestimmten, in § 100 a II StPO normierten, Fällen angeordnet werden; jedoch ist keine unverschlüsselte Kommunikation mehr sicher, sobald es einmal angeordnet wurde. Eine

---

<sup>31</sup> Ernst, NJW 2007, 2663.

<sup>32</sup> Löwe/Rosenberg-Schäfer, § 100 a Rn. 27.

einmal angeordnete Überwachung kann jedoch zum Einfallstor für Dritte werden, insbesondere, wenn spezielle Programme zur Überwachung benutzt werden, die z.B. bestimmte Ports verwenden. Auch kann der Betroffene, sollte er die Überwachung ahnen, versuchen, Schadprogramme zu senden, die im schlimmsten Fall dem Diensteanbieter und den Ermittlungsbehörden schaden.

Die Vorschriften führen auch dazu, selbst wenn sie der inneren Sicherheit dienen sollen, dass immer mehr Benutzer ihre Daten verschlüsseln, um sie dem Zugriff des Staates, aber auch unbefugter Dritter, zu entziehen. Dies ist natürlich kontraproduktiv, da ein besserer Schutz von Daten nur durch Verschlechterung staatlicher Zugriffsmechanismen erzielt werden kann.

#### **IV. Geplante Maßnahmen: Die Online-Durchsuchung**

##### **1. Aktuelle Gesetzeslage im Bund**

Ursprung der Diskussion ist der Beschluss des Ermittlungsrichters am Bundesgerichtshofs, der es ablehnte, die, vom Generalbundesanwalt geforderte, heimliche Durchsicht der persönlichen Daten eines Verdächtigen mit Hilfe eines speziell dafür entwickelten Spionageprogramms zu gestatten.<sup>33</sup> Die vom Generalbundesanwalt hiergegen eingebrachte Beschwerde hat der BGH mit Beschluss verworfen<sup>34</sup> und argumentiert, dass es keinerlei Ermächtigungsgrundlage für eine solche Maßnahme gäbe. Vor allem der vom Generalbundesanwalt angeführte § 102 StPO sei für diese Art der Spionage nicht als Ermächtigungsgrundlage tauglich, da er das Bild einer für den Beschuldigten erkennbaren Durchsuchung im Blickfeld hat. Aus §§ 105 II, 106 I StPO folgt demnach, dass ein Gericht keine solche Durchsuchung anordnen darf, die von vorne herein darauf abzielt, heimlich durchgeführt zu werden.

Ebenfalls nicht einschlägig sei die Norm des § 100 a StPO (s.o.), die nur den Zugriff auf Kommunikation erlaube. Wesen der Online-Durchsuchung sei es jedoch aber, auf Daten zuzugreifen, die man gerade nicht durch Kommunikationsüberwachung erhalten konnte.<sup>35</sup>

Nach Ansicht des Bundesgerichtshof existiert daher keine legale Möglichkeit zum Einsatz einer solchen verdeckten Online-Durchsuchung privater PCs.

---

<sup>33</sup> BGH, Beschl. v. 25.11.2006 - 1 BGs 184/2006.

<sup>34</sup> BGH, Beschl. v. 31.1.2007 - StB 18/06.

<sup>35</sup> *Leipold*, NJW-Spezial, 2007, 135 (136).

## 2. Gesetze zur Online-Durchsuchung

Als bisher einziges Land hat Nordrhein-Westfalen (Bayern will hier schnellstmöglich nachziehen<sup>36</sup>) bisher in seinem Verfassungsschutzgesetz (§ 5 Abs. 2 Nr. 11 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen) die sog. „Online-Durchsuchung“ als Maßnahme für Nachrichtendienste erlaubt.

Gegen dieses Gesetz ist eine Verfassungsbeschwerde unter anderem vom ehemaligen Bundesinnenminister Gerhart Baum (FDP) beim Bundesverfassungsgericht anhängig.<sup>37</sup> Eine Entscheidung hierüber wird im Frühjahr 2008 erwartet.<sup>38</sup>

## 3. Politische Positionen

### aa.) CDU / CSU

Klare Vorstellungen von der Umsetzung von Online-Durchsuchungen hat die CDU/CSU. Die Unionsparteien und vor allem Bundesinnenminister Wolfgang Schäuble (CDU) drängen mit allen Mitteln darauf, dass möglichst bald eine gesetzliche Regelung zur Online-Durchsuchung fällt.

Schäuble will vor allem im BKA-Gesetz diese Möglichkeit verankern und drängt darauf, dies möglichst schnell und umfassend zu erlauben.

Die CSU in Bayern will dies auch vor einer Entscheidung des Bundesverfassungsgerichts zum NRW-Verfassungsschutzgesetz in einem Landesgesetz regeln.<sup>39</sup>

### bb.) SPD

In den Reihen der Sozialdemokraten sind die Positionen nicht so klar. Vor allem Bundesjustizministerin Brigitte Zypries warnt vor überhasteten Entscheidungen und will zumindest eine Diskussion hierüber und die Entscheidung des Bundesverfassungsgerichts abwarten.<sup>40</sup>

Andere Stimmen in der SPD, vor allem der Sprecher des Innenausschusses, Dieter Wiefelspütz, haben dagegen, mit Hinweis auf die Koalitionstreue der SPD darauf verwiesen, dass die Partei eine solche Regelung auf jeden Fall mittragen werde, jedoch

---

<sup>36</sup> Tagesschau vom 19.01.2008: <http://www.tagesschau.de/inland/onlinedurchsuchung18.html> (Link geprüft am 22.1.08).

<sup>37</sup> Heise Online: „Heimliche Online-Durchsuchung beschäftigt Karlsruhe“; <http://www.heise.de/newsticker/meldung/93440> (Link geprüft am 22.1.08).

<sup>38</sup> Heise Online: „Viel Skepsis in Karlsruhe gegenüber verdeckten Online-Durchsuchungen“; <http://www.heise.de/newsticker/meldung/97212> (Link geprüft am 22.1.08).

<sup>39</sup> Siehe Fn. 36.

<sup>40</sup> *Leipold*, NJW-Spezial, 2007, 135 (136).

erst nach dem Urteil des Bundesverfassungsgerichts zum NRW-Verfassungsschutzgesetz, in dem Ausführungen zu den Grenzen solcher Maßnahmen erwartet werden.<sup>41</sup> Ebenso fällt die Reaktion der BayernSPD auf das von Staatsminister Herrmann geplante Gesetz zur Online-Durchsuchung auf Landesebene aus, auch hier gibt es nur Kritik am Versuch des bayerischen Sonderwegs, die Möglichkeit einer Einführung nach einer Entscheidung des BVerfG wird aber nicht in Frage gestellt.<sup>42</sup>

Anders die Stellungnahme in Nordrhein-Westfalen, wo die Landes-SPD sich klar gegen die bereits bestehende Regelung ausspricht und deren Abschaffung fordert.<sup>43</sup>

#### cc.) FDP

Die zur Zeit größte Oppositionspartei im Bundestag, die FDP, schließt die Einführung dieser Möglichkeit als Eingriff in die Grundrechte der Bürger kategorisch aus.<sup>44</sup> In Nordrhein-Westfalen, wo sie eine Koalitionsregierung mit der CDU bildet, hat sie einer solchen Regelung jedoch zugestimmt.

#### dd.) Bündnis 90 / Die Grünen

Klare Stellungnahmen zu diesem Thema sind von den Grünen nicht zu finden, Pressemitteilungen zum Verfahren vor dem BVerfG und zum geplanten neuen BKA-Gesetz lassen jedoch auf eine Ablehnung dieser Möglichkeit schließen.<sup>45</sup>

#### ee.) Die Linke

Die Linke hat sich klar gegen jegliche Online-Durchsuchungen ausgesprochen.<sup>46</sup>

### **4. Technische Grundlagen**

#### a.) Funktionsweise

Grundlage der Beschreibung der Funktionsweise ist die Annahme, dass die Maßnahme nur in einer geringen Zahl von Fällen angewandt wird. Nach allen Aussagen von Befürwortern dieser Möglichkeit soll die offiziell „Remote Forensic Software“

---

<sup>41</sup> Heise Online: „SPD: Entscheidung für Online-Durchsuchung ist gefallen“; <http://www.heise.de/newsticker/meldung/102027> (Link geprüft am 22.1.08).

<sup>42</sup> <http://www.bayernspd-landtag.de/aktuell/details.cfm?ID=10130&nav=aktuell> (Link geprüft am 22.1.08).

<sup>43</sup> NRW-LT-Drucksache 14/4246.

<sup>44</sup> So z.B. in „Liberale Argumente“ vom 18./21. September 2007:

<http://fdp.de/files/540/07-09-21-18-Online-Ueberwachung.pdf> (Link geprüft am 22.1.08).

<sup>45</sup> [http://www.gruene-bundestag.de/cms/presse/dok/200/200984.schaeuble\\_hoer\\_die\\_signale.html](http://www.gruene-bundestag.de/cms/presse/dok/200/200984.schaeuble_hoer_die_signale.html) (Link geprüft am 22.1.08).

<sup>46</sup> [http://www.die-linke.de/index.php?id=251&tx\\_ttnews\[tt\\_news\]=726](http://www.die-linke.de/index.php?id=251&tx_ttnews[tt_news]=726) (Link geprüft am 22.1.08).

getaufte<sup>47</sup>, in der Umgangssprache aber als „Bundestrojaner“ bekannte, Software für jeden Einsatz speziell auf das System des Verdächtigen angepasst bzw. neu programmiert werden.

Funktionieren soll der „Bundestrojaner“ wie der Name schon sagt wie ein sog. „Trojanisches Pferd“. Trojanische Pferde sind Programme, die sich im System einnisten und dort Daten ausspionieren, Tasteneingaben protokollieren und/oder Manipulationen ermöglichen.

So soll es, vom Opfer unbemerkt, möglich sein, dessen Daten nach Hinweisen zu durchsuchen oder seine Passwörter auszulesen, die eine Entschlüsselung gespeicherter Daten möglich machen können.<sup>48</sup>

### b.) Installation

Für die Installation eines trojanischen Pferdes am Rechner des Verdächtigen bzw. jedes Opfers eines solchen Angriffs eignen sich mehrere Möglichkeiten:<sup>49</sup>

- Versand einer E-Mail mit Dateianhang, möglicherweise getarnt als von einer anderen Behörde kommend
- Ausnutzen von Sicherheitslücken („Cracking“) und Installation über das Internet
- „Drive-by-Download“ unter Ausnutzen von Sicherheitslücken der Browser- oder Betriebssystem-Software<sup>50</sup>
- Verstecken der Software im Datenstrom der vom ISP zum Opfer versandt wird
- Manuelle Installation vor Ort (Eindringen in die Wohnung und Installation am PC des Verdächtigen)

Alle diese Maßnahmen stehen mehr oder weniger auch einem Viren-Benutzer zur Verfügung, weshalb viele Computerkundige solche Angriffe auch abwehren bzw. entdecken können.

## **5. Technische und sicherheitsbezogene Probleme**

### a.) Firewalls

Eine gute „Firewall“, die eigentlich jeder halbwegs computererfahrene Benutzer installiert haben dürfte, kann die vom Trojaner nach außen versandte Kommunikation

---

<sup>47</sup> Antwortschreiben des Bundesministerium des Inneren auf eine Anfrage der SPD-Bundestagsfraktion: (Link geprüft am 22.1.08)

<http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf>.

<sup>48</sup> *Leipold*, NJW-Spezial, 2007, 135.

<sup>49</sup> *Gercke*, CR 2007, 245 (248).

<sup>50</sup> *Leipold*, NJW-Spezial, 2007, 135.

erkennen und blockieren. Die Software könnte somit Daten sammeln, diese aber nicht nach außen kommunizieren.<sup>51</sup>

Umgehen ließe sich dies dadurch, indem der Schädling so genau auf das Opfer eingestellt ist, dass die verwendete Firewall und etwaige Schwachstellen bekannt sind und ausgenutzt werden können. Inwiefern diese Informationen zu bekommen sind, ist jedoch unklar.

#### b.) Router

Viele Internetbenutzer, vor allem mit mehreren Geräten oder Mitbenutzern, verwenden zur gemeinsamen Benutzung eines Zugangs einen sog. „Router“. Dies sind Geräte, die Datenströme je nachdem wer sie angefordert hat, an verschiedene Rechner weiterleiten. Vom Internet aus ist jedoch keiner dieser Computer, sondern nur der Router erkennbar. Dies erschwert nicht nur die Unterscheidung, von wem genau eigentlich die Daten stammen, die man auslesen wollte, sondern dürfte im Regelfall, durch eingebaute Firewall und sog. „Network Address Translation“ (NAT)<sup>52</sup>, unmöglich zu aktivieren sein.<sup>53</sup>

Umgehen ließe sich dies, wie bei einer lokal installierten Firewall, maximal durch Kenntnis des Routers und durch spezifische Schwächen des selbigen (überschreibbare Firmware, manipulierbare Sicherheitslücken), die eine Installation des Schädlings auf dem Router zulassen, von wo er sich dann auf den Computer überträgt. Die Möglichkeit der Kenntnis und/oder die Existenz solcher Zustände dürfte aber gering sein.

#### c.) Anti-Viren-Software

Ein trojanisches Pferd ist in erster Linie auch immer ein Virus. Dabei macht es keinen Unterschied, von wem dieser Virus stammt, denn auch die RFS offenbart virusartiges Verhalten und solche Viren werden früher oder später von Anti-Viren-Scannern erkannt und meist auch vernichtet. Verwendet der Betroffene also eine solche Software mit heuristischer Erkennung<sup>54</sup>, was heutzutage normal sein dürfte, dann kann diese den Bundestrojaner über früher oder später wohl erkennen und beseitigen. Wird zur Herstellung des Selbigen immer ein bestimmtes Schema verwendet, so kann dies auch als Signatur für die Anti-Viren-Software verwendet werden.

---

<sup>51</sup> Leipold, NJW-Spezial, 2007, 135.

<sup>52</sup> Eine Erklärung findet sich auf <http://de.wikipedia.org/wiki/NAPT> (Stand vom 13. Jan. 2008, 03:51 Uhr).

<sup>53</sup> Leipold, NJW-Spezial, 2007, 135.

<sup>54</sup> Heuristische Erkennung bedeutet, dass das Programm nicht nur Viren anhand bestimmte Merkmale, sog. „Signaturen“, erkennt, sondern auch schädliches Verhalten, dass von nicht bekannten Programmen ausgeführt wird.

Wie dies umgangen werden soll, ist fraglich. Etwaige vom „Bundestrojaner“ verwendete Sicherheitslücken solcher Software müssten, weil sie auch von Viren verwendet werden könnten, vom Hersteller beseitigt werden.<sup>55</sup>

Der Vorschlag einiger Politiker, in Deutschland verkaufte Software solle ein „BKA-Hintertor“ haben, ist nicht realisierbar:

- Jede für das RFS geschaffene Hintertür würde früher oder später bekannt werden und dann von Virenprogrammierern ausgenutzt werden
- Kein Unternehmen wird Software in Deutschland kaufen, die ganz offensichtlich Sicherheitslücken aufweist.<sup>56</sup> Dies führt entweder dazu, dass diese Unternehmen Software ausländischer Firmen kaufen, keinerlei Software einsetzen (was die Daten ihrer Kunden gefährden würde, s.o.) oder, im schlimmsten Fall, das Land verlassen um weiterhin Datensicherheit gewährleisten zu können
- Führende Anti-Viren-Hersteller haben bereits angekündigt, dass sie eine solche Hintertür nicht einbauen würden. Auf im Ausland sitzende Unternehmen hat der deutsche Staat keinen Einfluss, weshalb eine solche Pflicht maximal die Insolvenz deutscher Anbieter zur Folge hätte

#### d.) Betriebssystem

Während zwar 90% der Deutschen das für seine Sicherheitslücken bekannte Betriebssystem Microsoft Windows verwenden, kann nicht garantiert werden, dass diese Systemarchitektur auch beim Opfer vorhanden sein wird. Vor allem computererfahrene Kriminelle werden für ihre Tätigkeit eines der weniger anfälligen Betriebssysteme der \*NIX-Bauweise (wie Linux, BSD etc.) einsetzen, für das die Anstrengungen, Sicherheitslücken zu finden oder Viren zu schreiben viel höher sind. Eine Möglichkeit zur Einwirkung auf diese OpenSource-Betriebssysteme, Hintertüren bereit zu halten, wird nicht vorhanden sein.

#### e.) Read-Only Systeme

Ein leichtes ist es auch, den für die Kommunikation mit dem Internet bestimmten PC als Read-Only zu konfigurieren. Dabei wird das Betriebssystem entweder von CD/DVD gestartet oder ein Abbild des Systems erstellt, das bei jedem Neustart wieder überschrieben wird. Dadurch ist jede Installation eines trojanischen Pferdes nur temporär und spätestens im nächsten Systemneustart vernichtet. Zur

---

<sup>55</sup> *Leipold*, NJW-Spezial, 2007, 135.

<sup>56</sup> *Gercke*, CR 2007, 245 (249).

Datenaufbewahrung kann dann eine voll-verschlüsselte externe Festplatte dienen, deren Inhalt man nur nach Trennen des Netzkabels ausliest.

#### f.) Steganographie

Unter „Steganographie“ versteht man die Möglichkeit, Daten nicht nur zu verschlüsseln, sondern in simplen Bild-Dateien zu verstecken. Dabei werden Übergänge zwischen hellen und dunklen Bereichen zum Verstecken der Daten verwendet. Der Absender sendet dann den Hinweis, ab welchem Pixel zu suchen ist, auf andere Weise dem Empfänger. Eine solches Verbergen wird von einem Trojaner nicht erkennbar sein, da sie auch für den normalen, nicht eingeweihten, nicht erkennbar ist.

#### g.) Entdeckung und Fehlinformation

Klar bei solchen Fällen möglich ist, dass der Betroffene die Überwachung bemerkt und sich dies zu Nutze macht, indem er dem Überwacher falsche Informationen schickt und damit von seinen wahren Plänen ablenkt.

#### h.) Sicherheitslücken durch Disassembling

Nach dem ersten Einsatz solcher Technologie wird es recht bald dazu kommen, dass einer der Überwachten die RFS bemerkt und selbst oder durch Dritte den Bundestrojaner disassembled, d.h. das kompilierte Programm wieder in seinen Quellcode zurückverwandelt.<sup>57</sup> Dadurch ist der Besitzer des Quellcodes dann in der Lage, die Funktionsweise des Programms zu studieren und sich zu nutze zu machen (z.B. um Sicherheitslücken zu entdecken, die Systeme des BKA zu kompromittieren, andere Systeme zu infizieren etc.).<sup>58</sup>

## **6. Rechtliche Probleme**

### a.) Internationalität

Selten finden sich Täter wirklich nur in Deutschland. Aber bereits an der Bundesgrenze ist die Grenze des deutschen Rechts erreicht. Der potentielle Täter braucht also nur in ein Nachbarland auszuweichen und kann immer noch in Deutschland Straftaten begehen, die deutsche Justiz kann ihn aber nicht mit einer solchen Maßnahme belegen, ohne internationale Konflikte zu befürchten.<sup>59</sup>

---

<sup>57</sup> Oder diesen von einem der Programmierer der RFS abkauft. Solche Software sollte, vor allem wenn sie mehrfach-anwendbar ist, eine für Kriminelle lohnenswerte Investition sein.

<sup>58</sup> Gliss, DSB 2007, 15.

<sup>59</sup> Gliss, DSB 2007, 15.

## b.) Art. 13 GG

Ein wie auch immer gearteter Bundestrojaner dürfte unter Art. 13 GG fallen und demnach, selbst bei Nichtbefinden des Computers in der Wohnung, den Schranken des Grundrechts unterliegen.<sup>60</sup> Danach fallen bestimmte Gegenstände bei einer Wohnungsdurchsuchung unter eine Unverletzlichkeit, wie zum Beispiel Tagebücher. Der selbe Schutz muss streng genommen dann auch für denjenigen gelten, der ein Tagebuch auf dem Computer führt.<sup>61</sup>

## c.) Recht auf informationelle Selbstbestimmung

Bereits oben erwähnt wurde das aus Art. 1 i.V.m. Art. 2 GG gefolgerte Recht auf informationelle Selbstbestimmung. Dieses ist durch die Kombination von Merkmalen von Art. 1 GG und Art. 2 GG teilweise einschränkbar, vorausgesetzt es wird der Kernbereich der Privatsphäre und die Verhältnismäßigkeit gewahrt.

### aa.) Kernbereich der Privatsphäre

Im Urteil zum großen Lauschangriff hat das Bundesverfassungsgericht erkannt, dass es Bereiche gibt, die absolut geschützt sind.<sup>62</sup> Das Problem, wie mit diesem „Kernbereich der Privatsphäre“ umgegangen werden soll, ist ungelöst.<sup>63</sup> Faktisch verbietet es einer wie auch immer gearteten Software, Daten auszulesen und zu übertragen, die diesem Bereich zuzuordnen sind.<sup>64</sup> Jedoch dürfte es nicht möglich sein, eine Software zu programmieren, die eine solche Unterscheidung von selbst treffen kann.<sup>65</sup>

### bb.) Verhältnismäßigkeit

Jedes staatliche Handeln muss verhältnismäßig sein. Die Frage stellt sich also bei Erforderlichkeit, Geeignetheit und Milde des Mittels.

Über die Erforderlichkeit lässt sich streiten, wird aber wohl zu bejahen sein, wenn es um Fälle der Schwer- und Schwerstkriminalität geht.

Schwieriger ist es schon mit der Geeignetheit, existieren doch (s.o.) eine Reihe von Möglichkeiten, das Mittel leer laufen zu lassen. Bei Einführung einer solchen Maßnahme dürfte die Zahl derer, die solche Möglichkeiten wahrnehmen, drastisch steigen und die Geeignetheit des Mittels sehr verringern.

---

<sup>60</sup> *Kutscha*, NJW 2007, 1169 (1170).

<sup>61</sup> *Kutscha*, NJW 2007, 1169 (1171).

<sup>62</sup> BVerfGE 109, 278 (357).

<sup>63</sup> *Kutscha*, NJW 2007, 1169 (1171).

<sup>64</sup> *Tinnefeld*, MMR 2007, 137 (138).

<sup>65</sup> *Gercke*, CR 2007, 245 (249).

Milder als die Online-Durchsuchung wäre eigentlich eine Hausdurchsuchung nach § 102 StPO, bei der die Daten physikalisch in Form von Festplatten ergriffen werden könnten. Eine Online-Durchsuchung würde nicht nur die Daten des Betroffenen in die Hände des Staates bringen, sondern auch alle von ihm gespeicherten Daten über unbescholtene Dritte.<sup>66</sup>

#### d.) Gefahr der Ausweitung

Oftmals wird gewarnt, dass die Schaffung einer solchen Maßnahme für bestimmte, begrenzte Straftaten dazu führen wird, dass diese Hürden mit der Zeit aufgeweicht werden.<sup>67</sup> Dies wird vor allem mit Hinweis auf § 101 a StPO getan, dessen anfangs hohe Hürden nach und nach eingerissen wurden und heute bereits einfacher Tatverdacht für fast alle Verbrechen genügt, um eine Telekommunikationüberwachung zu genehmigen

#### e.) Gefahr der Manipulation

Gar nicht so fern ist die Gefahr der Manipulation: Wer einmal auf einen fremden Rechner zugreifen kann, der kann nicht nur Daten lesen, sondern auch Daten verändern. Damit ist die Gefahr eines unendlichen Missbrauchs geschaffen: Der Staat kann missliebigen Personen, denen er nichts nachweisen kann, einfach etwas unterschieben und dann bei Beschlagnahme des Computers genau darauf verweisen und dies als Beweis verwenden. Ein Nachweis der Manipulation ist fast unmöglich.<sup>68</sup>

#### f.) Gefahr kommerzieller Nutzung

Das Beispiel der Vorratsdatenspeicherung hat es gezeigt: Hat der Staat eine Ermittlungsmöglichkeit, die private Rechteinhaber für sich benutzen könnten, werden diese aktiv. Durch geschickte Lobbyarbeit haben die Platten- und Filmverbände es geschafft, dass die CDU/CSU im Bundesrat eine Ausweitung der Vorratsdatenspeicherung für private Zwecke gefordert hat, nach der Rechteinhaber auf die gespeicherten Daten zugreifen können sollen. Dass eine ähnliche Forderung im Falle der Online-Durchsuchung erhoben wird, dürfte nach deren Einführung nur eine Frage der Zeit sein.

---

<sup>66</sup> Kutscha, NJW 2007, 1169 (1172).

<sup>67</sup> Leipold, NJW-Spezial, 2007, 135 (136).

<sup>68</sup> Prantl, SZ v. 7.9.07; (Link geprüft am 22.1.08)

<http://www.sueddeutsche.de/deutschland/artikel/955/131720/>.

### g.) Schadensersatzforderungen gegen den Staat

Schon der bayerische Datenschutzbeauftragte Karl Michael Betzl warnt davor, dass im Falle der Beschädigung eines EDV-Systems durch den Staat im Zuge der Online-Durchsuchung der Staat Schadensersatz gegenüber dem geschädigten Unternehmen zu leisten habe. Auch könnten so Geschäftsgeheimnisse in fremde Hände fallen, die sich den „Bundestrojaner“ zu nutzen machen.<sup>69</sup>

### **V. Fazit**

Bereits bestehende Normen höhlen bereits die gesetzlichen Bestimmungen zum Datenschutz aus. Für Firmen stellt sich das Problem, Daten ihrer Kunden oder eigene Daten schützen zu müssen und gleichzeitig dem Staat unter bestimmten Umständen Zugang zu ermöglichen.

Die diskutierte Online-Durchsuchung fügt daran eine weitere Problematik an: Ist ein Provider z.B. gezwungen, Daten offen zu legen, so kann er dies unter Wahrung seiner Sicherheitssysteme tun.

Soll jedoch ein Einzelner oder ein Unternehmen überwacht werden ohne dass er oder es dies bemerkt, so kann es gut möglich sein, dass der Staat an genau den Sicherheitsmaßnahmen scheitert, die er gesetzlich zur Pflicht gemacht hat oder dass er diese Maßnahmen aushebelt und damit die Datensicherheit anderer gefährdet, wonach diese aber bei Schäden sich gegen den Staat richten dürfen, was dessen Budget wohl nicht vertragen dürfte (z.B. bei Verlust milliardenschwerer Informationen durch durch den Bundestrojaner geschaffener Lücken im System).

---

<sup>69</sup> *Leipold*, NJW-Spezial, 2007, 135.