

## „Internet als Datenfundgrube“

Dr. Ursula Widmer\*, Rechtsanwältin, Dr. Widmer & Partner, Bern

### I. Einleitung

Wenn Internet-Teilnehmer E-Mails verschicken, Beiträge an Newsgroups übermitteln, Websites für die Öffentlichkeit zugänglich machen bzw. aufrufen, Recherchen in Datenbanken vornehmen, Musik- und zunehmend auch Filmdateien kopieren, so handelt es sich in der Sache hierbei zunächst um einen sich täglich ereignenden Transport grosser Mengen von Daten: das Internet und –dienstleistungen ist somit auch eine gigantische „Datenfundgrube“. Die bei der Nutzung des Internet vom User hinterlassene elektronische Spur (auch unter der Bezeichnung „click-stream“ bekannt)<sup>1</sup>, eignet sich etwa hervorragend für Zwecke des Direkt-Marketings oder auch das Erstellen von Marketingstatistiken zur Bestimmung des Nutzerverhaltens eines jeden einzelnen<sup>2</sup>. Es liegt auf der Hand, dass diese Situation datenschutzrechtliche Fragestellungen aufwirft<sup>3</sup>.

Im folgenden sollen mit dem Charakter einer Einführung zur Vorbereitung der weiteren Beiträge des Tagungsbandes die Grundzüge des Datenschutzrechts in der Schweiz anhand von internetspezifischen Beispielen erläutert werden<sup>4</sup>. Zwei vertiefende Abschnitte sind den Rechtsfragen der im Internet naturgemäss besonders relevanten Datenübermittlung ins Ausland unter besonderer Berücksichtigung der EU-Rechtslage<sup>5</sup> sowie der Frage nach den Auskunftspflichten der Internet Service Provider (ISPs) gewidmet, die durch einen aktuellen Entscheid des Bundesgerichtes besondere Aktualität erlangt hat. In diesem Zusammenhang

---

\* Ich danke Herrn Referendar Thorsten Voss für seine umfassende Mitarbeit.

<sup>1</sup> Die Standard-Software eines WWW-Servers protokolliert den Zugriff mit Rechneradresse, Datum, Uhrzeit, Aktion und Zugriffsobjekt. Die Rechneradressen können anschliessend ausgewertet werden, so dass mit der Zeit bei einem Anbieter von Internet-Dienstleistungen und/oder -Produkten ein beträchtlicher Bestand an Daten seiner Websitebesucher und seiner Kunden zusammenkommt.

<sup>2</sup> Beispielsweise sammelte Microsoft in allen Word- und Excel-Dateien sog. GUID-Nummern. Hierunter versteht man eine Seriennummer, den "Globally Unique Identifier" (GUID), die aus der Netzwerkkarte ausgelesen werden kann. Unbemerkt übertrug nun der Musik-Player Realjokebox die GUID mit zahlreichen für Marketingziele nützlichen Informationen wie der Anzahl und der Formate der auf dem Rechner gespeicherten Musiktitel. Weiter ist bekannt geworden, dass Double-Click, eine prominente Internet-Marketingfirma, mit anderen Online-Agenturen einen Austausch von Informationen über User vornimmt. So ist zwischenzeitlich ein Werbenetzwerk entstanden, mit der Folge, dass einem Nutzer bei einem Aufruf mit Double-Click kooperierender Sites – wie z.B. Yahoo und Altavista - das „zu ihm passende“ Werbefbanner präsentiert wird.

<sup>3</sup> Siehe allgemein zum Thema „Datenschutz und Internet“ U. Widmer/K. Bähler, Rechtsfragen beim Electronic Commerce, 2. Aufl. Zürich 2000, S. 239-280; Th. Hoeren/U. Sieber (Hrsg.), Handbuch Multimedia-Recht, München, Loseblatt-Sammlung (Stand: Februar 2000), Teil 16; J.-P. Walter, La protection des données dans le cyberspace, medialex 2000, S. 88-96.

<sup>4</sup> Bei den Ausführungen wurde der Vortragsstil beibehalten. Ein Fussnotenapparat wurde insoweit erstellt, wie er zum Verständnis der gemachten Ausführungen unerlässlich ist.

<sup>5</sup> Zu beachten ist hier die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG 1995 L 281/31 (im folgenden: EU-Datenschutzrichtlinie bzw. EU-Richtlinie). Vgl. hierzu statt vieler M. Weber, EG-Datenschutzrichtlinie. Konsequenzen für die deutsche Datenschutzgesetzgebung, CR 1995, S. 297-303.

wird zudem rechtsvergleichend – nicht zuletzt wegen der engen wirtschaftlichen Verflechtung der beiden Länder – auf die Rechtslage in Deutschland eingegangen.

## II. Datenschutzrecht Schweiz

Zunächst ein Beispielsfall: Eine Segelfluggruppe unterhält eine Website zur Information über ihre Aktivitäten. Dabei hat der Webmaster auch das Mitgliederverzeichnis frei zugänglich auf der Website publiziert. Nun fragen einige Mitglieder an, ob dies datenschutzrechtlich zulässig ist.

Heutzutage verfügen alle Schweizer Kantone über ein Datenschutzgesetz, welches jeweils den Schutz *personenbezogener Daten bzw. der Persönlichkeit* gegenüber den kantonalen Behörden zum Regelungsgegenstand haben<sup>6</sup>. Das Datenschutzgesetz des Bundes (DSG) regelt die Bearbeitung von Daten natürlicher oder juristischer Personen<sup>7</sup> durch Behörden des Bundes und durch Private<sup>8</sup>. Ausgangspunkt der gesetzlichen Bestimmungen (und dementsprechend auch unserer Überlegungen) ist es damit, dass es sich um den Schutz „personenbezogener Daten“, also aller Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen<sup>9</sup>, handelt. Damit geht es im Ergebnis, was in der über weite Strecken eher technisch geprägten Diskussion leider häufig übersehen wird, beim „Datenschutz“ *nicht* um den *Schutz von Daten*, sondern vielmehr um den *Schutz von Personen*<sup>10</sup>.

In den Art. 4-7 DSG werden die allgemeinen Grundsätze der Datenbearbeitung behandelt. Dabei meint das „Bearbeiten von Daten“ jeden Umgang mit Personendaten, unabhängig von

<sup>6</sup> Als Pionier auf diesem Sektor hat sich dabei der Kanton Genf besondere Verdienste erworben, der ein Datenschutzgesetz bereits im Jahr 1976 (sic!) und damit lang vor dem Inkrafttreten des Eidgenössischen DSG von 1993 einführte. Zur Geschichte der Datenschutzgesetzgebung im Ausland siehe *U. Widmer/K. Bähler*, Rechtsfragen beim Electronic Commerce, 2. Aufl. Zürich 2000, S. 245 f. Vielfach sind es im übrigen aktuelle tagespolitische Ereignisse, wie beispielsweise die Fichen-Affäre in der Schweiz oder das Volkszählungsurteil des BVerfG in Deutschland (BVerfGE, 65, 1; hierzu eingehend *B. Holznagel*, Das Grundrecht auf informationelle Selbstbestimmung, <<http://www.uni-muenster.de/Jura.tkr/veranstaltungen/Ringvorlesung.pdf>> [Stand: 25.11.2000]), die der Datenschutzdiskussion in den einzelnen Ländern Auftrieb gegeben haben mit der abschliessenden Folge eines Tätigwerdens des Gesetzgebers.

<sup>7</sup> Die Daten juristischer Personen sind in vielen anderen Ländern, wie etwa in Deutschland, und im übrigen auch durch die EU-Richtlinie, durch die Datenschutzgesetzgebung nicht geschützt.

<sup>8</sup> Art. 2 Abs. 1 DSG.

<sup>9</sup> Vgl. Art. 3 lit. a DSG.

<sup>10</sup> Die personenbezogenen Daten sind abzugrenzen von den sog. „aggregierten Daten“, die nicht als personenbezogen behandelt werden, abgesehen von den Fällen, in denen einer Person eine Angabe zugeordnet werden könnte. Erwähnenswert ist, dass die EU-Datenschutzrichtlinie den Begriff der personenbezogenen Daten sprachlich sehr weit fasst. So heisst es wörtlich: „Im Sinne dieser Richtlinie bezeichnet der Ausdruck a) „personenbezogene Daten“ alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person gesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind; ...“. Damit weist die Richtlinie darauf hin, dass sogar eine indirekte Identifizierbarkeit des Betroffenen eine Qualifizierung der entsprechenden Daten als personenbezogen zur Folge hat. Demgemäss spricht einiges dafür, dass zumindest ein Teil der aggregierten Daten inskünftig in diesem Sinne als personenbezogen zu qualifizieren ist, womit die Bedeutung des Datenschutzes naturgemäss noch weiter zunehmen wird. Vgl. im übrigen zum Verhältnis von Persönlichkeits- und Datenschutz *H. M. Riemer*, Persönlichkeitsrechte und Persönlichkeitsschutz gemäss Art. 28 ff. ZGB im Verhältnis zum Datenschutz-, Immaterialgüter- und Wettbewerbsrecht, sic! 1999, S. 103-105.

den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten<sup>11</sup>. Es kommt für die Bearbeitung von Personendaten im Zusammenhang mit Transaktionen beim E-Commerce entscheidend darauf an, dass diese nach Massgabe der gesetzlichen Vorgaben auch erlaubt ist. Die Bearbeitung von Personendaten führt nämlich dann zu einer nicht erlaubten Verletzung des Persönlichkeitsrechts, wenn:

- die Bearbeitung von Personendaten in Missachtung der Bearbeitungsgrundsätze, wie sie in Art. 4-7 DSGVO geregelt sind, vorgenommen wird;
- eine Datenbearbeitung gegen den ausdrücklichen Willen des Betroffenen erfolgt;
- eine Bekanntgabe besonders schützenswerter Personendaten<sup>12</sup> oder Persönlichkeitsprofile gegeben ist.

Weiter muss die Bearbeitung von Personendaten nach dem Grundsatz von Treu und Glauben erfolgen<sup>13</sup> und zudem verhältnismässig<sup>14</sup> sein<sup>15</sup>. Weiter ist bei einer Bearbeitung von Personendaten der Zweckbindungsgrundsatz<sup>16</sup> zu beachten<sup>17</sup>.

Aus dem letztgenannten ergibt sich im Hinblick auf den eingangs erwähnten Beispielsfall, dass Personendaten, wie sie die Mitgliederverzeichnisse von Vereinen ohne weiteres darstellen, nur zu dem Zweck bearbeitet werden dürfen, welcher entweder bei der Beschaffung der Daten angegeben wurde, aus den Umständen ersichtlich ist oder durch ein Gesetz erlaubt wird. Bei Neumitgliedern des Vereins ist daher ein entsprechender Hinweis geboten, bei Altmitgliedern empfiehlt sich die Einholung einer Einwilligung<sup>18</sup>.

Allerdings ist zu bedenken, dass im Einzelfall ein Rechtfertigungstatbestand für eine Datenverarbeitung Platz greifen kann. Ein solcher liegt insbesondere dann vor, wenn Daten

---

<sup>11</sup> Art. 3 lit. e DSGVO.

<sup>12</sup> Zu den besonders schützenswerten Personendaten zählen Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit; Massnahmen der sozialen Hilfe und administrative bzw. strafrechtliche Verfolgungen und Sanktionen. Vor dem Hintergrund der zuletzt genannten Gruppe ist erwähnenswert, dass sich zunehmend die Strafverfolgungsbehörden „virtueller Steckbriefe“ bedienen, vgl. beispielsweise die FBI-Site unter < <http://www.fbi.gov/mostwanted/top100/fugitives/laden.htm> > (Stand: 25.11.2000).

<sup>13</sup> U. Widmer/K. Bähler, Rechtsfragen beim Electronic Commerce, 2. Aufl. Zürich 2000, S. 252. Hierdurch wird ausgeschlossen, dass Daten „heimlich“ ohne Wissen des Betroffenen, beispielsweise im Rahmen eines Lauschangriffs, beschafft werden.

<sup>14</sup> Daraus folgt in erster Linie, dass nicht mehr Daten als für den angegebenen Zweck notwendig erhoben werden dürfen.

<sup>15</sup> Art. 4 Abs. 1 DSGVO.

<sup>16</sup> Danach ist es unzulässig, Personendaten zu anderen Zwecken zu bearbeiten, als dies bei der Beschaffung dem Betroffenen explizit angegeben wurde oder für diesen aus den Umständen implizit ersichtlich oder gesetzlich vorgesehen ist.

<sup>17</sup> Art. 4 Abs. 2 DSGVO.

<sup>18</sup> Was zweckmässigerweise vor der geplanten Veröffentlichung über eine entsprechende Mitteilung im Informationsbulletin des Vereins geschehen kann, wobei darauf hinzuweisen ist, dass Mitglieder, welche die Veröffentlichung ihrer Daten ablehnen, durch eine entsprechende Mitteilung die Sperrung der Publikation veranlassen können und dass umgekehrt bei Unterlassen einer Mitteilung ein Einverständnis mit der Zugänglichmachung der Daten auf der Website angenommen wird. Weiter empfiehlt sich eine Erhöhung des Schutzstandards für die Mitglieder durch Vereinbarung eines Passwortschutzes sowie die Anbringung eines Hinweises, dass die zugänglich gemachten Daten nicht für Werbezwecke missbraucht werden dürfen.

mit Personenbezug in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages bearbeitet werden<sup>19</sup>. Daraus ergibt sich beispielsweise die Zulässigkeit der Speicherung und Bearbeitung von Daten durch einen Provider über die Nutzung des Internet durch seine Kunden, welche für die Rechnungstellung der von ihm erbrachten Leistungen erforderlich sind.

Schliesslich ist darauf hinzuweisen, dass bei einer gegebenen Rechtsverletzung durch eine unerlaubte Datenbearbeitung rechtliche Sanktionen vorgesehen sind. Hierzu verweist das DSG grundsätzlich auf die allgemeinen Ansprüche in den Fällen einer Persönlichkeitsrechtsverletzung nach dem Zivilgesetzbuch (ZGB). Im einzelnen kann ein in seiner Persönlichkeit verletzter Betroffener verlangen, dass eine drohende Verletzung durch den Richter verboten, eine bereits bestehende Verletzung beseitigt, die Berichtigung einer persönlichkeitsverletzenden Äusserung bzw. das einschlägige Urteil veröffentlicht oder hilfsweise gerichtlich das Vorhandensein einer Persönlichkeitsrechtsverletzung festgestellt wird. Das DSG präzisiert diese allgemein gegebenen Ansprüche dahingehend, dass zudem verlangt werden kann, Personendaten zu berichtigen oder zu vernichten bzw. die Bekanntgabe an Dritte zu sperren<sup>20</sup>.

### III. Die Übermittlung von Daten ins Ausland

Es liegt auf der Hand, dass die Zulässigkeitsvoraussetzungen für eine rechtlich erlaubte Datenübermittlung ins Ausland für die Akteure des E-Commerce von besonderer Bedeutung sind, weshalb auf diese hier gesondert einzugehen ist. Grundsätzlich gilt nach Schweizer Recht, dass Personendaten nicht ins Ausland bekanntgegeben werden dürfen, wenn dadurch die Persönlichkeit des Betroffenen gefährdet wird<sup>21</sup>. Das ist bereits dann zu bejahen, wenn eine Datenübermittlung in ein Land stattfindet, das ein dem schweizerischen Schutzstandard entsprechendes Datenschutzrecht nicht kennt. Betroffen sind damit nicht zuletzt Bekanntgaben von Daten in die USA, denn dort findet man allenfalls unvollständiges, sektorbezogenes, durch eine Vielzahl von Urteilen ergänztes Datenschutzrecht, wobei erschwerend hinzukommt, dass jeder Bundesstaat eine eigene Datenschutzgesetzgebung hat, mit der Folge eines datenschutzrechtlichen Regelungsstandards in den einzelnen Bundesstaaten von sehr unterschiedlichem Umfang bzw. inhaltlicher Tiefe<sup>22</sup>.

Derartige länderübergreifende Datentransfers waren schon vor dem Aufkommen des Internet gang und gäbe und haben in letzter Zeit selbstverständlich an Bedeutung hinzugewonnen. Zu denken ist z.B. an die Bereiche des grenzüberschreitenden Banküberweisungsverkehrs und der Kreditinformationssysteme, der Personaldatenverarbeitung in multinational tätigen

---

<sup>19</sup> Weitere Rechtfertigungsgründe sind gegeben bei der Bearbeitung von Daten durch Konkurrenten, im Zusammenhang mit Bonitätsprüfungen bzw. im Kontext von Forschung und Statistik. Die entsprechende Aufzählung im DSG hat keinen abschliessenden Charakter, so dass weitere Rechtfertigungsgründe einer Anerkennung durch die Gerichte zugänglich sind.

<sup>20</sup> Kann die Frage nach der Richtigkeit bestimmter personenbezogener Daten nicht mit hinreichender Eindeutigkeit geklärt werden, hat der Betroffene einen Anspruch auf die Anbringung eines Vermerks, der zum Ausdruck bringt, dass er die Richtigkeit der Daten bestreitet.

<sup>21</sup> Art. 6 DSG.

<sup>22</sup> Siehe hierzu *Th. Riemann*, Künftige Regelungen des grenzüberschreitenden Datenschutzverkehrs, CR 1997, S. 762 (763 f.).

Konzernen wie DaimlerChrysler etc.<sup>23</sup>, des transnationalen Flugreiseverkehrs und generell der grenzüberschreitenden Auftragsverarbeitung, wie sie etwa von Outsourcing-Dienstleistern angeboten wird. Um hier den internationalen Wirtschaftsverkehr nicht unangemessen zu beschneiden, muss eine praktikable Lösung gefunden werden. Besondere Beachtung verdient hierbei die EU-Datenschutzrichtlinie, die den rechtlichen Regelungsrahmen für den europäischen Binnenmarkt vorgibt.

Die Vorgaben der Richtlinie laufen auf eine Vertragslösung (ggf. in Verbindung mit einer Einwilligung) hinaus<sup>24</sup>. Bei länderübergreifenden Datenbekanntgaben kommen in erster Linie zwei vertragsrechtliche Konstruktionsmöglichkeiten<sup>25</sup> in Betracht<sup>26</sup>:

- ein Vertrag zwischen dem Datenexporteur und dem Datenempfänger, in welchem dem Betroffenen bestimmte Rechte eingeräumt werden;
- ein Vertrag zwischen dem Endkunden und dem Datenempfänger im Ausland, dessen Abschluss gegebenenfalls durch einen Dritten, wie z.B. der schweizerischen Tochtergesellschaft einer US-Firma, vermittelt wird.

Kommt bei der ersten Variante englisches Recht zur Anwendung, so ist diese Lösung jedoch nur schwer praktikabel. Denn in der Sache stellt die dort umschriebene Regelung einen "Vertrag zugunsten Dritter" dar, ein Rechtsinstitut, das dem anglo-amerikanischen Rechtsraum fremd ist<sup>27</sup>.

Im einzelnen ist es nun vor dem Hintergrund der Zielsetzung der EU-Datenschutzrichtlinie, nämlich der Schaffung eines entsprechenden internationalen Schutzniveaus, nach Art. 25 untersagt, dass eine Übermittlung von Daten in ein Land ohne angemessenes Schutzniveau stattfindet, was der in Art. 6 DSGVO getroffenen Regelung vergleichbar ist. Doch keine Regel ohne Ausnahme(n): Vorliegend hilft Art. 26 Abs. 1 der Richtlinie weiter und nennt einige Ausnahmen. Hier interessieren besonders

<sup>23</sup> Siehe hierzu *Ch. Klug*, Globaler Arbeitnehmerdatenschutz – Ausstrahlungswirkung der EG-Datenschutzrichtlinie auf Drittländer am Beispiel der USA, RDV 1999, S. 109-115.

<sup>24</sup> Siehe auch *R. Ellger*, Vertragslösungen als Ersatz für ein angemessenes Schutzniveau bei Datenübermittlungen in Drittstaaten nach dem neuen Europäischen Datenschutzrecht, *RabelsZ* 60 (1996), S. 738-770.

<sup>25</sup> Ein bekanntes Praxisbeispiel ist die gelungene vertragsrechtliche Lösung mit der Citibank im Rahmen des BahnCard-Projekts in Deutschland. Da die BahnCard und die Citibank Visa in konzerneigenen Rechenzentren in den USA produziert werden, erforderte der damit einhergehende Transfer der Daten der betroffenen Kunden eine eingehende vertragliche Regelung, die schliesslich unter der Federführung des Berliner Datenschutzbeauftragten geleistet wurde. Somit konnte noch vor Umsetzung der EU-Richtlinie erstmals eine Datenübermittlung von hohem Umfang in ein Drittland mit nicht angemessenem Datenschutzniveau durch die Beibringung entsprechender vertraglicher Garantien inter partes geregelt werden. Dies im übrigen zum Wohle der Kunden, die nunmehr ein zum Teil noch über dem (sehr hohen) deutschen Standard liegendes Datenschutzniveau geniessen. (Beispiel nach *H. Eul/Ch. Godefroid*, Übermittlung personenbezogener Daten ins Ausland nach Ablauf der Umsetzungsfrist der EG-Datenschutzrichtlinie, RDV 1998, S. 185 [190]).

<sup>26</sup> Vgl. auch die Einteilung bei *E. Ehmann*, "Vertragslösungen" auf Basis der EG-Datenschutzrichtlinie?, CR 1991, S. 234.

<sup>27</sup> Ausführlich hierzu *R. Ellger*, Vertragslösungen als Ersatz für ein angemessenes Schutzniveau bei Datenübermittlungen in Drittstaaten nach dem neuen Europäischen Datenschutzrecht, *RabelsZ* 60 (1996), 738 (763 ff.); *H. Eul/Ch. Godefroid*, Übermittlung personenbezogener Daten ins Ausland nach Ablauf der Umsetzungsfrist der EG-Datenschutzrichtlinie, RDV 1998, S. 185 (193); *E. Ehmann*, "Vertragslösungen" auf Basis der EG-Datenschutzrichtlinie?, CR 1991, S. 234.

- die Einwilligung des Betroffenen und
- die Datenübermittlung zur Erfüllung eines Vertrages.

Zu beachten ist auch Art. 26 Abs. 2 der Richtlinie, der den Mitgliedstaaten die Möglichkeit einräumt, eine Übermittlung in Drittländer ohne angemessenes Schutzniveau zu genehmigen, wenn derjenige, den die Verantwortlichkeit für die Datenverarbeitung trifft<sup>28</sup>, hinreichende Garantien beibringt für

- den Schutz der Privatsphäre,
- der Grundrechte und
- der Grundfreiheiten der Person hinsichtlich der Ausübung der damit verbundenen Rechte.

Diese Garantien können bei einer anstehenden Datenübermittlung in die USA praktisch insbesondere in der Form von Vertragsklauseln erbracht werden<sup>29</sup>. In diesem Kontext wirkt die EU-Richtlinie im übrigen nicht nur nach innen in die Gemeinschaft hinein, sie entfaltet vielmehr auch eine "Aussen- bzw. Ausstrahlungswirkung"<sup>30</sup>.

Dies soll an einem Beispiel verdeutlicht werden: Angenommen, eine amerikanische Produktions- und Vertriebsfirma hat eine Tochterfirma in der Schweiz. Diese ist im wesentlichen eine Vertriebsfirma. Der Vertrieb erfolgt via Internet über sog. Direktvertrieb mit direktem Versand-Verkauf an die privaten Endkunden. Von diesen sollen nun Daten in einem grösseren Umfang, als für die Vertragserfüllung benötigt, erhoben werden. Diese Daten sollen das Umfeld des Produktes betreffen, um so die Interessenlage des Kunden besser erfassen zu können. Da diese Daten nicht der Schweizer Tochtergesellschaft, sondern vielmehr der US-Firma zugute kommen sollen, stellt sich das Problem, dass die Betroffenen mit dieser kein eigenes Vertragsverhältnis haben. Hier ist nach den oben dargelegten Grundsätzen an die Schaffung eines entsprechenden vertraglichen Rahmens zu denken. Dieser könnte etwa so aussehen, dass die US-Firma eine Art „Nutzer-Club“ unterhält, bei dem man Mitglied werden und in dessen Rahmen man auch Bestellungen tätigen kann.

---

<sup>28</sup> Wer dies ist, ergibt sich aus Art. 2 d der EU-Datenschutzrichtlinie: die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

<sup>29</sup> Zu beachten ist auch, dass nach Art. 26 Abs. 4 der Richtlinie die Kommission befinden kann, dass bestimmte Standardvertragsklauseln ausreichende Garantien nach Art. 26 Abs. 2 bieten. Über einschlägige Initiativen zur Errichtung von Standardklauseln, die im übrigen trotz der ihnen immanenten Einschränkung der Handlungsfreiheit der Beteiligten ein probates Mittel zum Interessenausgleich zwischen den Parteien darstellen (anders etwa die Stellungnahme der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) zu den Entwürfen der Internationalen Handelskammer (ICC) und des Britischen Industrieverbandes (CBI), veröffentlicht in GDD-Mitteilungen 3-4/1998), berichten *H. Eul/Ch. Godefroid*, Übermittlung personenbezogener Daten ins Ausland nach Ablauf der Umsetzungsfrist der EG-Datenschutzrichtlinie, RDV 1998, S. 185 (191). Im übrigen hat der deutsche Gesetzgeber, der die Richtlinie noch nicht umgesetzt hat, in § 4 c II BDSG-E ausdrücklich die Möglichkeit aufgegriffen, entsprechende Garantien durch Vertragsklauseln beizubringen.

<sup>30</sup> Dies ergibt sich allein faktisch daraus, dass einige Länder die Brisanz der EU-Datenschutzrichtlinie für den Datenverkehr zwischen der EU und sich selbst erkannt und dementsprechend Gesetzesvorhaben auf den Weg gebracht haben, um ein angemessenes Datenschutzniveau sicherzustellen, vgl. auch die Beispiele bei *H. Eul/Ch. Godefroid*, Übermittlung personenbezogener Daten ins Ausland nach Ablauf der Umsetzungsfrist der EG-Datenschutzrichtlinie, RDV 1998, S. 185 (189).

Im Ergebnis ist die Zulässigkeit von Datenübermittlungen ins Ausland demnach vorrangig eine Frage effizienten Vertragsmanagements, bei dem die Vereinbarung entsprechender Klauseln gelingen sollte. Aus Raumgründen sei nur darauf hingewiesen, dass in diesem Zusammenhang die Beachtung der Frage nach dem anwendbaren Recht bei der Formulierung des Datenschutzvertrages nicht ausser acht gelassen werden darf<sup>31</sup>.

#### IV. Auskunftspflichten der ISPs

Abschliessend ist auf die Auskunftspflichten der ISPs gegenüber staatlichen Behörden einzugehen. Hier kommt als weitere einschlägige Rechtsquelle das Fernmeldegesetz (FMG) ins Spiel. Dieses verpflichtet die Anbieter von Fernmeldedienstleistungen zur Geheimhaltung des Fernmeldeverkehrs. Infolgedessen dürfen Fernmeldedienstleister grundsätzlich keine Auskunft über den Fernmeldeverkehr ihrer Kunden sowie anderer Teilnehmer an Dritte erteilen oder Dritten die Gelegenheit geben, Angaben über den Fernmeldeverkehr weiterzugeben. Andernfalls machen sie sich strafbar. Die Geheimhaltungspflicht ist umfassend. Ihr unterfallen nicht nur die im Fernmeldeverkehr ausgetauschten Inhalte von Meldungen, sondern darüber hinaus gleichfalls die sog. Randdaten, wie die Identität des Absenders und des Empfängers einer Nachricht sowie die betreffenden Adressierungselemente (z.B. die E-Mail-Adresse), der Zeitpunkt und die Übertragungsdauer einer Nachricht.

Dass dem Fernmeldegeheimnis nicht nur die herkömmlichen Telefonanbieter, sondern auch die ISPs unterstehen, hat das Bundesgericht erst kürzlich entschieden<sup>32</sup>. Unter einem Fernmeldedienst ist nach dem FMG „die fernmeldetechnische Übertragung von Informationen für Dritte“ zu verstehen<sup>33</sup>. Weiter wird dabei unter einer „fernmeldetechnischen Übertragung“ ein „elektrisches, magnetisches, optisches oder anderes elektromagnetisches Senden oder Empfangen von Informationen über Leitung oder Funk“ verstanden<sup>34</sup>. Folglich ist es hinsichtlich der Form gleichgültig, ob Nachrichten im Fernmeldeverkehr etwa per konventioneller Sprachtelefonie oder über die Nutzung von Internet-Diensten<sup>35</sup> übermittelt werden. Eine Ausnahme gilt lediglich für öffentlich zugänglich Informationen, die z.B. der Allgemeinheit auf einer Website zur Verfügung gestellt werden.

Zu beachten ist, dass das Fernmeldegeheimnis nicht ausnahmslos gilt<sup>36</sup>. Zunächst trifft die Fernmeldedienstleister nach Massgabe des FMG sowie der dieses präzisierenden

<sup>31</sup> Ausführlich zu Kollisionsrecht, anwendbarem Recht und Datenschutz *U. Widmer/K. Bähler*, Rechtsfragen beim Electronic Commerce, 2. Aufl. Zürich 2000, S. 264-269; *D. Korff*, Der EG-Richtlinientwurf über Datenschutz und „anwendbares Recht“, RDV 1994, S. 209-217; *P. Mankowski*, Internationales Privatrecht der Providerverträge, in: *G. Spindler* (Hrsg.), Vertragsrecht der Internet-Provider, Köln 2000, Rz. 64 ff.; *ders.*, Anwendbares Recht bei Providerverträgen mit Auslandsberührung, in: Tagungsunterlage Kölner Tage zum Informationsrecht vom 5./6.11.1999 „Vertragsrecht für Internet und Telekommunikation“.

<sup>32</sup> BG, Urteil vom 5.4.2000, sic! 2000, S. 522 = BGE 126 I 50. Siehe hierzu auch *U. Widmer*, Auskunftspflicht der Internet Service Provider über den E-Mail-Verkehr, SWITCHjournal 2000, S. 21-23.

<sup>33</sup> Art. 3 lit. a FMG.

<sup>34</sup> Art. 3 lit. c FMG.

<sup>35</sup> z.B. Voice over IP, E-Mail etc.

<sup>36</sup> Mit diesen Ausnahmen korrespondiert eine Verpflichtung der Anbieter zur Aufbewahrung der sog. Randdaten (betreffend den Verbindungsaufbau sowie die Abrechnungserstellung), damit sie diese ggf. der auskunftersuchenden Behörde mitteilen können.

Verordnung des Bundesrates über Fernmeldedienste die Verpflichtung, im Zusammenhang mit der Rechnungsstellung ihren Kunden zur Möglichkeit der Überprüfung der Korrektheit der Abrechnung über die hierfür erforderlichen Daten Auskunft zu erteilen<sup>37</sup>. Ein Unterschied zu den Abrechnungen der Telefonanbieter besteht insofern, als die Abrechnungsmodelle der ISPs nicht davon abhängig sind, wer Adressat eines E-Mails war bzw. auf welche Website Zugriff genommen wurde. Folglich ist auch ein Bedarf der Kunden an der Mitteilung der entsprechenden Daten zur Rechnungsüberprüfung zu verneinen, da es hierfür schlechthin an der Erforderlichkeit fehlt.

Weiter kommt eine Auskunftspflicht der ISPs in den Fällen in Betracht, in denen ein Kunde missbräuchlich, etwa in belästigender Art und Weise, angerufen wird<sup>38</sup>. Sinn und Zweck dieser Norm ist es darüber hinaus, die Verantwortlichen von IT-Sicherheitsattacken (Hacking etc.) aufzuspüren.

Im Zentrum des Interesses stehen aber allfällige Verpflichtungen der ISPs zur Unterstützung der Strafverfolgungsbehörden. Diese sind in zweierlei Hinsicht denkbar. Zum einen geht es um die Unterstützung der Strafverfolgungsbehörden im Rahmen einer laufenden Überwachung<sup>39</sup>, zum anderen um die Auskunftserteilung betreffend Randdaten. Das FMG spricht lediglich davon, dass die entsprechenden Auskünfte an die zuständigen Behörden zu erteilen seien. Jedoch lässt der Gesetzgeber die ISPs im unklaren darüber, unter welchen Voraussetzungen dies zu geschehen hat. Das Bundesgericht hat nunmehr herausgearbeitet, dass drei Erfordernisse zusammenkommen müssen:

- das verfolgte Delikt muss ein Verbrechen oder Vergehen darstellen, welches vom Unrechtsvorwurf her schwer genug ist, um eine Überwachung des Fernmeldeverkehrs zu rechtfertigen;
- die Behörde muss sich für die Anordnung zur Überwachung einer gesetzlichen Ermächtigungsgrundlage berufen können<sup>40</sup>;
- es muss eine gerichtliche Genehmigung vorliegen.

Eine verfahrensrechtliche Besonderheit besteht insofern, als dass mit dem Dienst für Besondere Aufgaben (DBA) aufgrund des FMG eine Vermittlungsstelle eingerichtet worden ist, die von den Strafverfolgungsbehörden bei einem Auskunftsbegehren angesprochen werden muss. Eine direkte Kontaktaufnahme mit dem Fernmeldeanbieter ist unzulässig, vorab

---

<sup>37</sup> Im einzelnen handelt es sich hierbei um:

- Adressierungselemente der angerufenen Anschlüsse bzw. die Rufnummern der anrufenden Anschlüsse ohne die vier letzten Ziffern;
- Datum, Zeit und Dauer der Verbindungen;
- das für eine einzelne Verbindung zu entrichtende Entgelt.

<sup>38</sup> Im einzelnen handelt es sich hierbei um:

- Datum, Zeit und Dauer der Verbindung;
- Adressierungselemente sowie Namen und Adresse des Inhabers des Anschlusses, über den die missbräuchlichen Verbindung hergestellt worden ist.

<sup>39</sup> Zu denken ist an z.B. an eine Telefonüberwachung im Rahmen einer Abhörschaltung.

<sup>40</sup> Konkret sind für die kantonalen Strafverfolgungsbehörden die jeweiligen Vorschriften der kantonalen Strafprozessordnung einschlägig; das Bundesstrafprozessrecht hilft mit entsprechenden gesetzlichen Grundlagen bei einem Tätigwerden der Strafverfolgungsbehörden des Bundes.

hat der DBA eine Prüfung der Rechtmässigkeit der Überwachungsmassnahme nach den Vorgaben der oben geschilderten Voraussetzungen vorzunehmen<sup>41</sup>.

Angesichts der zentralen Bedeutung für den Internet-Fernmeldeverkehr lohnt ein rechtsvergleichender Blick auf die Situation in Deutschland. Die vom Bundesgericht geprüfte Vorschrift des § 103 StPO/ZH, der eine aktive Mitwirkungsverpflichtung im Strafverfahren statuiert, hat in Deutschland eine Entsprechung in § 95 StPO, einem Bundesgesetz<sup>42</sup>. Die entsprechende Mitwirkung kann sowohl in der Schweiz als auch in Deutschland eben in einer schriftlichen Auskunft bestehen. Wie das Bundesgericht zutreffend erläutert, findet diese Mitwirkungspflicht ihre Grenze dort, wo das durch die gesetzliche Ermächtigung verlangte aktive Tun darin besteht, zusätzliche Handlungen vorzunehmen. Dies könnten in der Praxis beispielsweise eigene Beweisermittlungen sein. Jedoch ist in der deutschen Doktrin mittlerweile anerkannt, dass derartige Verpflichtungen zur Beweisbeschaffung nicht mehr vom Wortlaut der Ermächtigungsgrundlage gedeckt sind<sup>43</sup>. Es stellt sich daher die vom Bundesgericht nicht vertiefte Frage, ob die Grenzen der Mitwirkungspflicht nach § 103 StPO/ZH bzw. § 95 StPO überschritten sind, wenn der angefragte ISP nicht nur bei ihm gespeicherte Daten herausgeben, sondern darüber hinaus auch aus den angegebenen Daten den E-Mail-Absender mit entsprechender Berichterstattung ermitteln soll. Insofern besteht, was eine Präzisierung des Aufwands der Ermittlungen betrifft, noch Diskussionsbedarf. Zutreffenderweise ist wohl nur eine Mitwirkungspflicht in den Fällen anzunehmen, in denen die Daten abgespeichert auf einem Datenträger vorliegen, der wie ein herkömmlicher Aktenordner herausgegeben werden kann.

Dass zum Schutzbereich des Fernmeldegeheimnisses nicht nur die jeweiligen Inhaltsdaten der Kommunikation zu zählen sind, sondern auch die „Randdaten“, die in der deutschen Terminologie „Verbindungsdaten“ heissen und die näheren Kommunikationsumstände bezeichnen, gehört in der deutschen Diskussion gleichfalls zum „common sense“<sup>44</sup>. Die Geltung des Schutzbereiches des Fernmeldegeheimnisses auch für E-Mails, wie sie das Bundesgericht bejaht hat, ergibt sich für Deutschland daraus, dass beim E-Mail-Verkehr Nachrichten jeder Art mit technischen Mitteln nach der Legaldefinition des § 3 Nr. 16 TKG übertragen werden. Im Ergebnis ist damit die deutsche Rechtslage der schweizerischen durchaus vergleichbar, so dass sich grenzüberschreitend aktive ISPs an den durch das Bundesgericht aufgestellten Leitlinien durchaus orientieren können.

---

<sup>41</sup> Eine Ausnahme besteht allerdings für einen Bereich, in dem die Anzahl der Anfragen schlechthin zu gross ist, um vom DBA effizient bewältigt werden zu können: Es sind dies die Fälle, in denen es um die Bekanntgabe des Namens des Inhabers einer bestimmten Telefonnummer bzw. der von einer bestimmten Person gehaltenen Telefonanschlüsse geht.

<sup>42</sup> Gemäss Art. 74 Abs. 1 Nr. 1 GG steht in Deutschland dem Bund eine konkurrierende Gesetzgebungskompetenz für Strafverfahren zu, von der er zwischenzeitlich Gebrauch gemacht hat.

<sup>43</sup> *W. Bär*, Der Zugriff auf Computerdaten im Strafverfahren, 1992, S. 396 ff.; *ders.*, Anmerkung zu Schweiz. BG: Auskunftspflicht des Providers über Absender einer E-Mail, MMR 2000, S. 685.

<sup>44</sup> Vgl. etwa *A. Nack*, in: *Karlsruher Kommentar zur StPO* (4. Aufl. 1999), § 100a Rz. 2 m.w.N.

## V. Zusammenfassung

Die „Datenfundgrube Internet“ bedingt eine „rising tide“ des Datenschutzrechts. In einer Vielzahl von Fallkonstellationen ist den Vorgaben der Datenschutzgesetzgebung Rechnung zu tragen und es sind von den Anbietern von Internet-Dienstleistungen und –Produkten entsprechende Vorkehrungen zu treffen (wie z.B. die rechtzeitige Einholung von Einwilligungen, Beachtung des Zweckbindungsgrundsatzes etc.). Für die besonders praxisrelevanten Datenübermittlungen ins Ausland bieten sich Vertragslösungen unter Beachtung der Bestimmungen auch der EU-Datenschutzrichtlinie an. Was als weiteres Sonderproblem die Wahrung des Fernmeldegeheimnisses betrifft, so dürfen die ISPs aufgrund ihrer entsprechenden fernmelderechtlichen Verpflichtung grundsätzlich über den E-Mail-Verkehr ihrer Kunden keine Auskünfte an Dritte erteilen, andernfalls machen sie sich strafbar.

---

