Prof. Ursula Sury

Rechtsprobleme des Austausches digitaler Dokumente zwischen Privaten

Referat an der Tagung für Informatik und Recht, Bern, 26. Oktober 2004

Der Austausch digitaler Urkunden zwischen Privaten wird immer häufiger, ist aber rechtlich nicht unproblematisch. Der folgende Beitrag zeigt breit aber nicht abschliessend die verschiedenen Facetten der Rechtsaspekte auf und nimmt dabei Bezug auf Fragen, die durch die Technik generiert werden.

Inhaltsübersicht

I. Einleitung

[Rz 1] Dokumente werden in verschiedenen Lebenssituationen und zu verschiedenen Zwecken seit Jahrtausenden

zwischen Menschen ausgetauscht. Im heutigen Informationszeitalter, verbunden mit der wachsenden Globalisierung, werden immer mehr, zum Teil nur noch digitale, Dokumente ausgetauscht. Sobald der Austausch digitaler Dokumente für die Parteien, subjektiv oder objektiv, wichtige Lebenssachverhalte betrifft, besteht häufig eine gewisse Rechtsunsicherheit, und es stellen sich diverse Fragen wie beispielsweise:

- Ist ein Vertrag überhaupt gültig, wenn er nur per Mail abgeschlossen wird?
- Kann ich ein Geschäft vertraulich über das Internet abschliessen?
- Wo werden Entwürfe oder E-Mail-Verkehr durch wen gespeichert und gegebenenfalls ausgewertet?
- Darf ich ein Dokument elektronisch archivieren, also auf eine traditionelle Hardcopy verzichten?

[Rz 2] Um diese Fragen beantworten zu können, ist genau zu analysieren, inwieweit die Informationstechnologie nur ein neues weiteres Medium nebst den traditionelleren wie Papier, Telefax und Telefon ist und inwiefern sich tatsächlich neue Rechtsfragen oder gar Rechtsprobleme stellen.

[Rz 3] In den folgenden Ausführungen wird exemplarisch und nicht abschliessend auf einige aktuelle Rechtsprobleme oder vielmehr Rechtsaspekte des Austausches digitaler Urkunden unter Privaten eingegangen.

II. Digitale Dokumente und Recht

1. Definition des digitalen Dokuments

[Rz 4] Dokumente sind bildliche oder grafische Darstellungen, welche in aller Regel auch etwas beweisen sollen. Der Begriff «Dokument» wird gemäss Duden [1] dem Begriff «Urkunde» gleichgesetzt.

[Rz 5] Traditionelle Dokumente tragen die Information auf Papier oder papierähnlichen Trägern wie Pergament, Fell, Stoff oder andern Trägern wie Stein, Metall, Holz etc. Bei digitalen Dokumenten werden die Informationen in die Logik der Informationstechnologie übersetzt und dort als eine Folge von Nullen und Einsen gespeichert. Mit Hilfe von spezifischer Hard- und Software können diese dann in einer für den Menschen verständlichen Form wieder dargestellt und wiedergegeben werden.

2. Digitale Dokumente im geltenden Recht

[Rz 6] Das schweizerische *Strafgesetzbuch* (StGB)[2] hat den Begriff der digitalen Urkunde per 1. Januar 1995 aufgenommen. Art. 110 Ziff. 5 StGB besagt u.a.: *«Urkunden sind Schriften, die bestimmt und geeignet sind, oder Zeichen, die bestimmt sind, eine Tatsache von rechtlicher Bedeutung zu beweisen. Die Aufzeichnung auf Bild- und Datenträgern steht der Schriftform gleich, sofern sie demselben Zweck dient.»* Dies ist vor allem im Zusammenhang mit den Delikten betreffend Urkundenfälschung [3] von grosser Bedeutung. Seit der Ausweitung der Definition des Urkundenbegriffes für digitale Urkunden sind somit auch Urkundenfälschungen an digitalen Urkunden strafbar. [4]

[Rz 7] Die *Zertifizierungsdiensteverordnung* (ZertDV)[5], welche seit 1. Mai 2000 in Kraft ist, und die sich darauf stützende Verordnung des BAKOM[6] über Dienste der elektronischen Zertifizierung [7] gehen implizit von elektronischen Dokumenten aus. Die ZertDV und die Ausführungsbestimmungen des BAKOM regeln nämlich für einen beschränkten Zeitraum, längstens bis 31. Dezember 2009 [8], versuchsweise die Voraussetzungen für die freiwillige Anerkennung der Anbieterinnen von Zertifizierungsdiensten, welche elektronische Zertifikate ausstellen können.[9] Diese elektronischen Zertifikate können dann zur Erstellung einer digitalen Signatur, d.h. eines elektronischen Codes, verwendet werden, der ein Dokument eindeutig einer bestimmten (der signierenden) Person zuordnet.[10]

[Rz 8] Die *Verordnung des Eidgenössischen Finanzdepartements über elektronisch übermittelte Daten und Informationen* (EIDI-V)[11], seit 1. März 2002 in Kraft, stützt sich auf Art. 45 der Verordnung zum Bundesgesetz über die Mehrwertsteuer (MWSTGV)[12]. Auch sie befasst sich mit digitalen Dokumenten, namentlich mit Rechnungen. Diese werden für die Mehrwertsteuerabrechnung akzeptiert, wenn sie den dort beschriebenen Anforderungen insbesondere an Integrität, Datensicherheit, Überprüfbarkeit und Nachvollziehbarkeit des Datenverarbeitungsvorganges, unveränderter Reproduktion und Wiedergabe sowie Zugriffssicherheit entsprechen.

[Rz 9] Die *Geschäftsbücherverordnung* (GeBüV)[13], welche sich auf Art. 957 Abs. 5 OR [14] stützt, ist seit 1. Juni 2002 in Kraft. Sie regelt den Grundsatz und die Anforderungen an die kaufmännische Buchführung auf elektronische oder vergleichbare Weise. Auch hier geht man vom Bestehen digitaler Dokumente aus, seien dies die einzelnen Konti oder die dazugehörenden Belege. Die digitalen Dokumente nach GeBüV müssen deren Anforderungen an Integrität (Echtheit und Unverfälschbarkeit), Verfügbarkeit und Nachvollziehbarkeit der organisatorischen und elektronischen Vorgänge genügen.[15]

[Rz 10] Die *Verordnung über die Adressierungselemente im Fernmeldebereich* (AEFV)[16], in Kraft seit 1. Januar 1998, geht vom Bestehen digitaler Dokumente aus, welche Private mindestens indirekt betreffen. Diese Verordnung, welche sich auf das Fernmeldegesetz (FMG) [17] stützt, regelt die genaue Zuständigkeit und den Ablauf der Verwaltung und Zuteilung der Adressierungselemente wie insbesondere auch Domain-Namen. Die SWITCH [18] wird dabei verpflichtet, eine Kopie des Tätigkeitsjournals (welches ja nur elektronisch vorliegt!) dem Bundesamt für Kommunikation zur Verfügung zu stellen[19] und die zentrale Datenbank (welche auch elektronisch geführt wird) öffentlich zugänglich zu machen[20].

[Rz 11] Das *Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs* (BÜPF)[21] und die darauf gestützte **Verordnung über die Überwachung des Post- und Fernmeldeverkehrs** (VÜPF)[22], beide in Kraft seit 1. Januar 2002, regeln die Voraussetzungen und den Ablauf der Überwachung des Post- und Fernmeldeverkehrs, konkret folglich auch die Überwachung des Internetverkehrs[23]. Dies betrifft Private ganz zentral, da die Internetprovider bei Vorliegen der notwendigen Voraussetzungen den gesamten Internetverkehr eines möglichen Straftäters oder gar einer Drittperson aufzeichnen und der Untersuchungsbehörde übermitteln sollen. [24] Auch hier geht es um digitale Dokumente, welche Basis für eine mögliche Anklage und ein nachfolgendes Strafurteil bilden.

[Rz 12] Das *Bundesgesetz über das Urheberrecht und verwandte Schutzrechte* (URG)[25], in Kraft seit 1. Juli 1993, unterstellt das Computerprogramm, nebst den klassischen Werken der Literatur und Kunst, dem Urheberrechtsschutz.[26] Zudem werden die klassischen Werke des Urheberrechtes, wie Sprachwerke oder Werke der bildenden Kunst, vermehrt auch oder nur noch digital dargestellt resp. präsentiert. Folglich geht auch das Urheberrechtsgesetz vom Bestehen digitaler, urheberrechtsrelevanter Dokumente aus. [27]

[Rz 13] Das *Bundesgesetz über Datenschutz* (DSG)[28], in Kraft seit 1. Juli 1993, schützt das Recht auf informationelle Selbstbestimmung und verbietet somit unrechtmässige Datenbearbeitungen. Diese Bearbeitungen (jeder Umgang mit Personendaten gilt als Bearbeitung) [29] werden heute in aller Regel mit elektronischen Hilfsmitteln vorgenommen, weshalb auch hier der Gesetzgeber vom Bestehen und der Relevanz digitaler Dokumente ausgeht. [30]

3. Digitale Dokumente im künftigen Recht

[Rz 14] Auf 1. Januar 2005 soll das *Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur* (ZertES)[31] in Kraft treten. Das Gesetz enthält die rechtlichen und organisatorischen Voraussetzungen für die Erstellung elektronischer Signaturen inkl. der dafür notwendigen Institutionen, der sogenannten Anbieterinnen von Zertifizierungsdiensten. Wird ein Dokument mit der gemäss den Vorschriften dieses Gesetzes erstellten qualifizierten elektronischen Signatur[32] unterzeichnet, so ist dies rechtlich der eigenhändigen Unterschrift gleichgestellt.[33] Dies hat diverse Änderungen des Zivilrechts, insbesondere des Obligationenrechts, zur Folge. [34]

[Rz 15] Zeitgleich mit dem ZertES soll die *Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur* (VZertES)[35] in Kraft treten, welche verschiedene Ausführungsbestimmungen enthält. Die Ausführungsbestimmungen technischer und administrativer Art sollen in den Vorschriften des BAKOM betreffend die Zertifizierungsdienste im Bereich der elektronischen Signatur erfolgen. [36]

[Rz 16] Diese drei Erlasse bilden de lege ferenda die Basis für ein selbstverständliches Akzeptieren und einen selbstverständlichen Umgang mit digitalen Dokumenten im B2B, B2C und E-Government-Bereich.

4. Digitale Dokumente im Recht der Europäischen Gemeinschaft

[Rz 17] Die Europäische Gemeinschaft hat in ähnlichen oder gleichen Rechtsfragen legiferiert wie die Schweiz, mit der Zielsetzung, die Rechtssituation in den Mitgliedsländern diesbezüglich zu harmonisieren. Im Folgenden findet

sich eine Auswahl von Richtlinien, welche alle explizit oder implizit vom digitalen Dokument ausgehen und dessen Akzeptanz und Relevanz regeln.[37]

- Richtlinie über den rechtlichen Schutz von Datenbanken (96/9/EG)
- Richtlinien zur Harmonisierung der Schutzdauer der Urheberrechte und bestimmter verwandter Schutzrechte (93/98/EWG)
- Richtlinie über Urheberrecht verwandter Schutzrechte im Bereich Geistiges Eigentum (92/100/EWG)
- Richtlinie über den Rechtsschutz von Computerprogrammen (91/250/EWG)
- Datenschutz-Richtlinie für elektronische Kommunikation (02/58/EG)
- Schutz natürlicher Personen bei der Verarbeitung persönlicher Daten und zum freien Datenverkehr (95/46/EG)
- Richtlinie über den Schutz von zugangskontrollierten Diensten (98/84/EG)
- Richtlinie über gemeinsame Rechtsrahmen für elektronische Kommunikationsnetze (02/21/EG)
- Richtlinie über Wettbewerbsrecht für elektronische Kommunikationsnetze (02/77/EG)
- Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (99/93/EG)
- Richtlinie über den elektronischen Geschäftsverkehr (00/31/EG)
- Richtlinie über den Verbraucherschutz bei Vertragsabschluss im Fernabsatz (97/7/EG)
- Richtlinie über den rechtlichen Schutz von Datenbanken (96/9/EG)

III. Situationen des Austausches digitaler Dokumente

1. Alter Wein in neuen Schläuchen

[Rz 18] Die im Titel genannte Metapher hat wohl kaum je einmal besser gepasst! Wo Menschen leben, privat oder fürs Geschäftliche, tauschen sie – mehr oder weniger zielgerichtete – Informationen aus, sei dies im Rahmen belangloser Alltagskommunikation oder sei dies im Hinblick auf den Abschluss eines Vertrages. Diese Informationen wurden früher mündlich oder schriftlich auf traditionellen Papierträgern und heute mittels neuen Medien, eben elektronisch, übermittelt. Deshalb gilt, ob auf dem Forum Romanum oder im Highspeed-Internet: Menschen tauschen (Lebens-)Informationen aus. Das Medium, d.h. der Träger der Information, hat aber grundsätzlich darauf keinen Einfluss. Form und Inhalt sind grundsätzlich und klar zu unterscheiden und es ist genau zu überprüfen, inwiefern das neue Medium Internet als neue Form einen Einfluss auf den Inhalt der Information hat oder haben kann.

2. Vertragsabschluss

[Rz 19] Der Ablauf des Vertragsabschlusses ist in Art. 1-10 OR [38] geregelt. Diese Bestimmungen gelten selbstverständlich auch für den Vertragsabschluss über das Internet. [39]

[Rz 20] Da die meisten Vertragsabschlüsse keiner speziellen Formvorschrift unterliegen [40], unterstützt das geltende Recht grundsätzlich die Vertragsabschlüsse über das Internet.

[Rz 21] Trotzdem wünschen die Parteien häufig aus Gründen der Rechtssicherheit und der Beweisbarkeit den Abschluss von Verträgen mit einfacher Schriftlichkeit[41]. In der Praxis findet man dies sehr verbreitet, beispielsweise beim Abschluss von Mietverträgen für Wohnungen, Einzelarbeitsverträgen, Werkverträgen (etwa im Baugewerbe), Kaufverträgen (zum Beispiel in der Autobranche) etc.

[Rz 22] Zudem fehlt den Parteien für den Abschluss für sie bedeutender Verträge trotz der technischen Möglichkeiten der Verschlüsselung und der elektronischen Signatur das Vertrauen ins Medium Internet oder sie erachten das Einsetzen von Verschlüsselung und Signatur als lästige technische Verkomplizierung und ziehen den traditionellen Weg der einfachen Schriftlichkeit nach Art. 12 ff. OR [42] vor.

3. Vertragserfüllung

[Rz 23] Die Vertragserfüllung auf digitalem Wege findet man, soweit sie überhaupt grundsätzlich technisch möglich oder standardisiert ist. Dazu zählen die Lieferung und das Herunterladen von Software, Bildmaterial, Text, Musik [43]

und Musiknoten etc.

[Rz 24] Die Bezahlung über das Internet ist technisch noch nicht standardisiert und hat sich in allgemeiner Art deshalb auch noch nicht durchgesetzt. Wohl gibt es die Möglichkeit der indirekten Bezahlung, wenn man beim Contentprovider Leistungen bezieht und dort selbst auch ein Kontokorrent führt. Nicht als Bezahlung und schon gar nicht als Digicash gilt das Zumailen der Kreditkartennummer, dies eröffnet nämlich nur die Möglichkeit des Bezugs von Leistungen auf Kredit, welcher wegen der Garantie eines Dritten (Kreditkartengesellschaft) gewährt wird.

4. Kriminelle Handlungen

[Rz 25] Auch auf dem Wege krimineller Handlungen werden digitale Dokumente verschoben, darauf unberechtigt zugegriffen oder diese unberechtigt verändert.

[Rz 26] Im Bereich der Computer- oder Cyberkriminalität unterscheiden wir grundsätzlich zwei Arten von Delikten: Die Computerdelikte im engeren Sinn und Computerdelikte im weiteren Sinn. [44]

[Rz 27] Bei den *Computerdelikten im engeren Sinn* sind digitale Dokumente, digitale Daten und ICT [45] generell Rechtsschutzobjekte. Zu den Computerdelikten im engen Sinn zählen: unbefugte Datenbeschaffung (Art. 143 StGB), unbefugtes Eindringen in ein Datenverarbeitungssystem (Hacken; Art. 143bis StGB), Datenbeschädigung (Art. 144bis StGB) oder betrügerischer Missbrauch einer Datenverarbeitungsanlage (Computerbetrug; Art. 147 StGB). [46]

[Rz 28] *Computerdelikte im weiteren Sinn* sind Straftatbestände, welche zwar auch mittels traditioneller Medien aber immer häufiger mittels ICT begangen werden können. Dazu zählen beispielsweise: Gewaltdarstellungen (Art. 135 StGB), unbefugtes Beschaffen von Personendaten (Art. 179 StGB), Drohung (Art. 180 StGB), Nötigung (Art. 181 StGB), Ehrverletzungen (Art. 173 – 178 StGB), Pornographie (Art. 197 StGB), Störung der Glaubens- und Kulturfreiheit (Art. 261 StGB) oder Rassendiskriminierung (Art. 261bis StGB). Diese Aufzählung ist nicht abschliessend.

IV. Der Wert der Information

1. Unternehmerische Aspekte

[Rz 29] Informationen oder Daten stehen im Zentrum des unternehmerischen Interesses in der Informationsgesellschaft. Erfolgreich ist, wer mit Informationen und Daten optimal umgehen kann. So stellen sich Fragen des Handlings von Informationen im unternehmerischen Prozess (Wer hat wann auf welche Informationen warum und in welcher Form Zugriff?). Ist dies optimal organisiert, liegen wenig Medienbrüche vor und kann man von einem optimalen Workflow sprechen, arbeitet die Unternehmung grundsätzlich effizient und mit höherer Qualität.[47]

[Rz 30] Der Umgang mit Daten und digitalen Dokumenten ist für Unternehmungen aber vor allem auch dort wichtig, wo mit der Generierung und dem Austausch von neuem Wissen Mehrwert geschaffen werden soll. Die Frage des Beherrschens von Wissensmanagement[48] wird deshalb immer mehr zur Überlebensstrategie.

[Rz 31] Die Auswertung digitaler Dokumente oder ganzer Datenbanken liefert aber auch wichtige Managementinformationen. So können beispielsweise wichtige Entscheidungen für das Marketing heute nur noch gefällt werden, wenn mittels Data Mining mögliche neue Zielgruppen, Segmente oder Märkte gefunden werden.

[Rz 32] Die Betriebswirtschaftslehre bildet dieses Phänomen schon länger ab, zum einen gilt die Information heute nebst Boden, Arbeit und Kapital als vierter Produktionsfaktor [49] und zum andern lassen sich Informationen, unter Einhaltung der Buchführungsvorschriften und ergänzenden Standards, in der Bilanz aktivieren.

[Rz 33] Interessant ist in diesem Zusammenhang, dass dort, wo solche Informationen gesammelt werden können, die preisgebende Person häufig für den Wert und deren Bedeutung nicht sensibilisiert ist. Wie ist es anders zu erklären, dass Tausende von Personen verschiedenste Kunden- und Kreditkarten benutzen oder unverschlüsselt mailen?

2. Compliance[50] und Softlaw

[Rz 34] Viele Unternehmungen sind heute durch Vorgaben ihrer Zulieferanten, Kreditgeber, Mutter- oder Tochtergesellschaften gezwungen, nebst den gesetzlichen auch noch weiteren Anforderungen und Regelwerken zu genügen. Zu denken ist dabei an Anforderungen im Bereich von Qualitätsstandards, wie Vorgaben der ISO [51] oder beispielsweise Good Priv@cy oder best board practice [52]. Die Anforderungen der Zertifizierungsstellen müssen für die Unternehmung konkret umgesetzt werden. Dabei bedient man sich Leitbildern, Policen, Weisungen etc.

[Rz 35] Das Gleiche gilt auch für die Umsetzung der in letzter Zeit in der Branche stark diskutierten Regelwerke wie zum Beispiel der Sarbanes-Oxly Act (SOA), gemäss welchem strenge Anforderungen an Detaillierungsgrad und Wirksamkeit der unternehmensinternen Kontrollen, verbunden mit der eindeutigen Zuordnung von Handlungen zu Personen gestellt werden.[53] Auch gross diskutiert ist das Basel II-Abkommen [54], gemäss welchem Banken gehalten sind, ihre Kreditpolitik gemäss strengen Risikoregelungen zu handhaben. Gemäss Basel II müssen die Banken nämlich nebst der Beachtung klarer Gesamtratings (Eigenmittelhinterlegungen) über verschiedene Managementinformationen wie Analysen von Vergangenheitszahlen, Information über Führungsstruktur, Organisation, Controlling etc. verfügen. Auch dies wird mittels verschiedener Compliance-Instrumente aber auch der erhöhten Aufzeichnung und Archivierung digitaler Dokumente erreicht.

[Rz 36] Diese verschiedenen Compliance-Anforderungen haben einen direkten Einfluss auf die Kontrolle der Erstellung, Versendung, Empfang und Archivierung digitaler Dokumente. Das zentrale Problem ist dabei immer der Zielkonflikt zwischen einem Maximum an Kontrolle einerseits und dem Maximum an Datenschutz, Datensicherheit und der Einhaltung von Berufsgeheimnissen andererseits. [55]

V. Infrastruktur und deren Risiken

[Rz 37] Das Betreiben einer IT-Infrastruktur, mittels derer digitale Dokumente erstellt, übermittelt und aufbewahrt werden, ist heute für praktisch jede Unternehmung und eine Vielzahl von privaten Haushalten eine Selbstverständlichkeit. Der Betrieb dieser Infrastruktur ist erfahrungsgemäss mit vielen, für die Unternehmung zum Teil existenzbedrohenden Risiken verbunden.[56] So treten Probleme verschiedenster Art und daraus folgende Schäden auf, wie beispielsweise, dass Unberechtigte in ein System eindringen können und dort Dokumente lesen oder verändern können[57], so dass Dokumente nicht mehr vertraulich sind oder dass Dokumente in ihrer Originalversion nicht wieder lesbar gemacht werden können. Der Umgang mit solchen Risiken [58] bildet Bestandteil der unübertragbaren und unentziehbaren Verantwortlichkeit des Managements, wie dies beispielsweise für die Aktiengesellschaft in Art. 716a und 717 OR präzisiert ist. [59] Konkret im Rahmen der Organisations-, Compliance- und Führungsverantwortung des Verwaltungsrats (Art. 716a Abs. 1 Ziff. 1 – 5 OR) ist diesem Aspekt des unternehmerischen Unterstützungsprozesses höchste Aufmerksamkeit zu schenken. [60]

[Rz 38] Aber auch jeder Arbeitnehmer ist im Rahmen seiner arbeitsvertraglichen Tätigkeit verpflichtet, die ihm übertragene Arbeit sorgfältig auszuführen und die berechtigten Interessen des Arbeitgebers in guten Treuen zu wahren.[61] Dazu zählt auf jeden Fall auch die Sorgfalt bei jeglichem Umgang mit digitalen Dokumenten. [62] Im Sinne der Umsetzung der Führungsverantwortung empfiehlt es sich unbedingt, die diesbezüglichen spezifischen Pflichten ausdrücklich und konkret zum Bestandteil des Einzelarbeitsvertrages zu machen. Dies ist übrigens auch notwendig, um gegebenenfalls auf einen Arbeitnehmer, welcher seine Sorgfaltspflichten im Umgang mit digitalen Dokumenten verletzt, Rückgriff nehmen zu können. Um die stark subjektivierte Haftung nach Art. 321e OR zur Anwendung zu bringen, ist eine konkrete und adressatengerechte Formulierung der Sorgfaltspflichten zwingend. [63]

VI. Formfragen

1. Recht und Technik

[Rz 39] Wie oben ausgeführt, stellen sich für den Vertragsabschluss von Gesetzes wegen aktuell kaum Probleme. Trotzdem wünschen viele Privatpersonen für den Abschluss von «gewichtigeren» Verträgen das Einhalten der einfachen Schriftlichkeit.[64]

[Rz 40] Möglichkeiten zur Verschlüsselung von digitalen Dokumenten zum Austausch über das Internet gibt es schon relativ lange. Mit den heute gängigen Verschlüsselungs- und Signierungsprodukten kann man die Erfordernisse der Authentizität (Echtheit des Dokumentes), der Integrität (Sicherheit, dass das Dokument nicht verändert wurde), der Non-Repudiation (Nichtabstreitbarkeit des Sendens) und der Vertraulichkeit (niemand anders kann das Dokument lesen) sicherstellen. Obwohl diese Produkte relativ einfach zu handhaben sind, hat sich deren Verwendung interessanterweise noch nicht durchgesetzt.

[Rz 41] Das ZertES wird von Gesetzes wegen die qualifizierte digitale Signatur mit der eigenhändigen Unterschrift gleichstellen.[65] Digital signierte Dokumente genügen den Erfordernissen der Authentizität, der Non-Repudiation und der Integrität. Um das Erfordernis der Vertraulichkeit zu erreichen, muss das ganze Dokument zusätzlich noch verschlüsselt werden.

2. Elektronische Archivierung

[Rz 42] Will man digitale Dokumente korrekt archivieren, so müssen als Erstes auf jeden Fall die Erfordernisse der jeweiligen spezialgesetzlichen Grundlagen, wie beispielsweise der GeBüV oder der EIDI-V, erfüllt werden. Werden Dokumente signiert übermittelt und aufbewahrt, sei das wegen den Vorschriften einer EIDI-V, sei das wegen Sicherheitsstandards im Rahmen der Aufbewahrung von Geschäftsbüchern (GeBüV) oder sei das im Rahmen von zukünftig in einfacher Schriftlichkeit erstellten digitalen Dokumenten nach ZertES, so stellt sich die Frage, wie vorgegangen werden soll, falls die Signatur im Verlaufe der Zeit ungültig wird. Dies kann sich ergeben, weil ein Algorithmus ungültig wird oder weil die verwendeten Signaturschlüssel sich wegen technischer Entwicklungen als unsicher erweisen. Diese sehr interessanten Fragestellungen wurden im deutschen Recht (SigG) [66] grundsätzlich gelöst mit der Möglichkeit, bei bestimmten Voraussetzungen und in bestimmten Verfahren Nachsignaturen anzubringen. In den geplanten, bis jetzt veröffentlichten zukünftigen Rechtsgrundlagen für die Schweiz, insbesondere VZertES, wird dieses Problem jedoch nicht gelöst. Es stellen sich diesbezüglich insbesondere folgende Fragen:

- Welche rechtlichen Auswirkungen hat das automatische Ungültigwerden/Unsicherwerden der Signatur?
- Welche Pflichten treffen die Unternehmungen, welche Dokumente müssen aufbewahrt werden?
- Auf welche Art und Weise kann die ungültig gewordene Signatur kostengünstig wieder erneuert werden?

3. Beweistauglichkeit digitaler Dokumente

[Rz 43] Wie vorne ausgeführt, wird die digitale Urkunde im Recht an verschiedenen Orten schon explizit erwähnt oder von deren Bestehen implizit ausgegangen.

[Rz 44] Im Strafrecht gilt das digitale Dokument als Urkunde (Aufzeichnung auf Bild und Datenträgern [67]). Als Träger der Aufzeichnungen kommt grundsätzlich jedes Medium in Betracht; auch künftige technische Entwicklungen können somit strafrechtlich erfasst werden. [68]

[Rz 45] Urkunden im strafprozessrechtlichen Sinn sind nicht mit denjenigen des materiellen Rechts [69] identisch. Der Begriff ist weiter; so kommt es etwa nicht darauf an, ob der Aussteller erkennbar ist, ob es sich um ein Original oder eine Kopie handelt. Im Strafprozessrecht sind Urkunden Schriftstücke, die gedankliche Äusserungen wiedergeben und zu Beweiszwecken verwendet werden können. Ihr Merkmal besteht darin, dass sie gelesen oder verlesen werden können (Urkunden sind etwa Briefe, Tagebücher, Verträge, Geschäftsbücher, technische Berechnungen und Zeitungsartikel sowie u.U. auch die mittels eines Computers auf magnetischen Datenträgern gespeicherten Daten). [70] Hinsichtlich der digitalen Urkunden stellen sich hohe Anforderungen an die Untersuchungsbehörden (Forensics), damit diese beweisen können, dass die aufgelegten elektronischen Dokumente vom Angeschuldigten erstellt und zwischenzeitlich von niemand anderem abgeändert wurden. [71]

[Rz 46] Das Zivilrecht definiert den Begriff der öffentlichen Urkunde allgemein in Art. 9 Abs. 1 ZGB. Unter öffentlicher Urkunde ist die Feststellung bundesrechtlich bezeichneter Tatsachen oder Willenserklärungen durch eine [72]

zuständige Urkundsperson in gesetzlich geregeltem Verfahren zu verstehen. Die öffentliche Urkunde kann sich weder in einem Tonträger noch in einem elektronischen Datenträger verkörpern, sondern besteht aus einem ohne technische Hilfsmittel lesbaren Schrifttext oder in einem (rechtskräftig) erklärten Grundbuchplan. [73] Somit kann eine digitale Urkunde nicht als eine öffentliche Urkunde im zivilrechtlichen Sinn betrachtet werden.

[Rz 47] Im Zivilprozessrecht ist die Urkunde ein Augenscheinsobjekt besonderer Art. Sie wird regelmässig separat vom Augenschein behandelt. Wo genau die Trennlinie zwischen Urkunde und Augenscheinsobjekt liegt, ist kantonal unterschiedlich.[74] Eine Urkunde im weiten Sinn ist ein Gegenstand, der der Aufzeichnung von Gedanken dient (Schriftstücke, Pläne u. dgl.) oder Dinge der Aussenwelt darstellt (Fotografien, Zeichnungen, Datenträger etc.). [75] Gemäss Luzerner Zivilprozessrecht sind Urkunden Gegenstände, die eine Tatsache in Schrift, Bild, Plan oder ähnlicher Weise kundtun.[76] Unter diesen Begriff fallen Schriftstücke, Pläne, Fotografien, Zeichnungen und andere Gegenstände, die dem Betrachter bestimmte Tatsachen unmittelbar, d.h. ohne Vermittlung durch Wiedergabegeräte, kundtun. Andere Datenträger wie Magnetbänder, Filme, Schallträger und Disketten aller Art benötigen zur Kundgabe ein Wiedergabegerät, weshalb sie keine Urkunden, sondern Augenscheinsobjekte darstellen. [77] Digitale Urkunden zählen im Luzerner Zivilprozess folglich nicht zu den Urkunden, sondern gelten als Augenscheinsobjekte.

VII. Beteiligte Personen

1. Private Personen

[Rz 48] Vorliegend wird der Austausch digitaler Dokumente zwischen privaten Personen beleuchtet. Private Personen gelten als Oberbegriff, damit sind sowohl natürliche als auch juristische Personen gemeint.

[Rz 49] Diese privaten Personen bewegen sich beim Austausch digitaler Urkunden sowohl im Bereich ihres Privatlebens, beispielsweise wenn sie mittels E-Mail kommunizieren, über das Internet eine Reise buchen etc., als auch im Bereiche der Privatwirtschaft (Vertragsabschlüsse über Internet etc.). In seltenen Fällen tritt auch der Staat als Privatperson auf, etwa im nicht hoheitlichen Umfeld wie beim Einkauf von Verbrauchsgütern. [78]

2. Eigener Name oder fremder Name

[Rz 50] Der Austausch digitaler Dokumente kann eine Person für sich selber oder für einen Dritten und dort in direkter oder indirekter Stellvertretung, d.h. in eigenem oder fremdem Namen, [79] erfolgen. Diesbezüglich besteht kein grundsätzlicher Unterschied zum Austausch traditioneller Dokumente. Da aber der virtuose Umgang mit verschiedenen Identitäten im Internet beliebt ist, muss diesem Thema im Folgenden weiter nachgegangen werden.

3. Identity Management

[Rz 51] Mit der steigenden Durchdringung der Welt durch ICT-Systeme (Ubiquitous Computing) haben verschiedene Akteure das Bedürfnis nach Definition und Umgang mit Identitäten im digitalisierten Datenverkehr.

[Rz 52] Identität heisst (aus dem Lateinischen übersetzt) völlige Gleichheit bzw. Übereinstimmung. Identifikation bedeutet die Feststellung, dass etwas identisch, also gleich ist resp. übereinstimmt. Eine Person, sei das eine natürliche oder juristische, kann sich folglich verschiedener Identitäten resp. Teilidentitäten im Austausch mit der Welt, je nach der Rolle, die sie einnimmt, bedienen. Eine identifizierte Einheit im virtuellen Datenverkehr kann also nicht zwingend einer natürlichen oder juristischen Person in der realen Welt zugeordnet werden. Es kann vielmehr nur festgestellt werden, ob die identifizierte Einheit resp. deren Daten, mit den Daten, die andernorts hinterlegt sind, übereinstimmen. Wenn ich mich mit dem Passwort meiner Schwester einlogge und somit identifiziere, wird nur überprüft, ob der angemeldete Benutzer tatsächlich zur Anmeldung berechtigt ist. Das System überprüft somit nicht die Identität (Wer bin ich?; 1:n), sondern die Verifikation (Stimme ich überein?; 1:1).

[Rz 53] Die Regelungen betreffend die digitale Signatur gemäss ZertES sehen eine Identifikation vor, da nur derjenige ein Zertifikat zur Erstellung eines Schlüssels erhält, der sich mittels Pass oder Identitätskarte persönlich ausgewiesen hat.[80] Dass auf diesem Hintergrund das Abhandenkommen eines Zertifikates fatal ist, liegt auf der Hand, da im Gegensatz zur eigenhändigen Unterschrift der Signaturschlüssel auch ohne das Vorhandensein der entsprechenden natürlichen Person verwendet werden kann. Dieses Problem könnte nur mit der zwingenden

Verbindung der Signatur mit einem biometrischen Lebendmerkmal gelöst werden. Auf diesem Hintergrund ist auch verständlich, weshalb es nur natürlichen Personen möglich ist, qualifizierte digitale Signaturen nach ZertES zu erstellen und qualifizierte Zertifikate nach ZertES zu erhalten.

[Rz 54] Unter bestimmten Voraussetzungen ist es auch möglich, gemäss ZertES ein Pseudonym zu verwenden; dieses muss jedoch eindeutig angegeben sein.[81]

4. Privatheit und Anonymität

[Rz 55] Im Zusammenhang mit der Frage der Feststellung und dem Verwalten von Identitäten im digitalisierten Datenverkehr wird die Frage diskutiert, ob und in welchem Umfang Personen Anspruch auf Anonymität und damit verbunden auf Privatheit (Privacy) haben.

[Rz 56] Bezug genommen wird dabei auf die Wahrnehmung der Anonymität in der realen Welt. Zudem wird der Begriff der Privatheit grundsätzlich in der computerdurchdrungenen Welt speziell diskutiert und weiter entwickelt. Unter Privatheit verstehen wir grundsätzlich das Recht einer natürlichen Person in Bereichen, die unsere Kultur der Privatsphäre zuweist, autonom agieren zu können. Dazu zählt die private Wohnung, die Gestaltung privater Beziehungen, die Gestaltung von Freizeit und in diesem Zusammenhang sicher auch der entsprechende Austausch digitaler Urkunden.

[Rz 57] Ob und gegebenenfalls in welchem Umfang ein Recht auf absolute Anonymität besteht, ist offen und kann nicht allein von der anonymitätsbedürftigen Person bestimmt werden. Sobald eine Person mit ihrer Umwelt in Austausch tritt, sei das in der realen oder virtuellen, digitalen Welt, läuft dieser Austausch über eine Schnittstelle, welche per se eine absolute Anonymität ausschliesst. Selbst die Verwendung einer Maske oder eines Pseudonyms schliesst begrifflich eine absolute Anonymität aus. Auch eine Maske oder ein Pseudonym können, im Sinne eines Attributs, zur Verifizierung resp. zur Teilidentifizierung (stimmt die identifizierte Einheit überein, 1:1) verwendet werden.[82]

5. Identity Theft

[Rz 58] Im Rahmen der Diskussionen um die Bedingungen für den Durchbruch von B2B und B2C, verbunden mit der Frage, ob die Gleichstellung der digitalen Signatur mit der eigenhändigen Unterschrift dazu Voraussetzung sei, wurde häufig darauf aufmerksam gemacht, dass das Vertrauen nicht nur in die Sicherheit des Internets grundsätzlich, sondern auch das Vertrauen in das Gegenüber nicht sichergestellt sei. Es sei ja im Internet problemlos möglich, sich als jemand anders auszugeben.

[Rz 59] Tatsächlich kann man sich im Internet hinter einer anderen Person verstecken, zu diesem Zweck werden auch andere Identitäten auf technischem Wege gekapert. Dies ist nichts Neues; in der realen Welt gibt es eine Vielzahl von ähnlichen Situationen. Neu ist daran nur, dass es in der Regel im grenzüberschreitenden Datenverkehr geschieht, viele Adressaten betroffen sind und dies häufig zur Erzielung illegaler Zwecke (beispielsweise Spamming ab einem fremden User-Account) verwendet wird.

[Rz 60] Die rechtlichen Konsequenzen sind dieselben wie beim analogen Sachverhalt in der realen Welt. In zivilrechtlicher Hinsicht entstehen für den vollmachtlosen Vertretenen keine Obligationen, d.h. weder ein Vertrag noch ein Haftpflichtanspruch. Hingegen wird der vollmachtlose Stellvertreter, also derjenige, der ohne Erlaubnis unter einer anderen Identität oder Teilidentität aufgetreten ist, schadenersatzpflichtig. [83] Zudem wird in der Regel eine Datenschutzverletzung[84] vorliegen.

[Rz 61] Je nach konkreter Situation können zudem Straftatbestände wie beispielsweise Betrug (Art. 146 StGB), Verletzungen von Geheimhaltungen (Art. 161 StGB), Ehrverletzungen (Art. 173 ff. StGB) oder Urkundenfälschung (Art. 251 ff. StGB) vorliegen.[85]

VIII. Verhältnis zum Staat

1. Ansprüche der Staatsgewalt

[Rz 62] Will der Staat seiner Aufgabe gerecht werden, so muss er die Einhaltung der von ihm erlassenen Gesetze überprüfen und im Notfall sogar erzwingen. Mit dem Austausch digitaler Urkunden können, wie oben schon kurz ausgeführt, verschiedenste Interessen und Gesetze des Staates verletzt werden.

[Rz 63] Vorerst einmal ist dabei an verschiedenste Straftatbestände zu denken, seien sie im Strafgesetzbuch oder in Spezialgesetzen geregelt. Liegt ein sogenannter Katalogtatbestand gemäss Art. 3 Abs. 2 BÜPF vor, so ist, unter Einhaltung des Verhältnismässigkeitsprinzips, eine Überwachung des Internetverkehrs zulässig. Konkret heisst dies, dass der Staat, vorerst ohne Unterrichtung der betroffenen Person, sämtliche digitale Dokumente heimlich lesen kann.

[Rz 64] In Ergänzung dazu wird der Staat im Rahmen der Sicherung des Staatsschutzes gestützt auf das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) [86] und auf die Verordnung über das Staatsschutz-Informations-System (ISIS-Verordnung)[87] möglicherweise den Internetverkehr und den Austausch digitaler Dokumente überwachen, beispielsweise zur Verhinderung von Spionage oder um selber Spionage zu betreiben.

[Rz 65] In diesem Kontext sind der Vollständigkeit halber auch noch das Militärstrafgesetz [88], Kriegsmaterialgesetz[89] und Atomgesetz[90] zu erwähnen.

2. Infrastrukturelle Aufgaben des Staates

[Rz 66] Das ZertES setzt qualifizierte digitale Signaturen der eigenhändigen Unterschrift gleich [91], sofern und soweit diese sich auf ein qualifiziertes Zertifikat stützen, welches nur von einer vom Bund anerkannten Zertifizierungsstelle [92] herausgegeben werden kann.[93] Die Voraussetzungen, welche an eine solche Zertifizierungsstelle gestellt werden, sind dabei sehr hoch.[94] Ob sich auf diesem Hintergrund privatwirtschaftlich organisierte Unternehmungen für dieses Business interessieren, zumal für ein Zertifikat ja kaum kostendeckende Preise verlangt werden können, ist offen. Zudem stellt sich hier die Frage, ob für ein qualifiziertes Zertifikat, welches für die Identifizierung von Personen und die Möglichkeit des Abschlusses von Verträgen in einfacher Schriftlichkeit usw. [95] sehr bedeutsam ist, nicht ähnliche Überlegungen gelten wie für die Ausstellung einer Identitätskarte oder eines Passes und somit gefolgert werden müsste, es handle sich um eine zwingende hoheitliche staatliche Aufgabe.

3. Menschenrechtsdimension

[Rz 67] Ein weiteres Rechtsproblem im Zusammenhang mit dem Austausch digitaler Dokumente ist die Frage, inwieweit damit Menschenrechte tangiert werden.

[Rz 68] Die unbeschränkte aber auch ungestörte Möglichkeit zum Austausch von Informationen ist ein wesentlicher Bestandteil zur Meinungsbildung und somit Voraussetzung für das Funktionieren einer Demokratie. In diesem Sinne bildet das Recht auf Information das Pendant zur Meinungsäusserungsfreiheit. [96]

[Rz 69] Im Verhältnis zum Staat, also im E-Government-Umfeld, besteht zudem ein Bedürfnis nach Geheimhaltung im Sinne des traditionellen Amtsgeheimnisses und somit auf sichere Übermittlung, sichere Zugriffe und sichere Aufbewahrung von Dokumenten.

[Rz 70] Damit der Austausch digitaler Dokumente zwischen Privaten oder auch zum Staat und somit auch der Austausch von Informationen generell sichergestellt ist, könnte man sich die Frage stellen, ob und in welchem Umfang der Staat verpflichtet ist, eine sichere Internetinfrastruktur allen zur Verfügung zu stellen und somit einerseits das Vertrauen in den Austausch digitaler Dokumente zu erhöhen und anderseits die digitale Spaltung zu reduzieren oder gar zu verhindern.

IX. Spezialfragen betreffend digitaler Dokumente

1. Digitale Dokumente: ein Dauerthema

[Rz 71] Der Umgang und Austausch digitaler Dokumente ist und bleibt auf jeden Fall ein sehr aktuelles Thema. Es ist nämlich Angelpunkt bei verschiedenen wirtschaftlichen Vorgängen wie beispielsweise dem Spamming, den Diskussionen um Digital Right Management, den Rechtsfragen rund um Trusted Computing oder Intrusion Detection etc.

[Rz 72] Im Folgenden wird an diesen Themen die Problematik exemplarisch, aber nicht abschliessend, aufgezeigt.

2. Spamming

[Rz 73] Unter Spam[97] versteht man die unverlangte Zusendung von E-Mail-Nachrichten, also in aller Regel digitaler Dokumente.

[Rz 74] Die zweite Kammer der Schweizerischen Lauterkeitskommission hat am 21. November 2001 im Rahmen der Beurteilung eines konkreten Sachverhalts die Zusendung von Werbe-E-Mails als unlauter erachtet. Spams gelten danach als unlauter, insbesondere wenn zwischen Versender und Empfänger keine Kundenbeziehung oder kein Sachzusammenhang zwischen der angebotenen Ware und dem Empfänger besteht. Zudem gilt die Verkaufsmethode als besonders aggressiv und somit das Bundesgesetz über den unlauteren Wettbewerb (UWG) [98] verletzend, wenn sie die Entscheidungsfreiheit des Empfängers beeinträchtigt, insbesondere auch wenn der Absender nicht klar identifizierbar ist, beispielsweise sich einer andern URL bedient (was häufig vorkommt!) oder sich auch in Worten eine andere, sogar falsche Identität anmasst.

[Rz 75] Mit der Revision des Fernmeldegesetzes (FMG) [99] und des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) soll das Spamming in Zukunft ausdrücklich geregelt werden. Geplant ist, eine EU-konforme Opt-In-Regelung[100] einzuführen, welche faktisch einem Verbot von unverlangten Werbe-E-Mails gleichkommt.

[Rz 76] So verlangt der neue Art. 3 lit. o UWG [101], dass, wer Massenwerbung ohne Zusammenhang mit einem angeforderten Inhalt fernmeldetechnisch sendet, vorher die Einwilligung des Kunden einholen, den korrekten Absender angeben oder auf eine problemlose und kostenlose Ablehnungsmöglichkeit hinweisen muss. Unter Massenwerbung im Sinne dieser Bestimmung sind alle Arten der automatisierten Werbung zu verstehen, wie z.B. SMS, E-Mail, Fax, etc. Für Werbung, welche menschliche Aktivitäten erfordert und daher nicht automatisiert ist, gilt weiterhin die Opt-Out-Regelung[102] (z.B. Kennzeichnung durch * im Telefonbuch), welche in Art. 65 Abs. 1 der Verordnung über Fernmeldedienste (FDV) [103] enthalten ist.

[Rz 77] Zudem sollen die Anbieter von Fernmeldediensten gemäss Art. 45a FMG [104] neu verpflichtet werden, die unlautere Massenwerbung aktiv zu bekämpfen.

[Rz 78] Der Eidgenössische Datenschutzbeauftragte begrüsst in seinem Tätigkeitsbericht 2003 diese neuen gesetzlichen Bestimmungen ausdrücklich und betont, dass die unerwünschte Werbung per E-Mail, abgesehen vom Aufwand und den Kosten, für den EDSB [105] auch datenschutzrechtlich unzulässig ist.

3. Trusted Computing

[Rz 79] Unter Trusted Computing versteht man die Bemühungen verschiedener Hardware- und Softwareanbieter [106], mittels eines im Rechner fest eingebauten Chip («Fritz-Chip») die Sicherheit des Betriebssystems zu erhöhen.

[Rz 80] Damit soll insbesondere vor dem Startvorgang jeweils die Integrität des Betriebssystems geprüft und die Hardware gegenüber dem Betriebssystem aber auch externen Kommunikationspartnern authentisiert werden. Man erhofft sich damit insbesondere Schutz vor Malware. Damit verknüpft ist aber auch die Möglichkeit, nur bestimmte (rechtmässig lizenzierte!) Software auf einem Rechner laufen zu lassen. Zudem können Programme so gestaltet werden, dass (vom Anwender erstellte) Daten fest mit der (rechtmässig!) lizenzierten Software verknüpft sind und ohne diese nicht mehr lesbar gemacht oder weiterbearbeitet werden können. Bei diesen Daten handelt es sich um digitale Dokumente! Folglich hat die Diskussion um die Einführung und Anwendung von Trusted Computing direkt einen grossen Einfluss auf den Austausch digitaler Dokumente unter Privaten. [107]

4. Digital Right Management[108]

[Rz 81] Individuelle geistige Werkschöpfungen, insbesondere auch Sprachwerke und Bilder, unterliegen dem Urheberrechtsschutz[109] und werden sehr häufig in digitaler Form erstellt und ausgetauscht. Mit dem Aufkommen des Internets und dem Wachsen der Softwareindustrie sind zum einen die Urheberrechtsverletzungen stark angestiegen, zum andern wurden aber auch verschiedene technische Instrumente entwickelt, die es den Urhebern effizient erlauben, Verletzungen zu verhindern.[110]

[Rz 82] Digital Right Management-Systeme[111] ermöglichen den Benutzern eine fragmentierte, individualisierte, aber auch kontrollierte Benutzung ihrer urheberrechtlich geschützten Werke für den Eigengebrauch.[112] Dies hat einen Einfluss auf die Art und Weise des Austausches diesbezüglicher digitaler Dokumente, insbesondere auf das Billing. In diesem Zusammenhang wird übrigens diskutiert, ob die kollektiven Verwertungsgesellschaften[113] überhaupt noch eine Daseinsberechtigung haben oder nicht.

[Rz 83] Auch vor dem Hintergrund der verbreiteten Verletzung von Urheberrechten sind in den verschiedenen Staaten nun Bestrebungen im Gange, das Recht des Urhebers auf Urheberrechtsschutz, auch mittels technischer Verfahren, stärker zu gewichten als das Recht auf Eigengebrauch insbesondere durch Private im persönlichen Bereich wie unter Verwandten, Freunden oder bei Werkverwendungen in der Klasse[114].

5. Intrusion Detection Systeme

[Rz 84] Unter Intrusion versteht man die nicht autorisierte Bedrohung der IT-Ressourcen durch einen Angreifer, beispielsweise einen Hacker. Unter Intrusion Detection versteht man folglich sämtliche Vorkehrungen, die böswillige Aktivitäten gegen die eigene eingesetzten IT-Ressourcen feststellen und sämtliche daraus folgenden Aktivitäten zur Vermeidung grösseren Schadens zur Behebung von Lücken etc. Intrusion Detection Systeme (IDS) sind spezielle Sicherheitsmanagement-Software-Werkzeuge, welche im Intrusion Detection-Prozess eingesetzt werden.

[Rz 85] Beim Einsatz von IDS wird normalerweise der gesamte Internetverkehr überprüft und dafür jeweils (wenn auch häufig auch nur für kurze Zeit, d.h. für wenige Sekunden) aufgezeichnet. Je nach System werden dabei Vorkommnisse, welche das System als ungewöhnlich einstuft, herausgefiltert und einem Operator zur Überprüfung resp. Behebung des Problems zugeführt. Bei grossen Unternehmungen wird der Operator 24 Stunden bereit sein, um auf mögliche Attacken reagieren zu können. Zudem versuchen die Systeme auch selber zu reagieren und weitere Abklärungen zu tätigen.[115]

[Rz 86] Viele der Systeme erkennen gewissen Internetverkehr fälschlicherweise als Angriff, dann spricht man von False Positive. Tatsächliche Angriffe, die nicht erkannt werden, nennt man False Negative. Der Einsatz eines IDS kann für die am Austausch digitaler Urkunden beteiligten Personen grosse Auswirkungen haben. Einmal muss man sich bewusst sein (und sollte darüber orientiert sein!), dass der ganze Internet-Verkehr laufend überprüft wird. Zudem könnte es sein, dass ein etwas speziell aufgebautes Dokument als False Positive herausgefischt und genauer, d.h. bewusst, gelesen wird. Wer macht in diesem Fall was damit, wie ist das Problemlösungsvorgehen in der Unternehmung organisiert? Und zuletzt kann es sein, dass das System nicht alle Angriffe erkennt und somit verschiedene intern bestehende Dokumente durch Angreifer gefährdet sein können.

X. Zusammenfassung

[Rz 87] Rechtsprobleme beim Austausch digitaler Urkunden zwischen Privaten gibt es zweifellos sehr viele und in Zukunft immer mehr. Trotzdem ist immer genau zu unterscheiden, entsteht das Problem

- im Inhalt des Dokumentes, weil es elektronisch ist (korrupt werden, mangelnde Vertraulichkeit)?
- wegen der Form des Dokumentes, weil es elektronisch ist (gesetzliche oder von den Parteien gewünschte Anforderung an Formvorschrift)?

- daraus, dass sich traditionelle Fragen akzentuieren, weil das Dokument digital erstellt und ausgetauscht wird (Identität, Non-Repudiation)?

[Rz 88] Die Rechtsprobleme, die sich stellen, lassen sich hauptsächlich wie folgt zusammenfassen:

- Wer digital kommuniziert, ist in seiner Sphäre für die entsprechenden Risiken verantwortlich. Dies trifft speziell das Management von Unternehmungen, bei Aktiengesellschaften den Verwaltungsrat.

- Zwischen den verschiedenen Compliance-Anforderungen und Bedürfnissen nach Forensics einerseits und den Erfordernissen des Datenschutzes und der Berufsgeheimnisse andererseits besteht ein grosser Zielkonflikt. [116]

Literaturverzeichnis

Beutler Stephan, Multimedia und Urheberrecht, Bern 1998.

Brunnstein Klaus, Aktuelle Probleme der IT-Sicherheit und Lösungsansätze = Topical problems of IT-Security and solution approaches, Velbert Online 1994.

Buff Herbert G., Compliance Führungskontrolle durch den Verwaltungsrat, Zürich 2000.

Bühler Lukas, Schweizerisches und internationales Urheberrecht im Internet, Freiburg i.Ü. 1999.

BSI, Bundesamt für Sicherheit in der Informatiktechnik (Hrsg.), IT-Grundschutzhandbuch 2000, Bonn 2000.

Druey Jean Nicolas, Information als Gegenstand des Rechts, Zürich 1995.

Duden, Das Fremdwörterbuch, 7. Auflage, Band 5, Mannheim 2001.

Duden, Das Synonymwörterbuch, 3. Auflage, Band 8, Mannheim 2004.

Guhl Theo, Das Schweizerische Obligationenrecht, 9. Auflage, Zürich 2000.

Guldener Max, Schweizerisches Zivilprozessrecht, 3. Auflage, Zürich 1979.

Häfelin Ulrich / Müller Georg, Grundriss des Allgemeinen Verwaltungsrechts, 4. Auflage, Zürich 2002.

Hansjakob Thomas, BÜPF / VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, St. Gallen 2002.

Hauser Robert / Schweri Erhard, Schweizerisches Strafprozessrecht, 5. Auflage, Basel 2002.

Honsell Heinrich / Vogt Nedim Peter / Geiser Thomas, Schweizerisches Zivilgesetzbuch I Art. 1 – 359 ZGB, 2. Auflage, Basel 2002.

Jahns Christopher / Heim Gerhard, Handbuch Management, Stuttgart 2003.

Maurer Urs / Nedim Peter Vogt, Kommentar zum Schweizerischen Datenschutzgesetz, Basel 1995.

Meier Andreas, Internet & Business, Herausforderung an das Management, Zürich 2001.

Meyer Alfred, DRMS können die Verwertungsgesellschaften nicht ersetzen, in: Zeitschrift Media Lex 2004.

Rehbinder Manfred, Schweizerisches Urheberrecht, 3. Auflage, Bern 2000.

Roth Monika, Compliance, Begriff Bedeutung Beispiele, Basel 1991.

Schmid Niklaus, Computer- sowie Check- und Kreditkarten-Kriminalität: Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994.

Straub C., Informatik-Sicherheitsmanagement, Eine Herausforderung für die Unternehmensführung, Stuttgart 1991.

Studer Matthias, Urheberrechtliche Schranken im Spannungsfeld neuer Rechtsentwicklungen, in: Jusletter vom 15. März 2004.

Studer Urs / Rüegg Viktor / Eiholzer Heiner, Der Luzerner Zivilprozess, Luzern 1994.

Sury Ursula, Aufbewahrung von Unterlagen in elektronischer Form, in: Zeitschrift der schweizerischen Informatikorganisationen, 1/2001 (zit. Aufbewahrung).

Sury Ursula, Die Haftung des Arbeitnehmers bei Verletzung von Informatiksicherheit, in: Zeitschrift der schweizerischen Informatikorganisationen, 4/1999 (zit. Haftung des Arbeitnehmers).

Sury Ursula, Compliance und IT-Security-Law, in: Informatik Spektrum, Heft 5/2002 (zit. Compliance).

Sury Ursula, Computer- und Cyberkriminalität, in: Informatik Spektrum, Heft 3/2003 (zit. Cyperkriminalität).

Sury Ursula, Copying, Downloading, Scanning und Links setzen rechtliche Aspekte rund ums Internet, in: Informatik Spektrum, Heft 6/2002 (zit. Copying).

Sury Ursula, Forensics, in: Zeitschrift der schweizerischen Informatikorganisationen, 2/2002 (zit. Forensics).

Sury Ursula, Identity-Management und Recht, in: Informatik Spektrum, Heft 3/2004 (zit. Identity-Management).

Sury Ursula, Rechtliche Aspekte der IT-Sicherheit, in: Informatik Spektrum, Heft 3/2002 (zit. IT-Sicherheit).

Sury Ursula, Rechtliche Aspekte der IT-Sicherheit, in: Zeitschrift der schweizerischen Informatikorganisationen, 3/2002 (zit. Rechtliche Aspekte).

Sury Ursula, Riskmanagement und IT-Sicherheit, in: Informatik Spektrum, 5/2004 (zit. Riskmanagement).

Sury Ursula, Trusted Computing in der rechtlichen Dimension, in: Informatik Spektrum, Heft 5/2003 (zit. Trusted Computing).

Sury Ursula, Verantwortung und Haftung für menschliche Fehler im IT-Bereich, in: Zeitschrift der schweizerischen Informatikorganisationen, 6/2000 (zit. Verantwortung).

Sury Ursula, Vertragsabschluss und digitale Signatur, in: Zeitschrift der schweizerischen Informatikorganisationen, 2/2000 (zit. digitale Signatur).

Teufel Stephanie / Schlienger Thomas, Informationssicherheit - Wege zur kontrollierten Unsicherheit, in: Praxis der Wirtschaftsinformatik (HMD), Heft 216, 2000.

Thommen Jean-Paul, Managementorientierte Betriebswirtschaftslehre, 7. Auflage, 2004.

Trechsel Stefan, Schweizerisches Strafgesetzbuch, Kurzkommentar, 2. Auflage, Zürich 1997.

Vogel Oskar / Spühler Karl, Grundriss des Zivilprozessrechts, 6. Auflage, Bern 2002.

Vosseler Peter, Neue Geschäftsmodelle mit DRMS, in: Zeitschrift Media Lex, 2004.

Die Autorin ist Rechtsanwältin in Luzern und leitet den Fachhochschul-Lehrgang Wirtschaftsinformatik an der Hochschule für Wirtschaft HSW Luzern der Fachhochschule Zentralschweiz. Sie ist zudem Dozentin für Informatikrecht an verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden.

Résumé français de l’exposé de Me Ursula Sury aux Journées d’informatique juridique 2004 à Berne: Jacques Tissot, Problèmes juridiques posés par l'échange de documents entre particuliers, in: Jusletter 8. November 2004.

1 Duden, Das Fremdwörterbuch, S. 238; Duden, Das Synonymwörterbuch, S. 755.
2 SR 311.0.
3 Art. 251 - 257 StGB.
4 BGE 116 IV 343.
5 SR 784.103.
6 www.bakom.ch.
7 SR 784.103.1.
8 Art. 21 Abs. 2 ZertDV.
9 Art. 1 Abs. 1 ZertDV.
10 Die ZertDV gilt bis zum Inkrafttreten einer entsprechenden gesetzlichen Regelung, welche aktuell auf 1.1.2005 mit dem geplanten Inkrafttreten des Bundesgesetzes über Zertifizierungsdienste im Bereiche der elektronischen Signatur geplant ist, vgl. dazu www.ofj.admin.ch/themen/digsig/intro-d.htm.
11 SR 641.201.1.
12 SR 641.201.
13 SR 221.431.
14 Obligationenrecht; SR 220.
15 Art. 10 Abs. 2 GeBüV.
16 SR 784.104.
17 SR 784.10.
18 www.switch.ch.
19 Art. 13g AEFV.
20 Art. 14h AEFV.
21 SR 780.1.
22 SR 780.11.
23 Art. 1 Abs. 2 BÜPF.
24 Art. 14 Abs. 4 BÜPF; vgl. dazu Hansjakob Thomas, S. 269 f.
25 SR 231.1.
26 vgl. Art. 2 Abs. 3 URG.
27 Vgl. dazu: Rehbinder, N 103 f; Beutler, S. 192 ff; vgl. dazu auch Bühler, Schweizerisches und internationales Urheberrecht im Internet.
28 SR 235.1.
29 Vgl. Art. 3 lit. e DSG.
30 Vgl. dazu Maurer / Nedim, N 22 zu Art. 3 DSG.
31 SR 943.03.
32

Art. 2 lit. c ZertES.
[33] Art. 14 Abs. 2bis OR (ab 1.1.2005), vgl. dazu Meier Andreas, S. 202.
[34] Vgl. Anhang des ZertES.
[35] SR 946.512.
[36] www.bakom.ch.
[37] http://europa.eu.int/eur-lex/index.html.
[38] SR 220.
[39] Vgl. Sury (digitale Signatur), 2/2000.
[40] Art. 11 OR.
[41] Art. 12 ff. OR.
[42] vgl. Guhl Theo / Koller Alfred, § 14 N 13.
[43] Vgl. dazu Sury (digitale Signatur), 2/2000.
[44] Vgl. dazu Sury (Cyberkriminalität), Heft 3/2003.
[45] ICT: Informations- und Kommunikationstechnologie.
[46] SR 311.0; vgl. dazu Schmid, Computer- sowie Check- und Kreditkarten-Kriminalität.
[47] Thommen, S. 7851 f.
[48] Vgl. dazu Jahns / Heim, Handbuch Management.
[49] Thommen, S. 33, 40.
[50] Begriff Compliance: vgl. dazu Roth, Compliance, Begriff Bedeutung Beispiele.
[51] ISO: International Organization for Standardization.
[52] www.sqs.ch.
[53] www.pwc.com/de/ger/ins-sol/online-sol/themenpools/tpool_sarbanes-oxley.html.
[54] www.ebk.ch, http://basel-ii.info.
[55] Vgl. Sury (Compliance), Heft 5/2002.
[56] Vgl. dazu Brunnstein, Aktuelle Probleme der IT-Sicherheit und Lösungsansätze; Sury (Verantwortung), 6/2000.
[57] Teufel / Schlienger, S. 18 - 31.
[58] Vgl. dazu Straub, Informatik-Sicherheitsmanagement.
[59] Vgl. dazu Sury (IT-Sicherheit), Heft 3/2002.
[60] Vgl. dazu Sury (Riskmanagement), Heft 5/2004; BSI, IT-Grundschutzhandbuch; Roth, S. 73; Buff, S. 101 ff.
[61] Art. 321a Abs. 1 OR.
[62] Vgl. dazu Sury (Haftung des Arbeitnehmers), 4/1999.
[63] Vgl. dazu Sury (Rechtliche Aspekte), 3/2002.
[64] Art. 13 – 15 OR.
[65] Art. 14 Abs. 2bis OR (ab 1.1.2005).
[66] Gesetz zur digitalen Signatur vom 16. Mai 2001 (BGBI I 2001 876).
[67] Art. 110 Ziff. 5 StGB.
[68] Trechsel, N 11c zu Vor Art. 251 StGB.
[69] Art. 110 Ziff. 5 StGB.
[70] BGE 116 IV 345 E. 3; Hauser / Schweri, § 66 N 1.
[71] Vgl. dazu Sury (Aufbewahrung), 1/2001.
[72] Honsell / Vogt / Geiser, N 7 zu Art. 9 ZGB.
[73] Honsell / Vogt / Geiser, N 13 f. zu Art. 9 ZGB.
[74] Guldener, S. 332.
[75] Vogel / Spühler, 10 N 107.
[76] § 149 der Luzerner Zivilprozessordnung; SRL 260a.

[77] Studer / Rüegg / Eiholzer, § 149 N 1.
[78] Vgl. dazu Häfelin / Müller, N 272 ff.
[79] Vgl. dazu Guhl / Koller, § 18 N 8.
[80] Art. 8 Abs. 1 ZertES.
[81] Art. 6 Abs. 3 lit. f ZertES; Sury (Identity-Management), Heft 3/2004.
[82] Vgl. Sury (Identity-Management), Heft 3/2004.
[83] Art. 32 – 40 OR.
[84] Art. 34 f. DSG.
[85] Vgl. Sury (Identity-Management), Heft 3/2004.
[86] SR 120.
[87] SR 120.3.
[88] SR 321.0.
[89] SR 514.51.
[90] SR 732.0.
[91] Vgl. Art. 14 Abs. 2bis OR (ab 1.1.2005).
[92] Akkreditierungsstelle; Art. 4 ZertES.
[93] Vgl. Meier, S. 197 f.
[94] Vgl. insbesondere Art. 3 – 5 und 8 – 14 ZertES.
[95] Vgl. Ausführungen oben.
[96] Vgl. dazu Druey, Information als Gegenstand des Rechts.
[97] Spiced ham, Kurzform für Würzfleisch spiced ham, wurde durch die Komikergruppe Monthy Python in einem Sketch immer wieder unverlangt/unbestellt serviert.
[98] SR 241.
[99] SR 784.10.
[100] Opt-In: Verfahren, bei dem der Anwender für den Empfang von Werbemail bei einem Anbieter in eine sog. «Opt-In-Liste» eintragen kann. Er erhält dann auf eigenen Wunsch Werbung.
[101] Dieser Artikel ist zurzeit noch nicht in Kraft getreten.
[102] Opt-Out: Verfahren, bei dem der Empfänger einer Werbemail die Möglichkeit hat, sich aus der Verteilerliste des Anbieters entfernen zu lassen, wenn er keine weitere Werbung wünscht.
[103] SR 784.101.1.
[104] Dieser Artikel ist zurzeit noch nicht in Kraft getreten.
[105] Eidgenössischer Datenschutzbeauftragter.
[106] TCPA, Trusted Computing Platform Alliance, vgl. www.trustedcomputing.org.
[107] Vgl. Sury (Trusted Computing), Heft 5/2003.
[108] Vgl. Studer Matthias: Das Digital Rights Management wird, pointiert gesagt, zu einem Digital Restriction Management; vgl. auch www.fsf.org/philosophy/words-to-avoid.html#DigitalRightsManagement.
[109] Art. 2 URG.
[110] Vgl. Sury (Copying), Heft 6/2002.
[111] Vosseler, S. 69.
[112] Meyer, S. 67.
[113] Vgl. Art. 20, insbesondere Abs. 4 URG.
[114] vgl. Art. 19 URG.
[115] Vgl. Sury (Identity-Management), Heft 3/2004.
[116] Vgl. Sury (Forensics), 2/2002.

Rechtsgebiet:	Informatikrecht
Erschienen in:	Jusletter 8. November 2004
Zitiervorschlag:	Ursula Sury, Rechtsprobleme des Austausches digitaler Dokumente zwischen Privaten, in: Jusletter 8. November 2004
Internetadresse:	http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=3450