Agnes Berlakovich

Kryptographie

In der Informationsgesellschaft, die derzeit im Entstehen ist, wird bereits ein großer Teil der Kommunikation über Computernetze vorgenommen. Altbekannte Kommunikationsmittel werden durch entsprechende elektronische Formen ergänzt oder sogar abgelöst.
Der Vorteil der neue Kommunikationsmittel liegt nicht nur in ihrer Nutzungsmöglichkeit für private Kommunikation. Diese ermöglichen auch die Einführung neuer Transaktionsmöglichkeiten für den Geschäftsverkehr (E-Commerce), und bringen neue Möglichkeiten für das Verwaltungshandeln des Staates bzw. der Partizipationsmöglichkeiten der BürgerInnen (E- Government, E-Voting) mit sich.

Die Nachteile liegen auf der Hand: Unsicherheit, ob der, mit dem ich kommuniziere wirklich derjenige ist, der er vorgibt zu sein bzw. auf der anderen Seite, ob die Informationen, die ich über das Netz schicke auch wirklich nur von demjenigen lesbar sind, für den sie gedacht sind; sowie ob die Informationen, die gesendet werden, nicht verfälscht bzw. geändert werden.

Der Einsatz von Kryptographie bietet die Möglichkeit, oben genannte Risiken zu minimieren[1] bzw. auszuschalten.

Was ist Kryptographie?
Kryptographie ist die Technik der Verschlüsselung von Nachrichten. Verschlüsselung ist die Substituierung eines bestimmten Zeichens durch ein willkürlich gewähltes anderes Zeichen.
Kryptographie hat für viele etwas geheimnisvolles an sich. Dabei ist verschlüsselte bzw. codierte Kommunikation so alt wie Kommunikation an sich.
Das Wort Kryptographie leitet sich aus den griechischen Wörtern "krypto" (ich verberge) und "graphe" (das Schriftstück) ab. Kryptographie ist die Wissenschaft, die sich mit der Absicherung von Nachrichten beschäftigt. Als Kryptanalyse wird die

[1] Sorgloser Umgang, Sicherheitslöcher...

Kunst bezeichnet, chiffrierte Nachrichten aufzubrechen, d. h. deren geheime Inhalte lesbar zu machen. Zusammenfassend wird jener Zweig der Mathematik, der Kryptographie und Kryptoanalyse umfasst, als Kryptologie bezeichnet. Nicht abgesicherte Daten werden als Klartext, abgesicherte Daten als Chiffretext bezeichnet. Der Vorgang, Klartext in Chiffretext umzuwandeln, wird als Chiffrierung (auch Verschlüsselung) bezeichnet. Der umgekehrte Vorgang, die Umwandlung von Chiffretext in Klartext, wird als Dechiffrierung (Entschlüsselung) bezeichnet.

a) Algorithmen und Schlüssel

Um Kryptographie tatsächlich anwenden zu können, müssen sich Sender und Empfänger auf ein bestimmtes Verfahren einigen, das sie verwenden wollen; das ist der **Algorithmus**. Wäre das Wissen um den verwendeten Algorithmus aber alles, was zur Entschlüsselung notwendig ist, so ließe sich Kryptographie praktisch nicht verwenden, da etwa bei einer Implementierung in Software jedermann Einsicht in das Verfahren nehmen und somit abgesicherte Nachrichten unbefugt mitlesen könnte. Dem Verfahren wird deshalb ein variabler Parameter hinzugefügt, der sogenannte **Schlüssel**. Auch auf diesen müssen die Beteiligten sich einigen, er bleibt jedoch ihr Geheimnis und ist auch innerhalb eines Algorithmus veränderlich.

Bereits im klassischen Altertum sind Nachrichten chiffriert worden, um sie vor fremden Augen zu schützen. Caesar vertauschte beispielsweise nach einer einfachen Regel die einzelnen Buchstaben des lateinischen Alphabets, so dass der Text für einen Uneingeweihten wie ein unsinniger Buchstabensalat aussah.

In Zusammenhang mit einer sicheren Kommunikation im Internet werden an die Kryptographie vier Forderungen gestellt. Erstens muss dem Empfänger einer Nachricht die Identität des Autors ersichtlich sein. Vom Empfänger einer Nachricht muss aber auch sichergestellt sein, dass er überhaupt berechtigt ist, dieses zu empfangen. Als zweite Anforderung ist die Integrität der übermittelten Daten zu nennen, d. h. diese dürfen nicht verändert worden sein. Drittens soll der Urheber der übermittelten Daten seine Urheberschaft nicht abstreiten können und der Empfänger der Daten soll den Empfang nicht abstreiten können. Schliesslich ist die Sicherstellung der Vertraulichkeit von Daten zu gewährleisten.

Die Geschichte der Kryptographie

Ver- und Entschlüsselung war jahrhundertelang die Spielwiese von Geheimdiensten und wurde nur von diesen genutzt. Kriege wurden gewonnen und verloren, weil Verschlüsselungscodes „geknackt“ wurden.

Bereits im klassischen Altertum sind Nachrichten chiffriert worden, um sie vor fremden Augen zu schützen. Julius Caesar hat Verschlüsselung dermaßen oft angewendet, dass Valerius Probus ein eigenes Buch über Caesars Verschlüsselungsmethoden schrieb. In Caesars „Gallische Kriege“ ist auch erste Einsatz von Kryptographie für militärische Zwecke dokumentiert.

Bekannte Beispiele, die das vergangenen Jahrhunderts, insbesondere den Ausgang der beiden Weltkriege mitprägten, sind die Entschlüsselung der Zimmermann-Depesche und die der ENIGMA- Maschine.

Arthur Zimmermann war deutscher Innenminister während des WK I und die Amerikaner sahen ihn als Friedensstifter und sahen daher nicht die Notwendigkeit, in den Krieg einzugreifen. Erst nachdem die Briten ein Telegramm von Zimmermann, in dem dieser die Kriegsstrategien an die Bündnispartner der Deutschen mitteilte, stiegen die Amerikaner in den Krieg ein, was letztendlich dann auch kriegsentscheidend gewesen ist.

Oder ENIGMA: ENIGMA bedeutet soviel wie Rätsel, und das sollte die Chiffriermaschine für die Kryptoanlytiker auch sein. Die ENIGMA wurde von dem deutschen Erfinder Arthur Scherbius entwickelt. Er erwarb 1918 das Patent und 1925 ging die Produktion der ENIGMA in die Serienfertigung. Die ENIGMA ist die meist verkaufte mechanische Verschlüsselungsmaschine. Die ENIGMA war so erfolgreich, weil das deutsche Militär die kryptologischen Debakel des 1. Weltkrieges (hier vor allem die Zimmermann-Depesche) nicht wiederholt sehen wollte. Das deutsche Militär kaufte zwischen 1925 und 1945 über 30000 ENIGMAS. Der Erfolg der Kryptoanalytiker ist mit zwei Namen verbunden: Marian Rejewski (1905-1980) und Alan Turing (1912-1954). Diese beiden entdeckten jeweils die Achilles-Ferse der ENIGMA, bedingt sowohl durch schlechtes und schlampiges Bedienen der ENIGMA durch die Deutschen als auch durch Spionagetätigkeit bzw. Glücksfunde. Die erfolgreiche Kryptoanalyse gilt als wichtiger Schritt auf dem Weg zum Sieg der Alliierten über das Dritte Reich. Da es gleichzeitig auch gelang in gesunkenen U-Booten der Deutschen die Codes zu finden, konnte durch die damit mögliche

Entschlüsselung der durch die ENIGMA verschlüsselte Korrespondenz der Deutschen der zweite Weltkrieg zumindest verkürzt werden.

Symmetrische/Asymmetrische Schlüssel

Kryptographie bietet die Möglichkeit, anhand von mathematischen Verfahren, Daten so umzuwandeln, dass sie nur mit dem passenden Schlüssel wieder zurückverwandelt werden können.

Die anhand der Kryptographie erstellten Systeme zur Verschlüsselung von Nachrichten werden eingeteilt in symmetrische und asymmetrische Verfahren.

Symmetrisches Verfahren: es gibt nur einen Schlüssel, der zum ver- und entschlüsseln verwendet wird. Das Problem ist die sichere Übertragbarkeit des Schlüssels. Bevor man bei dieser Methode verschlüsselt miteinander kommunizieren kann, ist ein Austausch des Schlüssels notwendig. So beschäftigten in den 70- er Jahren große Gesellschaften, insbesondere Banken „dispatch- rider", deren Aufgabe es war, die Schlüssel in einem verschlossenen Koffer den Kunden auf der ganzen Welt zu überbringen: die Kosten dieser Übertragungsmethode stiegen jedoch mit der Zeit in das Unermessliche und so wurden die damaligen mathematischen und technischen Errungenschaften der 70- er- Jahre begrüßt. So gelang es durch die Anwendung modularer arithmetischer Einwegfunktionen[2] eine Methode zu finden, die ermöglichte, dass die an der Kommunikation beteiligten sich über einen Schlüssel einigten, ohne sich treffen zu müssen.

Der nächste Schritt war die Standardisierung der Systeme, die für die Kommunikation zwischen verschiedenen Organisationen essentiell ist. So gelang es vorerst mit DES (Data encryption standard) einen Standard für Verschlüsselungscodes zu finden, der bis vor einigen Jahren in den USA noch Standard gewesen ist.

Mit der Entwicklung des asymmetrischen Schlüssels durch Wissenschaftler des MIT Ende der 70-er- Jahre gelang es, den Grundstein für sichere verschlüsselte Kommunikation auch in elektronischer Form zu legen.

Dieses Verfahren basiert darauf, dass ein öffentlicher Schlüssel (der z. B. auf der Website zugänglich gemacht bzw. dem jeweiligen Kommunikationspartner übermittelt

[2] Modulare arithmetische Einwegfunktionen sind leicht zu erstellen, aber sie sind nicht reversibel (z.B. das Mischen von blauer und gelber Farbe, das Aufschlagen eines Eis)

wird) zum Verschlüsseln verwendet wird und ein privater Schlüssel -der nur für den user, dem er zugeordnet ist, zugänglich ist- zum Entschlüsseln.
Bei hybriden Verfahren (z.B. PGP) Verfahren werden die Vorteile von symmetrischen und asymmetrischen Verfahren kombiniert, um die Nachteile des beiden Systemen (asymmetrischer Schlüssel: „groß“ und braucht viel Kapazität; symmetrischer Schlüssel: Notwendigkeit des Schlüsselaustausches) auszuschließen.

Kryptographie und Politik

Kryptographie war – aufgrund deren technischen Überlegenheit“ jahrhundertelang Nachrichtendiensten vorbehalten. Erst die Entwicklung des Computers und dessen „Massenverbreitung“, insbesondere der Einsatz der durch diese ermöglichten „neuen“ Kommunikationsmöglichkeiten machten Verschlüsselung zu einem Thema für die „Allgemeinheit“.
Mit der größeren Verbreitung von Verschlüsselungssoftware haben sich die Geheimdienste bzw. die Staaten dann wieder eingeschaltet. Während es in der Vergangenheit aufgrund der technischen Überlegenheit der Nachrichtendienste für diese rasch und einfach möglich gewesen ist, durch das Ausprobieren von verschiedenen Schlüsseln, verschlüsselte Texte zu knacken, erlauben die technischen Entwicklungen der letzten Jahre Verschlüsselungen, die nicht so einfach geknackt werden können.
Das Thema Kryptographie ist zu einem rechtspolitischen Thema geworden, bei dem die Meinungen hart aufeinanderprallen. Auf der einen Seite sehen Befürworter von Kryptographie die Möglichkeit, dem Bürger durch die Einschränkung des Informationsstrebens des Staates ein Mindestmass an Privatheit zuzubilligen. Diese argumentieren unter anderem mit dem Briefgeheimnis. Die unverschlüsselte E- Mail sei lediglich eine Postkarte, erst durch die Verschlüsselung (die einen elektronsichen Briefumschlag datstelle) werde dieses zu einem Brief und erst dadurch könne das Briefgeheimnis auch für elektronische Kommunikation gewahrt werden.
Auf der anderen Seite argumentieren Befürworter einer Regulierung, dass die Kryptographie nur dem organisierten Verbrechen und Terroristen nütze. Der gesetzestreue Bürger, unter dem Motto „das beste Ruhekissen ist ein gutes Gewissen“ hätte durch eine potentielle Zugänglichkeit seiner Nachrichten ja sowieso nichts zu befürchten.

In vielen Staaten wurde mit dieser Argumentation Verschlüsselung beschränkt und auch Import- und Exportbeschränkungen für Verschlüsselungssoftware eingeführt.
So wurde z. B. in den USA Verschlüsselungssoftware als Waffe definiert. Phil Zimmermann, der Erfinder von PGP bekam dies zu spüren. Er wurde verhaftet und gegen ihn wurden jahrelang Ermittlungen geführt, weil er PGP
In den USA wurden erst im Jahre 2000 die Exportbestimmungen geändert und ist nur der Export in gewisse „kritische" Länder verboten.

Reglementierungsmöglichkeiten

Als mögliche Regulierungsmaßnahmen kommen insbesondere ein Totalverbot, die Verwendung kurzer Schlüssel bzw. schwacher Algorithmen, die Schlüsselhinterlegung (key-escrow-system) und die Schlüsselrückgewinnung in Betracht.

Totalverbot

Ein Totalverbot trifft alle Verschlüsselungsmethoden. Ausgenommen von solchen Verboten werden regelmäßig digitale Signaturverfahren, die nur der Integrität und Authentifikation dienen.
Ein Totalverbot mit Erlaubnisvorbehalt besteht z. B. in Frankreich und in Russland, wo jede Verwendung von Kryptoverfahren genehmigungspflichtig ist.
Um ein Totalverbot „administrieren" zu können, müssten Stichproben gemacht werden, bei denen nach verschlüsselten Nachrichten gesucht wird.

Verwendung kurzer Schlüssel bzw. schwacher Algorithmen

Lizenzierungsverfahren, bei dem von staatlicher Seite nur schwache Verschlüsselungsalgorithmen bzw. Verfahren mit kurzen Schlüssellängen zugelassen werden. Ein technisch versierter Angreifer, der über ausreichende Rechenkapazität verfügt, wie dies bei einem Großunternehmen oder Geheimdiensten anzunehmen ist, kann diese Schlüssel jedoch relativ leicht „knacken"

Schlüsselhinterlegung/ Key Escrow System

Der Verschlüsselungsschlüssel wird einer „trusted third party" anvertraut.
Folgende Verfahren sind hier denkbar:

1. eine key escrow- Lösung, bei der Anbieter von Verschlüsselungsdienstleistungen bei Bedarf den Sicherheitsbehörden die Schlüssel von Kunden zur Verfügung stellen müssen.
2. eine key- escrow- Lösung, bei der jedoch ausschließlich staatlich linzenzierte Anbieter von Verschlüsselungsdienstleistungen operieren dürfen
3. eine key- escrow- Lösung mit gleichzeitigem Verbot aller nicht amtlich zugelassenen Verfahren.

In der USA wird ein Schlüsselhinterlegungsverfahren auf freiwilligen Basis mit Hilfe des sogenannten Clipper- Chips angeboten.

Schlüsselrückgewinnung

Kryptographische Verfahren mit Schlüsselrückgewinnungseigenschaften verfügen über einen elektronischen Hintergang, durch den der Schlüssel aus einer Chiffretextnachricht rekonstruiert werden kann. Solche Verfahren haben jedoch bisher das Entwicklungsstadium noch nicht überschritten.

Reglementierung und Grundrechte

Im Folgenden folgt eine kurze Darstellung der Grundrechte, in die bei einer Regulierung von Kryptographie von staatlicher Seite eingegriffen wird.

Recht auf Achtung des Privatlebens (Art 8 EMRK)

Das Recht auf Achtung des Privatlebens soll (nach der EKMR) dem einzelnen seinen privaten Bereich sichern, in dem er seine Persönlichkeit frei entwickeln und entfalten kann.

Dieses Recht ist ein „Auffangrecht“, das –über speziell gewährleistete liberale Freiheiten hinaus- jedem Menschen einen Bereich sichern soll, in dem er ohne unerwünschte Teilhabe von aussen seine Persönlichkeit und Individualität frei zum Ausdruck bringen, entwickeln und entfalten kann. Das Grundrecht ist „offen“ wie kein anderes, das heißt, dass die von ihm im einzelnen geschützten Lebensbereiche erst im Einzelfall über die Rechtsprechung konkretisierbare sin. Das Grundrecht umfasst nach der bisherigen Rechtsprechung und Literatur den Schutz der Selbstbestimmung und Privatsphäre jedes Menschen, und ist demgemäß überaus vielfältig.

Ihren Ausdruck findet die Selbstbestimmung des Menschen etwa in der informationellen Selbstbestimmung:
Bei Datenübertragungen im Internet fallen Verbindungsdaten an. Diese geben Auskunft über Datum und Uhrzeit der Übertragung, Sender- und Empfangsadresse sowie benützte Internet- Dienste. Zusätzlich werden von vielen Personen weitere Daten, wie z. B. E-Mail- Adresse, die Benutzeranschrift oder die Kreditkartennummer im Internet gespeichert. Obwohl diese Daten meistens im Netz verstreut sind, besteht die Möglichkeit diese Daten zu sammeln und zu Kommunikations- und Persönlichkeitsprofilen zu verdichten, ohne dass der Nutzer darauf Einfluss hat.
Das deutsche Bundesverfassungsgericht hat z. B. im Volkszählungsurteil das Recht auf informationelle Selbstbestimmung entwickelt. Dieses gewährleistet nach Rechtsprechung des Bundesverfassungsgerichtes das Bedürfnis des Einzelnen, grundsätzlich selbst darüber zu urteilen, in welchem Umfang und an wen er Informationen über sich selbst mitteilt. Das Zusammentragen und Auswerten von persönlichen Daten und Informationen sowie die inhaltliche Überwachung und Aufzeichnung von persönlichen Mitteilungen stellen somit einen Eingriff in das Recht auf informationelle Selbstverwaltung dar.

Ein Eingriff in den Schutzbereich des Art. 8 MRK ist nur zulässig, wenn er
Gesetzlich vorgesehen ist und in einer demokratischen Gesellschaft zur Erreichung eines der im Art 8 MRK angeführten Zwecke notwendig ist („materieller Gesetzesvorbehalt“). Das Grundrecht steht also unter einem materiellen Gesetzesvorbehalt.
Eingriffe in die geschützten Bereiche müssen gem. Art 8 Abs. 2 EMRK gesetzlich vorgesehen und in einer demokratischen Gesellschaft

- für die nationale Sicherheit und das wirtschaftliche Wohl des Staates,
- zur Aufrechterhaltung der öffentlichen Ruhe und Ordnung,
- zur Verhinderung strafbarer Handlungen,
- zum Schutz der Gesundheit und Moral und
- zum Schutze der Rechte und Freiheiten anderer

notwendig sein und dem Verhältnismäßigkeitsgrundsatz genügen.

Datengeheimnisaspekt des allgemeinen Datenschutzes: (§ 1 Datenschutzgesetz 2000; Art 8 EMRK)

Das Datenschutzrecht gewährt natürlichen und juristischen Personen zum Schutz des Privatsphäre, vor allem ein Recht auf Geheimhaltung personenbezogener Daten, soweit ein schutzwürdiges Interesse daran besteht. Dieses Recht kann insbesondere mit Zustimmung des Betroffenen oder zur Wahrung überwiegender berechtigter Interessen eines anderen eingeschränkt werden. Daneben treten die weiteren Rechte auf Auskunft, Richtigstellung und Löschung.

Besonderer Datenschutz: Recht auf Achtung des Brief- und Fernmeldegeheimnisses (Art 10 und Art 10a StGG; Art 8 EMRK)
Nach Art 10 StGG darf „das Briefgeheimnis nicht verletzt und die Beschlagnahme von Briefen, außer dem Falle einer gesetzlichen Verhaftung oder Hausdurchsuchung, nur in Kriegsfällen oder auf Grund eines richterlichen Befehls in Gemäßheit bestehender Gesetze vorgenommen werden“; Art 8 EMRK bestimmt, dass „jedermann...Anspruch auf Achtung seines Briefverkehrs“ hat. Die Beschlagnahme von Briefen ist demnach im Zuge einer Hausdurchsuchung, im Falle einer Verhaftung -und in Kriegsfällen immer und ohne richterlichen Befehl, sonst- soweit dies gesetzlich vorgesehen ist- nur auf Grund eines richterlichen Befehls.

Nicht verschlüsselte E-Mails fallen nach h.A. nicht unter den Schutz des Briefgeheimnisses. Bei verschlüsselten E-Mails kann man der Verschlüsselung durchaus den Charakter eines elektronischen Kuverts zukommen lasse.

An Stelle des Briefgeheimnisses tritt aber bei elektronischer Post das Fernmeldegeheimnis nach Art 10a StGG, das die Vertraulichkeit der über Fernmeldeanlagen vermittelten und nicht zur Kenntnisnahme durch Dritte bestimmten Kommunikation schützt. Eine Durchbrechung des Fernmeldegeheimnisses ist nur auf richterlichen Befehl zulässig. Die Überwachung des Fernmeldeverkehrs ist in den §§ 149a ff StPO geregelt, wonach das Abhören einer Telephonanlage nur zum Zweck der Aufklärung schwerer Straftaten zulässig ist und eines gerichtlichen Beschlusses bedarf. Dasselbe gilt für das Lesen von E-Mails.
Einschränkungen: nur nach Maßgabe des Art 8 Abs. 2 zulässig.

Grundrecht der Meinungsäußerungsfreiheit (Art 13 StGG iVm Art 10 MRK)

Nach dem Wortlaut des Art 13 StGG haben alle Menschen das Recht, durch Wort, Schrift, Druck oder auch durch bildliche Darstellung ihrer Meinung innerhalb der gesetzlichen Schranken frei zu äußern. Die Presse darf weder unter Zensur gestellt, noch durch ein Konzessionssystem beschränkt werden. Art 10 EMRK gewährleistet allen Menschen die freie Meinungsäußerung einschließlich der Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen.

Geschützt werden die Freiheit, sich eine Meinung zu bilden, sowie- grenzüberschreitend- die Freiheit der Mitteilung („aktive Informationsfreiheit“) und die Freiheit, Mitteilungen zu empfangen („passive Informationsfreiheit“).
Die Garantie des Art. 10 erstreckt sich sowohl auf den Inhalt als auch die Form von Kommunikation. In offenen Netzwerken können Gedanken und Meinungen unbemerkt abgefangen und verändert werden, so dass es dem Empfänger nicht mehr möglich ist eine Äußerungen sicher einer bestimmten anderen Person zuzuordnen. Dies kann nur durch die Verwendung digitaler Signaturen erreicht werden. Art. 10 gewährt außerdem das Recht von der Äußerung gegenüber anderen abzusehen (negative Meinungsäußerungsfreiheit). Soll also verhindert werden, daß Dritte den Kommunikationsvorgang mitverfolgen können, ist es nötigen diesen zu verschlüsseln. Der Schutzbereich von Art. 10 EMRK ist demzufolge eröffnet.

Art. 10 EMRK wird nicht schrankenlos gewährt, staatliche Eingriffe sind nach den Verhältnismäßigkeitsgrundsatz zu beurteilen.

Verhältnismäßigkeitsgrundsatz: Schranke für den Gesetzgeber,
Der Verhältnismäßigkeitsgrundsatz stellt eine Schranke für den einfachen Gesetzgeber dar. Dieser wurde vom VfGH entwickelt und wird von diesem bei der Prüfung von Grundrechten mit Gesetzesvorbehalt angewendet.
Wobei die Prüfung nicht einheitlich, sondern differenziert nach einzelnen Grundrechten erfolgt.
Eine Verhältnismäßigkeitsprüfung sollte folgende Prüfungsschritte umfassen:

- Liegt die Regelung im öffentlichen Interesses?
- Geeignetheit der vom Gesetzgeber getroffenen Regelungen zur Erreichung des (im öffentlichen Interesse liegenden) Zieles

- Erforderlichkeit: ist die Regelung das „gelindeste“ Mittel zur Erreichung dieses Zieles, d. h. jenes Mittel, das die Grundrechtsposition am wenigsten einschränkt?
- Angemessenheit („Verhältnismäßigkeit im engeren Sinn“): zwischen dem öffentlichen Interesse und der durch den Eingriff verkürzten Grundrechtsposition muss eine angemessene Relation bestehen; insofern ist eine Güterabwägung vorzunehmen.

Diese Frage, ob durch staatliche Regulierungsmaßnahmen eine Grundrechts-verletzung stattfindet, abschließend zu beantworten ist ohne das Vorliegen eines konkreten Regulierungsmodells nur schwer möglich.

Conclusio

Kryptographische Verfahren helfen dabei, Grundrechte des Persönlichkeitsschutzes im Internet durchzusetzen, indem sie Nachrichteninhalte gegen unbefugte Kenntnisnahme schützen, eine Identitäts- und Authenzitätsprüfung für elektronische Unterschriften ermöglichen und einen Grad an Anonoymität schaffen, der die spurlose Verwendung von elektronsichen Zahlungsmitteln erlaubt oder die Aufzeichnung von personenbezogenen Daten und deren Verdichtung zu einem Perönlichkeitsprofil verhindert.

Die Schattenseite besteht darin, dass Kriminelle ebenfalls von diesem Schutz der Anonymisierung profitieren. Ein Verbot von Kryptographie würde diese nicht daran hindern, das Netz weiterhin geheim und unbemerkt für ihre Machenschaften nutzen zu können, da es noch immer die Möglichkeit gäbe, verschlüsselte Nachrichten zu verstecken (Steganographie) oder zu überschlüsseln. Und es sollte verwundern, wenn dies den politischen Entscheidungsträgern nicht ebenfalls bewusst wäre.

Abschließend noch eine politische Bemerkung: staatliche Ermittlungsbehörden haben schon des öfteren mangelhafte Sensibilität gegenüber Grundrechten der BürgerInnen an den Tag gelegt. Der Umgang mit vertrauenswürdigen Daten von Seiten einiger Verantwortlicher in den vergangenen Jahren führt mindestens zu einer gewisse Grundvorsicht gegenüber Maßnahmen, die Eingriffe in Grundrechte gesetzlich absichern wollen.