LIFIS ONLINE [20.11.13]
www.leibniz-institut.de
ISSN 1864-6972

Falk Peters[1]

Data Leakage Prevention zum Zweck des Datenschutzes

– Eine vergleichende Betrachtung zweier Bedrohungsszenarien, den Datenschutz sowie die Erwägung möglicher Abwehrmaßnahmen betreffend

Der Irrsinn ist bei Einzelnen etwas Seltenes,
aber bei Gruppen, Parteien, Völkern und
Zeiten die Regel.
(Friedrich Nietzsche)

1. Data Leakage – was ist das?

Ob geheimdienstliche Spionage, Wirtschaftsspionage oder nur personenbezogenes Profiling – der Ansatz der Ausspähung ist stets derselbe: Weil Daten in IT-Systemen gespeichert und über Netze übertragen werden, konzentriert sich jegliche Ausspähung darauf, sog. Datenlecks (Data Leaks) anzuzapfen. Darunter sind Schnittstellen, Kanäle und Medien zu verstehen, mittels derer man Daten jedweder Art – in aller Regel unentdeckt – 'absaugen', an jeden beliebigen Ort der IT-Welt übermitteln und zu beliebigen Zwecken verwenden kann. Wie die Autoren Heinrich Kersten (T-Systems) und Gerhard Klett (BASF IT Services) in ihrem Buch *'Data Leakage Prevention'* (erschienen 2013) erklären, handelt es sich bei der Ausspähung in der Regel um individualisierte Angriffe von 'außen', bestehend aus Kombinationen technischer Methoden und dem Ausnutzen typisch menschlicher Schwächen. Die Hauptursachen für Data Leakage sind demnach die zunehmende Verbreitung von Schadsoftware (Malware) und der 'Faktor Mensch'.[2]

Im Folgenden werden zwei Bedrohungsszenarien, die durch Data Leakage gekennzeichnet sind, aus der Sicht des Datenschutzes betrachtet, nämlich zunächst die internationale Datenspionage (siehe unter 2.) und sodann der unverschlüsselte De-Mail-Betrieb in Deutschland (siehe unter 3.). Anhand des Vergleichs der unterschiedlichen, aggressiven Wucht beider Szenarien, also eines *internationalen* und eines *nationalen* Szenarios, soll verdeutlich werden, ob und inwieweit ihnen der Datenschutz überhaupt entgegenzuwirken vermag bzw. wann es sich um ein aussichtsloses Unterfangen handelt.

---

1 Der Autor ist promovierter Rechtsanwalt in Berlin, Lehrbeauftragter für Rechtsinformatik an der Brandenburgischen Technischen Universität Cottbus-Senftenberg und Verfasser zahlreicher Veröffentlichungen zu technikbezogenen Rechtsmaterien.

2 vgl. Kersten, Heinrich; Klett, Gerhard: Data Leakage Prevention, Verlagsgruppe Hüthig Jehle Rehm GmbH, Heidelberg 2013, S. 24

2. Bedrohungsszenario: Internationale Datenspionage

Vergegenwärtigen wir uns noch einmal die große internationale Ausspähung ECHELON und CARNIVORE: Diese Überwachungsprojekte waren in der politischen Berichterstattung schon seit Langem Fanale der IT-gestützten US-amerikanischen Überwachungsoffensive nach dem 11. September 2001 unter Führung des US-Nachrichtendienstes NSA. Doch erst durch die 2013 erfolgten Enthüllungen des Edward Snowden zu PRISM und TEMPORA und dem daraufhin mehr oder weniger systematischen Entdecken oder gar nur zufälligen Bekanntwerden von Art und Ausmaß der Datenspionage wurde dem kritischen Bürger vollends klar, dass bei rechtlich unkontrolliertem Einsatz derartiger Überwachungssysteme alles und alle einer Ausforschung ausgesetzt sind, die von sich aus vor keiner rechtlichen Schranke halt macht, und die sich schon jetzt auf dem Weg in einen sinnlich nicht wahrnehmbaren und daher umso gefährlicheren globalen Totalitarismus befindet.

Den Akteuren auf diesem Weg – allen voran die sog. Five Eyes: USA, Kanada, Großbritannien, Australien und Neuseeland, im Gefolge aber durchaus alle IT-potenten Staaten (darunter auch Deutschland, s.u.) – wird es auch noch leicht gemacht, und zwar durch den Medienwahn der breiten Massen, die das trügerische Universum der digitalen bzw. virtuellen Welt mit dem Internet als Hauptsache nicht als solches zu begreifen vermögen und geradezu kritiklos, ja nahezu bewusstlos alle Angebote aus diesem Universum annehmen. Das Phänomen *'Big Data'* ist eine Ausgeburt dieser virtuellen Welt. Der Autor Rudi Klausnitzer (Kommunikationsagentur DMC) hat in seinem Buch *'Das Ende des Zufalls'* (erschienen 2013) gezeigt, wie Big Data uns und unser Leben vorhersagbar macht, und die Autoren Viktor Mayer-Schönberger (Oxford Internet Institut) und Kenneth Cukier (Data Editor of the Economist) schätzen in ihrem Buch *'Big Data: A Revolution That Will Transform How We Live, Work and Think'* (erschienen 2013) den Betrag der weltweit gesammelten Daten auf (nur vorläufige) 1,2 Zettabyt. Dabei entspricht 1 Zettabyte 1 Milliarde Terabytes. Mittlerweile verfügt die NSA in dem neuen Spionagezentrum in Bluffdale im Mormonenstaat Utah über einen Yottabyte-Speicher. Ein Yottabyte entspricht 1.000 Zettabytes.[3]

Weil es heute zudem technisch möglich ist, nahezu jede Kommunikation von jedem Ort der Welt aus zu belauschen, werden mit allen verfügbaren Mitteln Daten unmerklich entwendet, verarbeitet und mittels intelligenter Algorithmen genutzt – einerseits begründet mit nationalen Sicherheitsinteressen, also zwecks Garantie der eigenen homeland security, andererseits motiviert durch Wirtschaftsinteressen, z.B. zur Steigerung der Wettbewerbsfähigkeit der eigenen Unternehmen. So kann das 2004 in Dienst gestellte 138 m lange U-Boot *'USS Jimmy Carter'* am Meeresgrund unbemerkt Glasfaserkabel anzapfen,[4] was eine Revolution in der Geheimdienstwelt darstellt,[5] und wohl nicht zufällig stehen alle IT-Anbieter in den USA unter dem Generalverdacht, eng mit der NSA beim Datenabsaugen zu kooperieren.[6]

Vergegenwärtigen wir uns aber auch die Situation in Deutschland. Der ehemalige NSA-Direktor Michael Hayden betonte in einer Fernsehsendung, diejenigen Europäer, die die internationale Spionage durch die NSA so lebhaft beklagten, sollten doch zunächst nachfragen, was eigentlich ihre eigenen Regierungen tun.[7] Dazu passend zitierte ein führendes deutsches Nachrichtenmagazin auf der Titelseite – bezogen auf die NSA-Aktivitäten – Edward Snowden mit den Worten "Die stecken

3 vgl. http://www.conspirare.net/w2/nsa-yottabyte-speicher-bluffdale-kein-bluff-sondern-...
4 vgl. http://de.wikipedia.org/wiki/USS_Jimmy_Carter_(SSN-23)
5 vgl. Wirtschaftswoche Nr. 28 v. 08.07.13, S. 58
6 vgl. Wirtschaftswoche Nr. 38 v. 16.09.13, S.70
7 vgl. Cicero 8.2013, S. 65

unter einer Decke mit den Deutschen".[8] Diese Behauptung Snowdens trifft mit an Sicherheit grenzender Wahrscheinlichkeit zu, denn Bundesregierung und Bundestag waren durch den Präsidenten des Bundesnachrichtendienstes darüber informiert, dass die NSA in Wiesbaden ein neues Abhörzentrum baut,[9] das Bundesamt für Verfassungsschutz räumte ein, dass es – ebenso wie der BND – Spionageprogramme der NSA testet, der BND, der bei der Entwicklung von Internetspionage-Technik in Europa sogar führend sein soll,[10] setzte sich gleichzeitig für eine laxere Auslegung deutscher Datenschutzgesetze ein, um den Austausch von Spionagesoftware zu erleichtern.[11] Und überhaupt bauen deutsche Behörden die Überwachung durch heimliches Anzapfen von Telefonleitungen immer weiter aus und dies sogar bei Berufsgruppen, die einer gesetzlichen Schweigepflicht unterliegen.[12]

Interessant ist in diesem Zusammenhang: Facebook veröffentlichte einen Bericht, in dem das soziale Netzwerk aufschlüsselt, aus welchem Land wie viele Anfragen nach Nutzerdaten von Seiten der Regierungsbehörden eingingen. Im ersten Halbjahr 2013 nahmen die USA die erwartete Spitzenreiterposition ein. Doch auch Deutschland hält sich nicht zurück, seinen Bürgern im Internet hinterher zu schnüffeln. Deutschland liegt auf Platz 4.[13] Also: Kein IT-potentes Land braucht auf ein anderes als alleinigen Bösewicht zu zeigen; alle stehen im Kampf um einen der wichtigsten Rohstoffe der Zukunft: Daten.

2.1 Im Fokus der Debatte: Der Datenschutz

Die Enthüllungen des Edward Snowden haben Datenschutzpolitiker, professionelle Datenschützer und am Datenschutz interessierte Medien in Scharen auf den Plan gerufen, denn alle wissen: Letztlich geht es bei jeder Überwachung um die Ausforschung vergangenen bzw. aktuellen menschlichen Verhaltens zwecks Möglichkeit der Prognose oder gar der Manipulation künftigen menschlichen Verhaltens,[14] was durch den Datenschutz ja gerade verhindert werden soll. Alle im Deutschen Bundestag vertretenen Fraktionen reagierten folglich empört auf solch massive Verletzung des Datenschutzes,[15] einige FDP-Minister wollten eine UN-Initiative für den Datenschutz starten,[16] der Bundesdatenschutzbeauftragte forderte klare Grenzen für die nachrichtendienstliche Überwachung[17], das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein forderte ein Grundrecht auf Datenschutz zumindest in der westlichen Welt[18], ein Presseorgan konstatierte, der 'Verrat' des Edward Snowden sei Bürgerpflicht[19], teilweise wurde sogar von der Kernschmelze der Demokratie gesprochen,[20] und der frühere amerikanische Präsident Jimmy Carter äußerte, Amerika habe derzeit keine funktionierende Demokratie.[21]

---

8 vgl. DER SPIEGEL Nr. 28 v. 08.07.13, Titelblatt
9 vgl. http://www.t-online.de/nachrichten/specials/id_64544236/nsa-baut-neues-abhoerzentr..
10 vgl. http://www.t-online.de/nachrichten/specials/id_66315064/gcgq-und-bnd-kooperierten-
11 vgl. http://www.t-online.de/nachrichten/specials/id_64604904/spionage-skandal-erreicht-d..
12 vgl. Berliner Morgenpost v. 15.07.13, S. 2; DER SPIEGEL Nr. 41 v. 07.10.13, S. 50 (zur telefonischen Überwachung von Strafverteidigern)
13 vgl. http://www.t-online.de/computer/internet/facebook/id_65180142/facebook-bericht-ue...
14 vgl. Fn. 3, S. 3
15 vgl. Newsletter Behörden Spiegel Nr. 466, Sondernewsletter zur Abhör-Affäre v. 11. 07. 13, S. 2 und 4-7
16 vgl. Berliner Morgenpost v. 24.07.13, S. 2
17 vgl. Newsletter Behörden Spiegel Nr. 466, Juli 2013, S. 3
18 vgl. Newsletter E- Government Behörden Spiegel Nr. 612, Juli 2013, S. 6
19 vgl. Cicero 8.2013, S. 48
20 http://www.t-online.de/nachrichten/specials/id_66322138/claudia-roth-will-wegen-nsa...
21 vgl. http://www.t-online.de/nachrichten/specials/id_64537950/usa-ex-praesident-jimmy-ca.

Der Unmenge von Kommentaren, Stellungnahmen usw. zu PRISM, TEMPORA & Co., von denen dieser Beitrag nur wenige in Bezug nehmen kann, lässt sich eines entnehmen: Die öffentliche Meinung wertet ganz überwiegend die vorstehend kurz skizzierten Überwachungsaktivitäten als Angriff auf Rechtsstaat und Demokratie.

Der analysierende Jurist präzisiert dahin gehend, dass es bei den bekannt gewordenen Überwachungspraktiken um die Verletzung der höchsten Verfassungswerte geht, nämlich der Menschenwürde und der persönlichen Freiheit, deren Inbegriff im digitalen Zeitalter der Datenschutz ist, und dass auch bei der Abwägung von öffentlicher Sicherheit und Datenschutz – wie bei jeder Güterabwägung – das *Verhältnismäßigkeitsprinzip* gewahrt bleiben muss.[22]

2.2 Globale Macht der IT – regionale Geltung und Auslegung des Datenschutzrechts

Der Datenschutz ist 'traditionell' *national* geregelt. Die bisher einzige internationale Datenschutzregelung ist – soweit bekannt – die Datenschutzrichtlinie 95/46/EG der Europäischen Union aus dem Jahre 1995. In der deutschen Datenschutzpolitik herrscht daher durchaus die Vorstellung vor – das zeigt sich auch in den unter 2.1 erwähnten Reaktionen von Datenschützern auf PRISM und TEMPORA –, man könne durch weitere internationale Harmonisierung des Datenschutzrechts die internationale Datenspionage kontrollierbar machen und den genannten Überwachungspraktiken vorbeugen.

Diese Vorstellung ist zum einen politisch naiv, denn jeder internationale Datenschutzpolitiker weiss, welch unsägliche Mühe und Geduld es kostet, das Datenschutzrecht zu inter- nationalisieren, und wie kompromissverdorben sodann das Ergebnis ist. Ein überzeugendes Beispiel dafür ist die beabsichtigte EU-Datenschutzgrundverordnung, die im Januar 2012 von der EU-Kommission nach jahrelangen Beratungen zwischen den Mitgliedstaaten vorgeschlagen wurde, und deren Verabschiedung wegen der vielen beteiligten Interessen sich zu Lasten der Klarheit bzw. Wirksamkeit der Datenschutzregeln immer weiter verzögert, wie die EU-Justizkommissarin enttäuscht feststellen musste.[23]

Zum anderen ist der Glaube an rechtliche Datenschutzregeln aber auch von einem juristischen bzw. rechtstheoretischen Standpunkt aus naiv, denn das Datenschutzrecht wurde seit jeher – national wie international – mehr als politische Zeichensetzung denn als konkrete Regelung von IT-bezogenen Sachverhalten verstanden, geriet somit zu fast rein symbolischem Recht und ist daher extrem auslegbar.[24] So versteht denn jeder unter Datenschutz, was er darunter verstehen will und begrenzt die Reichweite des Datenschutzes so, wie es ihm passt. Diese Feststellung wird durch das oben erwähnte Ansinnen des BND, das Datenschutzrecht laxer auszulegen, nahezu bestätigt.

2.3 Data Leakage Prevention bei internationaler Datenspionage – Vorschläge, Ratschläge, Handlungsempfehlungen

Namhafte deutsche Organisationen, die mit der digitalen Welt üblicherweise in Verbindung gebracht werden, ließen mit ihren Reaktionen auf PRISM, TEMPORA & Co. nicht auf sich warten,

---

22 So z.B. der Bundesbeauftragte für den Datenschutz, s. Fn 14; desgleichen Clemens Binninger MdB, Innenausschuss des Deutschen Bundestages, vgl. Fn. 15, S. 5

23 vgl. http://www.telemedicus.info/article/2584-EU-Datenschutzverordnung-vorerst-auf-Eis..

24 Ausführlich dazu Peters, Falk: Verfassungsgerechter Datenschutz in der digitalen Gesellschaft, LIFIS ONLINE [29.06.10], http://www.leibniz-institut.de/archiv/peters_29_06_10.pdf

allen voran die Deutsche Telekom, der Bundesverband IT-Sicherheit e.V. (TeleTrust) und der BITKOM.

2.3.1 Deutsche Telekom

Die erste – wohl marketinggetriebene – Reaktion der Deutschen Telekom AG nach Bekanntwerden der geschilderten Überwachungspraktiken war der Vorschlag einer *E-Mail made in Germany*. Die Telekom und ihre Preiswertpartner gmx.de und web.de versprachen, den E-Mail-Verkehr innerhalb Deutschlands mit einem SSL-Protokoll zu verschlüsseln und die Daten nur noch innerhalb von deutschen Rechenzentren zu hosten. Sodann regte der Telekom-Vorstand für Datenschutz eine gesetzliche Regelung für ein 'National Routing' von E-Mails und anderen Datenpaketen zwecks Meidung der in Verruf geratenen Internet-Knotenpunkte in Großbritannien und in den USA an.[25]

2.3.2 Bundesverband IT-Sicherheit

Auch der Bundesverband IT- Sicherheit e. V. sah sich zu einer konstruktiven Stellungnahme genötigt. Er forderte die amtierende Bundesregierung zur Erarbeitung und Umsetzung einer nationalen *Security Roadmap* auf und sprach dabei eine Reihe von Handlungsempfehlungen aus, nämlich:

- hinsichtlich eines hohen IT-Sicherheitsniveaus
  - Verpflichtung zur Einhaltung branchenspezifischer IT-Sicherheitsstandards in kritischen Infrastrukturen,
  - Nationales Routing der nationalen Kommunikationsverkehre (z.B. IP, E-Mail, Voice),
  - Definition messbarer Sicherheitsziele für Deutschland (z.B. Domänenzertifizierung, E-Mail-Verschlüsselung).
- hinsichtlich der Stärkung der Evaluierungskapazitäten von IT-Sicherheitsprodukten
  - Überprüfung der Produkthaftung für IT-Sicherheitsmängel,
  - Aufbau von zertifizierten IT-Sicherheitsdienstleistern zur Bewertung von IT- Sicherheits- produkten,
  - Ausbau des Bundesamtes für Sicherheit in der Informationstechnik zur kompetenten Begleitung der Digitalisierung der Gesellschaft durch verstärkte Beratungs- und Zertifizierungskapazitäten,
  - Ausbau der Deutschen IT-Sicherheitswirtschaft.
- hinsichtlich der Flankierung bei der Bereitstellung von Risikokapital für IT-Sicherheits-unternehmen
  - stärkere Berücksichtigung nationaler IT-Sicherheitsinteressen bei öffentlichen Vergaben.[26]

2.3.3 BITKOM

Schließlich bezog auch der BITKOM nach gründlichen Beratungen zu den geschilderten Ausspähungen Position und formulierte folgende Vorschläge bzw. forderte Regierungen, Kontrollgremien der Parlamente und die zuständigen Aufsichtsbehörden zu folgenden Maßnahmen auf.

---

25 vgl. Wirtschaftswoche Nr. 42 v. 14.10.13, S. 8

26 vgl. Newsletter E-Government BehördenSpiegel Nr. 628, Oktober 2013, S. 2

1 Schnellstmögliche Herstellung von Transparenz hinsichtlich der Aktionen von Geheimdiensten und Sicherheitsbehörden betreffend den Umfang und die Details von Abhörmaßnahmen, die dafür vorhandenen Rechtsgrundlagen in den jeweiligen Ländern, die Umsetzung dieser Rechtsgrundlagen in die Praxis und die vorgesehenen Kontrollmechanismen.

2 Schaffung von Rechtssicherheit durch internationale Übereinkommen zur Zusammenarbeit von Unternehmen mit Sicherheitsbehörden und Datenschutz, z.B. durch ein Antispy-Abkommen und durch möglichst schnelle Verabschiedung der EU-Datenschutz-Grundverordnung.

3 Europaweiter Schutz der EU-Bürger vor Ausspähung durch Entwicklung eines gemeinsamen Ansatzes für die Aktivitäten der Geheimdienste der Mitgliedstaaten zwecks Wahrung der verfassungsrechtlich garantierten Rechte auf das Fernmeldegeheimnis und auf informationelle Selbstbestimmung.

4 Legitimation und Bestimmung des Umfangs nachrichtendienstlicher Überwachung durch Findung einer Balance zwischen der Sicherheit auf der einen und der Freiheit des einzelnen sowie der Berufsausübungsfreiheit der betroffenen Unternehmen auf der anderen Seite.

5 Prüfung der technischen Möglichkeiten im Bereich des Routings im nationalen Raum und im Schengen-Raum als Beitrag zum Datenschutz und zur Datensicherheit.

6 Errichtung eines nationalen Rats – ähnlich dem Nationalen Ethikrat – zur ständigen Begleitung der Frage des Verhältnisses von Freiheit und Sicherheit, von Anonymität und Verantwortung, um Orientierungshilfe bei der Weiterentwicklung der digitalen Welt und bei der Ausformulierung des entsprechenden Rechtsrahmens und seiner Umsetzung geben zu können.

7 Schutz von Unternehmensgeheimnissen vor Wirtschaftsspionage durch Schaffung entsprechender straf- und zivilrechtlicher Vorschriften auf nationaler und internationaler Ebene, durch internationale Ächtung der Wirtschaftsspionage aufgrund eines entsprechenden Abkommens und durch die Verpflichtung zum Einsatz zeitgemäßer IT-Sicherheitstechnologien, sowohl bei der Festnetz-Kommunikation als auch bei der mobilen Kommunikation.

8 Stärkung der Sicherheitskultur in Deutschland sowohl bei Unternehmen als auch bei Verbrauchern, z.B. Erhöhung der Medienkompetenz durch Vermittlung insbesondere informationstechnischer Kenntnisse in Schulungen oder sonstigen Weiterbildungsmaßnahmen.

9 Entwicklung und Umsetzung einer Strategie zur Stärkung des IT-Standorts Deutschland zwecks Nutzung der Chancen, die sich mit der Digitalisierung für den Standort Deutschland verbinden.[27]

2.4 Sind die vorgeschlagenen Maßnahmen zur Data Leakage Prevention bei internationaler Datenspionage tauglich?

So gut gemeint alle vorstehend genannten Vorschläge, Ratschläge und Handlungs- empfehlungen sein mögen, so problematisch wird ihre Befolgung bzw. Umsetzung in der Praxis sein.

Bei den *technikbezogenen* Vorschlägen handelt es sich – jedenfalls teilweise – um Maßnahmen, deren Realisierung fraglich bleiben muss. Was insbesondere das National Routing betrifft, so halten Experten es für de facto unmöglich, im Internet zu klären, wo Datenströme – ob national oder international – geroutet werden.[28]

---

27 vgl. BITKOM-Positionspapier zu Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden, Datenschutz und Datensicherheit v. 31.10.13, s. web-Seite des BITKOM

28 vgl. Newsletter E-Government Behörden Spiegel Nr.626, Oktober 2013, S. 5

Bei den *rechtlichen* Vorschlägen auf nationaler Ebene wird es bezüglich deren verbindlicher Fixierung Interessengegensätze geben, die selbstverständlich jeweils rechtlich begründet werden, die aber das Zu-Stande-Kommen etwa einer verbindlichen Security Roadmap auf unabsehbar lange Zeit verhindern werden. Bestes Beispiel insoweit ist die Vorbereitung eines IT-Sicherheitsgesetzes mittels einer IT-Sicherheitsleitlinie durch den IT-Planungsrat, die sich schon bisher über drei Jahre hinzieht und die sich möglicherweise über insgesamt acht Jahre hinziehen wird.[29]

Bei den *völkerrechtlichen* Vorschlägen stellt sich darüber hinaus noch das Problem der Durchsetzbarkeit der getroffenen Vereinbarungen.

Schließlich darf auch das persönliche Qualitätsproblem nicht vergessen werden, das bei den verantwortlichen Funktionären in Regierungen und Parlamenten nach wie vor vorhanden ist, denn dort wimmelt es von *digital greenhorns*, denen auch durch die Beratung von Seiten der ihnen unterstellten *digital natives*, die zur Bewältigung der Probleme in der digitalen Welt unverzichtbar sind,[30] nicht geholfen werden kann, denn jeder Beratene braucht ein Mindestmaß an Vorverständnis vom Beratungsgegenstand, damit die Beratung fruchtet.

2.5 Die Konsequenzen für den internationalen Datenschutz

Nachdem seit dem Sommer 2013 immer neue Einzelheiten des Ausmaßes der internationalen Datenspionage bekannt wurden (z.B. systematisches Knacken oder Umgehen von Verschlüsselungen im Internet, Auslesen von SIM-Karten, Lauschangriffe per Trojaner, massenhafte Infizierung von Computern, Abhören der Telefonate beliebiger Personen einschließlich hoher Funktionäre in Politik, Wirtschaft, Wissenschaft usw., monatelange Speicherung der Inhalte der Telefonate in riesigen Datenbanken und Auswertung derselben in Berichten zwecks persönlichen Profilings)[31], konnte man nicht mehr umhin zuzugeben, dass sowohl in rechtlicher wie in technischer Hinsicht keinerlei taugliche Mittel vorhanden sind, um die Aktivitäten von Geheimdiensten in die demokratische Gesamtstaatlichkeit einzubinden und zu verhindern, dass Geheimdienste ein unkontrolliertes Eigenleben entfalten.[32] Was somit den internationalen Datenschutz betrifft, muss man sich über das Folgende im Klaren sein.

Angesichts der Hilflosigkeit der Experten bei ihren juristischen und sicherheitstechnischen Vorschlägen zur Kontrolle internationaler Spionageaktivitäten – die Ratlosigkeit wird insbesondere durch die Abstraktheit aller gemachten Vorschläge, Ratschläge und Handlungsempfehlungen deutlich – kann man den internationalen Datenschutz getrost vergessen, weil alle bisherigen Vorschläge, ihn international zu realisieren, Versuche mit untauglichen Mitteln sind. Folglich besteht auch weiterhin für diejenigen, denen ein hohes rechtliches Datenschutzniveau in ihrem eigenen Land im Wege ist, die Möglichkeit, ihre personenbezogene Datenverarbeitung in anderen Ländern abzuwickeln, die kein oder ein nur geringes Datenschutzniveau vorzuweisen haben.

---

29 vgl. BehördenSpiegel Berlin und Bonn, April 2013, S. 17

30 vgl. Newsletter Netzwerk Sicherheit BehördenSpiegel Nr.471, August 2013, S. 2; Newsletter E-Government BehördenSpiegel Nr. 615, Juli 2013, S. 7

31 vgl. http://www.t-online.decomputer/sicherheit/id_66311506/nsa-prism-tempora-so-fange..

32 vgl. BehördenSpiegel Berlin und Bonn, August 2013, S. 1

3. Bedrohungsszenario: Der unverschlüsselte De-Mail-Betrieb in Deutschland

Immerhin handelt es sich hierbei um ein Bedrohungsszenario, das sich – im Unterschied zum Bedrohungsszenario der internationalen Datenspionage – im Geltungsbereich eines *einheitlichen* Rechts abspielt und das wohl auch weniger komplex ist, solange man die aggressive Datenspionage von außen außer Betracht lässt und nur den Fall betrachtet, dass der De-Mail-Diensteanbieter von sich aus – vorsätzlich oder fahrlässig – das Datenschutzrecht verletzt, indem er sich selbst zum Datenleck macht.

Die Etablierung von De-Mail-Diensten als Basis einer zuverlässigen und geschützten Kommunikations-Infrastruktur ist Teil der High-Tech-Strategie der Bundesregierung, namentlich des e-government-Programms 2.0 und des 12-Punkte-Plans für ein bürgerfreundliches Deutschland. Es wird federführend vom BMI in Zusammenarbeit mit einer Reihe öffentlicher Institutionen sowie privater Organisationen und Unternehmen durchgeführt. Die erste Pilotierung fand ab 2009 in Friedrichshafen statt und ist mittlerweile erfolgreich abgeschlossen.[33] Auch Pilotprojekte mit rein kommunalem Bezug scheinen erfolgreich zu sein, wie z.B. der De-Mail-Praxistest in der Städte-Region Aachen gezeigt hat.[34] Und am 6. März 2012 erhielten auf der CeBIT 2012 die ersten drei Anbieter von De-Mail-Diensten – die Firmen Deutsche Telekom, T-Systems und MentanaClaimsoft – vom BSI ihre Zulassung als De-Mail-Anbieter in Deutschland. Damit konnte die flächendeckende Einführung von De-Mail in Deutschland beginnen.[35] Datenschutzrechtlich bemerkenswert ist: Eine Ende-zu-Ende-Verschlüsselung der De-Mail war im De-Mail-Gesetz von Anfang an nicht vorgesehen.

3.1 Datenschutzrechtliche Bedenken im Gesetzgebungsverfahren

Bei der Anhörung von Sachverständigen zum De-Mail-Gesetz wurde insbesondere bei der Diskussion über das Fehlen einer gesetzlichen Verpflichtung des Diensteanbieters auf eine Ende-zu-Ende-Verschlüsselung der De-Mail der Verdacht laut, dass auf diese Weise das Post- und Fernmeldegeheimnis unmerklich unterlaufen werden könne und dass es gar möglich sein werde, die im De-Mail-Postfach liegende Post, ob sie nun geöffnet ist oder nicht oder ob sie als zugestellt gilt oder nicht, Geheimdiensten und Polizei ohne richterliche Anordnung zugänglich zu machen.[36] Der Verdacht war durchaus gerechtfertigt vor dem Hintergrund der Tatsache, dass der Bundesnachrichtendienst schon seit Langem – gestützt auf den sehr auslegbaren Art. 5 Abs. 2 G 10 – E-Mails mittels Suchbegriffen systematisch filtert und damit massiv in Grundrechte eingreift – das Ganze abgesegnet durch die Geheimdienst- kontrolleure des Deutschen Bundestages.[37]

3.2 Vertrauen ist gut – Kontrolle ist besser

Setzt sich die De-Mail flächendeckend durch – und davon ist auszugehen –, so läuft das auf einen einheitlichen, staatlich überwachten Kommunikationsraum hinaus, dessen Vorteil die hohe Sicherheit gegenüber Datenkriminellen ist. Aber ist dieser Raum – durch die Brille des Datenschutzes besehen – auch vertrauenswürdig? Zweifel sind angebracht, wenn man sich die De-Mail-Organisation genauer anschaut.

---

33 https://www.bsi.bund.de/DE/Themen/EGovernment/DeMail/DeMail_node.html
34 vgl. Kommune 21-2/2012, S.44 f.
35 http://www.CIO.bund.de/SharedDocs/Kurzmeldungen/DE/2012/20120306_demail_einfuehrung.html
36 vgl. Deutscher Bundestag, 17. Wahlperiode, Innenausschuss – Protokoll 17/31, S.18 f. et passim
37 http://www.cr-online.de (Blog>Niko Härting>28.02.2012: Massive Eingriffe in Grundrechte – BND filtert systematisch E-Mails)

Das Hauptproblem ist die Koppelung von De-Mail-Gesetz[38] und BSI-Gesetz[39]. Gemäß § 2 des De-Mail-Gesetzes ist die zuständige Behörde nach diesem Gesetz das BSI, das nach § 1 des BSI-Gesetzes dem BMI untersteht. Das BSI hat damit die Rechts- und die Fachaufsicht über die De-Mail-Diensteanbieter. Wie es diese Aufsicht ausübt, ergibt sich aus seinem Aufgabenprofil gemäß § 3 und seiner Vorgabenbefugnis gemäß § 8 des BSI-Gesetzes. Hält man sich im Bewußtsein, dass es – wie oben (s. unter 1. vorletzter und letzter Absatz und 3.1) dargestellt – auch deutsche Behörden mit dem Datenschutz häufig nicht hinreichend genau nehmen, so wird der Wunsch verständlich, nicht vom Wohlverhalten der De-Mail-Diensteanbieter bzw. ihrer Vorgesetzten abhängig sein zu wollen, sondern sich selbst – wenigstens stichprobenartig – davon überzeugen zu können, dass alles mit rechten Dingen zugeht.

3.3 Data Leakage Prevention beim De-Mail-Diensteanbieter – das geht!

Beschränken wir uns also im Folgenden – gemäß der 'klassischen Problemlage' beim Datenschutz – auf die Betrachtung des Falles, dass der De-Mail-Diensteanbieter selbst das Datenleck ist.

Wenn man heutzutage von Informationskontrolle zwecks Datenschutzes spricht, wird immer häufiger das Opt-in-Verfahren genannt. Das ist in diesem Zusammenhang ein Verfahren, bei dem der Betroffene die Art und Weise des Umgangs mit seinen personenbezogenen Daten, also beabsichtigte Maßnahmen der Erhebung, Verarbeitung und Nutzung derselben, vorher bejahend oder verneinend bestätigt, was heutzutage meistens noch per E-Mail, SMS oder Telefon geschieht. Das Opt-in-Verfahren basiert also auf dem datenschutzrechtlichen Erlaubnistatbestand der Einwilligung des Betroffenen. Soll das Verfahren im massenhaften De-Mail-Verkehr eingesetzt werden und dabei praktikabel sein, muss es automatisiert werden. Dahin geht der folgende Vorschlag.[40]

– Eine Person P, die Kunde des De-Mail-Dienstleisters X ist, soll im Sinne der neuen Datenschutzziele der Transparenz, Nichtverkettbarkeit und Intervenierbarkeit die Möglichkeit erhalten, sich zu beliebiger Zeit davon zu überzeugen, was mit ihrer De-Mail samt den Verbindungsdaten geschieht, und gegebenenfalls einzuschreiten.

– Eine autorisierende Stelle A (am besten der für X zuständige Datenschutzbeauftragte) legt die Zweckbindung, also den Verwendungszeck Z bzw. die Verwendungszwecke Z1 – Zn, beim Umgang mit der De-Mail fest. Dazu modelliert A die Aufgaben, also die Befugnisse und Pflichten von X nach dem De-Mail-Gesetz sowie des BSI nach dem De-Mail-Gesetz und dem BSI-Gesetz, bis zur Eindeutigkeit, also mindestens zu semiformalen Spezifikationen, sodass diese sodann programmiert werden können.

– A stellt für X eine Chipkarte zur Verfügung mit
  a) einem üblichen Zertifikat zum Identitätsnachweis (mit einem öffentlichen und einem privaten Schlüssel zum Signieren und Verschlüsseln),
  b) einem Autorisierungszertifikat. Dieses enthält einen an den Zweck Z gebundenen öffentlichen Schlüssel.

– A führt eine öffentlich zugängliche Liste, die zu jedem erlaubten Zweck den zugehörigen öffentlichen Autorisierungsschlüssel enthält.

38 Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften v. 28. April 2011, BGBl. I 2011, S. 666

39 Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes v. 14. August 2009, BGBl. I 2009, S. 2821

40 Entnommen aus dem Beitrag von Falk Peters in: Peters, Falk; Kersten, Heinrich; Wolfenstetter, Klaus-Dieter: Innovativer Datenschutz, Verlag Duncker & Humblot, Berlin 2012, S. 166 ff.

– X sendet an P, mit deren De-Mail Dp gesetzeskonform umgegangen werden soll, unter Nennung der programmierten Z und der Autorisierung von Z durch A, die Nachricht, jegliche De-Mail Dp unter den genannten Voraussetzungen über X versenden zu können. X signiert diese Nachricht elektronisch.

– P besitzt ebenfalls eine Chipkarte, die seine Identität bestätigt und ihm die Möglichkeit zum elektronischen Signieren und Verschlüsseln gibt. P ist anhand der elektronischen Unterschrift von X in der Lage, die Identität von X zu verifizieren und anhand des Autorisierungszertifikats i.V.m. der von A bereitgestellten Liste (siehe 4**.** Aufzählungszeichen) die Autorisierung von X für den Verwendungszweck Z zu überprüfen und – entweder positiv oder negativ – zu bestätigen.

– Bei positiver Bestätigung verschlüsselt P nun zunächst die De-Mail Dp mit dem öffentlichen Autorisierungsschlüssel für den Verwendungszweck Z (das Ergebnis ist Dp') und mit dem öffentlichen Schlüssel von X (das Ergebnis ist Dp''). Er signiert anschließend Dp'' elektronisch und übermittelt diese De-Mail mit seinem Zertifikat an X.

– X kann durch Überprüfung der elektronischen Unterschrift feststellen, ob die De-Mail von P stammt und auf dem Transportweg nicht verändert wurde.

– Ist das der Fall, kann X durch Anwendung seines privaten Schlüssels anschließend die De-Mail Dp' zurückgewinnen. Niemand anders ist dazu in der Lage.

– X hat nun die Wahl zwischen zulässiger Verwendung (nämlich Z) und nicht zulässiger Verwendung (-Z). Dabei wird Z durch eine Software SWz repräsentiert (siehe 2. Aufzählungszeichen).

– Die De-Mail Dp' wird nun der Software SWz zur Verfügung gestellt. Zwischen der Software SWz und der Chipkarte von X läuft ein Authentisierungsprotokoll ab, sodass 'beide Seiten' erkennen können, dass die jeweils andere Seite die entsprechende Berechtigung besitzt. Der Einfachheit halber soll angenommen werden, dass das geheime Gegenstück zum öffentlichen Autorisierungsschlüssel (nämlich der private Autorisierungsschlüssel) für den Verarbeitungszweck Z in zwei Teile zerlegt worden ist: Eine Hälfte ist auf der Chipkarte von X mit dem Attribut Z gespeichert, die andere ist in der Software SWz integriert. Nur durch Zusammenwirken beider Hälften ist es möglich, die unverschlüsselte De-Mail Dp zu gewinnen.

– Die De-Mail Dp wird nunmehr durch SWz zulässigerweise verarbeitet.

– Vor irgendeiner Speicherung oder Übertragung muss die De-Mail Dp wieder verschlüsselt werden und zwar stets mit
  a) dem öffentlichen Autorisierungsschlüssel (hierfür benötigt die SWz die Chipkarte von X nicht) und
  b) dem öffentlichen Identitätsschlüssel von X (hierfür wird das entsprechende Zertifikat auf der Chipkarte benötigt).

Durch das Authentisierungsprotokoll ist damit sichergestellt, dass

– die De-Mail Dp nur von X gelesen werden kann,
– X sicher sein kann, dass die De-Mail tatsächlich von P kommt,
– X keine Chance hat, von dem Verwendungszweck Z bzw. von den Verwendungszwecken Z1 – Zn abzuweichen,
– Dritte keine Möglichkeit zu irgendeiner Verwendung von Dp haben.

Ergebnis: Die zweckgerechte Verwendung der De-Mail ist damit gegeben.

Erläuterung
Das vorstehend vorgeschlagene technisch-organisatorische Verfahren basiert auf einer sog. *Public Key Infrastructure* (PKI). Die autorisierende Stelle A hat die Funktion eines Trustcenters. Da es um die datenschutzgerechte Zweckbindung des Umgangs mit der De-Mail geht, muss der Datenschutzbeauftragte diese Trustcenter-Funktion übernehmen. Das BSI kommt dafür nicht infrage, weil es zu den zu kontrollierenden Akteuren gehört. Ebenso wenig die BNetzA, weil sie nur für Netzregulierungen am Markt zuständig ist. Allerdings muss der Datenschutzbeauftragte technisch, personell und finanziell weitaus besser ausgerüstet werden, um die interdisziplinären Aufgaben zwischen den beiden staatstragenden Säulen Recht und Informationstechnik wissenschaftlich optimal wahrnehmen zu können.
Selbstverständlich funktioniert auch das vorstehend vorgeschlagene PKI-Verfahren nur dann fehlerfrei, wenn es keinen Angriffen von außen, also keiner Datenspionage ausgesetzt ist.

4. Zur Ohnmacht des klassischen Rechts in der digitalen Welt

Vor mehr als einem halben Jahrhundert hat der Staatsrechtler Forsthoff in seinem berühmten Vortrag *'Der Jurist in der industriellen Gesellschaft*' ausgeführt: "Mit den Augen des Technikers gesehen ist der Jurist ein Funktionär, der für sich in Anspruch nimmt, alles zu können,… obgleich er in technisch-fachlichem Sinne nichts gelernt hat. Aber die Entwicklung erreicht einmal einen Punkt, an dem die Technik vermöge ihres gewachsenen Eigengewichts die Funktionsweisen des Juristen überwältigt."[41]

In diesem Sinne brachte es der Vizepräsident des Deutschen Anwaltvereins und Vorsitzende des Berliner Anwaltvereins auf den Punkt, als er unter Bezug auf die US-amerikanischen und britischen Überwachungsaktivitäten schrieb: "Wie naiv muss man eigentlich sein um zu glauben, dass unsere verfassungsmäßige Ordnung auch in Zeiten des globalen Internets in der Lage wäre, unsere Freiheitsrechte tatsächlich schützen zu können? Die Antwort liegt auf der Hand: Es bedarf genau desselben Maßes an Naivität, die erforderlich ist, daran zu glauben, dass das Recht es vermag, sich der faktischen Kraft reiner Macht entgegenzustellen." [42]

Der von Forsthoff prophezeite 'Punkt in der Entwicklung' wurde spätestens mit Beginn des digitalen Zeitalters erreicht. Deswegen sind die oben erwähnten Reaktionen der Politik und des professionellen Datenschutzes auf PRISM, TEMPORA &Co (siehe unter 1.2) nichts anderes als Bestätigungen der vorstehend zitierten Naivität. Geradezu deprimierend ist es, wenn ein rechtsprofessorales Vorstandsmitglied einer professionellen Datenschutzorganisation als Reaktion auf PRISM und TEMPORA mit Vorschlägen aufwartet, die zwar rechtspolitisch in Ordnung, aber Jahrzehnte alt sind, unzählige Male diskutiert wurden und deswegen heute nur noch als Platitüden bezeichnet werden können, in denen aber mit keinem Wort darauf eingegangen wird, was technisch-organisatorisch zu geschehen hat.[43]

Die Naivität (besser: die IT-Ignoranz) ist immer noch 'flächendeckend'. Man hat den Eindruck, dass insbesondere auch Juristen nicht wahrhaben wollen, dass herkömmliche Paragraphen in der digitalen Welt – und das wird beim Datenschutz besonders deutlich – nichts und niemanden lebendig machen, weil sie mangels Gefahr, dass die Nichtbefolgung entdeckt wird, nicht befolgt werden. Das mit der Nichtbefolgung verbundene Risiko ist deshalb so gering, weil mangels Kom-

41 NJW 1960, S. 1275
42 Berliner Anwaltsblatt 9/2013, S. 261
43 vgl. Thüsing, Gregor, FAZ v. 02.09.2013, S. 7

petenz auf Seiten der (oft Juristen anheim gegebenen) Datenschutzkontrolle – wenn eine solche überhaupt existiert – mit einer Ahndung nur bei zufälligen Ausnahmen gerechnet werden muss.

5. Zur Erhaltung der gesellschaftlichen Ordnungsfunktion des Rechts in der digitalen Welt am Beispiel des Datenschutzes

Juristen, die zugleich IT-Spezialisten sind, wissen schon seit Jahrzehnten, dass ein schwerfälliges System von rechtlichen Wertungen und Begriffen wie der Datenschutz mit der Rasanz der informationstechnischen Entwicklung nicht zu synchronisieren ist, sondern dass es für eine tatsächliche Garantie des Datenschutzes in erster Linie technisch-organisatorischer Vorkehrungen bedarf.[44] In diesem Sinne hat sich der Autor dieses Beitrags anlässlich der Präsentation des Buches *'Innovativer Datenschutz'* [45] im Bundesministerium der Justiz am 20. Februar 2013 geäußert, indem er ausführte:[46] "Zu einem aussichtslosen Unterfangen wird der Datenschutz bald geraten, wenn wir einfach im alten Stil weitermachen und meinen, mit dem Erlass von Rechtsvorschriften sei ihm Genüge getan. Das ist ganz bestimmt ein Fehlschluss, wie die zahllosen und nicht enden wollenden Datenskandale seit Bestehen des Datenschutzrechts zeigen. Was wir daher dringend brauchen, sind technische Lösungen für den Datenschutz, gesichert gegen Manipulationen und selbstverständlich produktneutral. Paragraphen sind im Rechtsstaat als Legitimationsgrundlagen zwar unverzichtbar, aber sie allein – und das gilt überall in der digitalen Welt und wird am Datenschutz besonders deutlich – erwecken nichts und niemanden zum Leben; soll der von der Rechtspolitik bei jeder sich bietenden Gelegenheit propagierte Satz "Das Internet ist kein rechtsfreier Raum" keine hohle Phrase bleiben, so müssen auf die Paragraphen draufgesattelt werden – und zwar vorgeschrieben vom Gesetzgeber bzw. vom Verordnungsgeber selbst mittels technischen Organisationsrechts – formalwissenschaftlich, also mathematisch-informatisch konzipierte und ingenieurtechnisch umsetzbare Verfahren der Zweckbindung bzw. der Informationskontrolle, zudem möglichst so allgemeingültig beschrieben, dass nicht bei jeder informationstechnischen Neuerung zugleich auch eine Gesetzesnovellierung nötig wird. Kurzum: Der Datenschutz muss – wie das bereits seit Langem schon für die Datensicherheit angestrebt wird – Konstruktionselement einer jeden Informationstechnik werden, vom Supercomputer bis zum Smartphone, vom Internet bis zur Cloud. Nur so hat der Datenschutz als Quintessenz unserer höchsten Verfassungswerte, der Menschenwürde und der persönlichen Freiheit, in der digitalen Welt eine Zukunft."

5.1 Kritik der legistischen Qualität der aktuellen Fassung des Art. 23 der EU-Datenschutzgrundverordnung

Die aktuelle Fassung des Art. 23 der EU-Datenschutzgrundverordnung lautet:

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

1. Der für die Verarbeitung Verantwortliche führt unter Berücksichtigung des Stands der Technik und der Implementierungskosten sowohl zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung technische und organisatorische Maßnahmen und Ver-

44 vgl. Peters, Falk, Arbeitnehmerdatenschutz, Dissertation 1982; ders. CR 1986, S. 790 ff; Peters, Falk; Kersten, Heinrich: CR 2001, S. 576 ff m.w.H.

45 s. Fn. 40

46 Zitat (auszugsweise), unveröffentlicht

fahren durch, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und die Rechte der betroffenen Person gewahrt werden.

2. Der für die Verarbeitung Verantwortliche setzt Verfahren ein, die sicherstellen, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, die für die spezifischen Zwecke der Verarbeitung benötigt werden, und dass vor allem nicht mehr personenbezogene Daten zusammengetragen oder vorgehalten werden als für diese Zwecke unbedingt nötig ist und diese Daten auch nicht länger als für diese Zwecke unbedingt erforderlich gespeichert werden. Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um etwaige weitere Kriterien und Anforderungen in Bezug auf die in den Absätzen 1 und 2 genannten Maßnahmen und Verfahren festzulegen, speziell was die Anforderungen an den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen für ganze Sektoren und bestimmte Erzeugnisse und Dienstleistungen betrifft.

4. Die Kommission kann technische Standards für die in den Absätzen 1 und 2 genannten Anforderungen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Abs. 2 genannten Prüfverfahren erlassen.

Art. 23 ist ein eklatantes Beispiel für die Flucht des Gesetzgebers in symbolisches Recht. Schon das Sprachgefühl verrät jedem Gebildeten und gerade auch dem Nichtjuristen, dass der Wortlaut von Art. 23 geeignet ist, einer 'Wolkenschieberei' Vorschub zu leisten, wie sie im Datenschutz leider seit eh und je Usus ist. Der Normadressat ist zu nichts Konkretem gezwungen, denn

– in Abs. 1 ist nur erkennbar, dass der Datenschutz zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung durch technische und organisatorische Maßnahmen und Verfahren gewahrt werden soll, wie das aber geschehen soll, ist mit keinem Wort erwähnt. Die Maßnahmen zur Sicherstellung des Datenschutzes bleiben völlig dem Gutdünken des Normadressaten überlassen.

– in Abs. 2 werden die Grundsätze der Zweckbindung, der Datensparsamkeit und der Datenvermeidung zwar angesprochen; aber wiederum bleiben die Maßnahmen zur Implementierung dieser Grundsätze völlig dem Gutdünken des Normadressaten überlassen. Formulierungen wie "die für die spezifischen Zwecke der Verarbeitung benötigt werden" und "als für diese Zwecke unbedingt nötig" sowie "für diese Zwecke unbedingt erforderlich" zeigen, dass dem Normadressaten ein unbegrenzter Spielraum bei der Auslegung dieser wertausfüllungsbedürftigen Formulierungen bleibt.

– in Abs. 3 findet sich eine fragwürdige Ermächtigungsgrundlage für die Kommission, per delegierte Rechtsakte "etwaige weitere Kriterien und Anforderungen in Bezug auf die in den Abs.1 und 2 genannten Maßnahmen und Verfahren festzulegen". In den Abs. 1 und 2 sind aber gar keine Kriterien, Maßnahmen und Verfahren genannt.

– in Abs. 4 endlich findet sich die Ermächtigungsgrundlage zur Festlegung technischer Standards. Dieser Absatz, als Muss-Vorschrift mit verbindlicher Frist zur Erledigung formuliert, hätte als Legitimationsgrundlage für das Tätigwerden in Sachen technischen Datenschutzes gereicht.

Fazit: Art. 23 der EU-Datenschutzgrundverordnung enthält nahezu rein finales Recht, welches dem Normadressaten keinerlei technische oder organisatorische Maßnahmen vorschreibt bzw. zur

Mittelwahl vorgibt, sondern es völlig seinem Belieben überlässt, welche Maßnahmen er de facto zur Sicherstellung des Datenschutzes trifft.

5.2 Postulate

Aus der vorstehenden Kritik am Art. 23 der EU-Datenschutzgrundverordnung ergeben sich für den Datenschutz folgende Postulate ganz allgemein.

5.2.1 Hersteller einbeziehen

Auch für Hersteller muss der Datenschutz, der aus rechtlicher Sicht ein intrinsisches Problem der Dynamik der informationstechnischen Entwicklung ist, diese repräsentiert durch den Computer als des finalen Inbegriffs einer rationalen Welt, ein zentrales Anliegen werden. Der Datenschutz – soll er nicht bloß de jure vorgeschrieben, sondern auch de facto wirksam werden – muss daher Konstruktionselement jeglicher Informationstechnik werden. Also müssen noch vor den datenverarbeitenden Stellen die Hersteller von Informationstechnik in das Datenschutzrecht einbezogen werden.

5.2.2 Präventives Recht statt sanktionierenden Rechts

In der digitalen Welt, für die insbesondere das Internet repräsentativ ist, sind personen- bezogene Daten in beliebiger Menge in Sekundenschnelle weltweit verfügbar und nutzbar. Die basalen Vorgänge sind sinnlich nicht wahrnehmbar. Deswegen ist es für daten- verarbeitende Stellen – handle es sich nun um öffentliche oder nicht-öffentliche Stellen – verlockend, das Datenschutzrecht unbeachtet zu lassen, denn der wirtschaftliche Wert personenbezogener Daten ist sehr hoch und das Risiko, wegen Nichtbeachtung des Datenschutzes belangt zu werden, ist sehr gering. Außerdem ist Naturalrestitution beim Datenschutz nicht möglich und etwaiger Schadensersatz bzw. Entschädigungen haben ohnehin nur symbolische Bedeutung.

Im Unterschied zum klassischen Datenschutzrecht, welches – wie fast das gesamte klassische Recht – aus Zulässigkeitsvorschriften (Geboten und Verboten), Anspruchsgrundlagen und Legaldefinitionen besteht und demzufolge ein System aus beliebig befolgbaren Verhaltens- appellen darstellt, betrifft das technische Organisationsrecht die Reglementierung der Technik durch den Gesetzgeber selbst und stellt ein IT-gestütztes System der Normbefolgungs- bzw. Normkonkretisierungskontrolle dar.

Charakteristika des *klassischen* Rechts sind: präskriptiv-normativ, auslegbar, beliebig befolgbar, sanktionierend. Charakteristika des *technischen* Organisationsrechts sind: empirisch-deskriptiv, eindeutig, Befolgung zwingend, präventiv.

5.2.3 Datenschutz durch Datensicherung

Datenschutz wird seit jeher als rechtliche Regelungsmaterie unter dem Normzweck verstanden, die missbräuchliche bzw. rechtswidrige Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch dazu grundsätzlich Befugte zu verhindern. Er ist Ausdruck der verfassungsrechtlich garantierten informationellen Selbstbestimmung des Menschen.[47]

47 vgl. 1BvR 209/83 u.a. – Urteil vom 15. Dezember 1983

Datensicherheit wird grundsätzlich als technisch-organisatorische Aufgabe mit dem Ziel verstanden, Unbefugten den Zugang, die Verarbeitung und die Nutzung jeglicher Daten unmöglich zu machen. Kurz gesagt: Sie bezweckt die Bekämpfung der Datenkriminalität.

Jedoch ist *Datenschutz durch Datensicherung*, also technisch-organisatorischer Datenschutz, von Anfang an durch das Bundesdatenschutzgesetz und sodann durch die höchstrichterliche, insbesondere durch die verfassungsgerichtliche Rechtsprechung zur informationellen Selbstbestimmung längst legitimiert, ja sogar gefordert.

Daten, die vom Gesetz oder von datenverarbeitenden Stellen als schutzwürdig oder gar als geheimhaltungsbedürftig eingestuft werden – personenbezogene Daten gehören dazu –, fallen in den diesbezüglichen Sicherheitskonzepten unter das Sicherheitsziel der *Vertraulichkeit*, das indes immer durch technische oder menschliche Schwachstellen bedroht ist. Den damit verbundenen Risiken begegnet man üblicherweise mit einer *Access Control*, i.e. eine Zugriffs- bzw. Zugangskontrolle, die im Sicherheitskonzept detailliert geplant und sodann technisch umgesetzt wird. Abgesehen von der Binsenweisheit, dass es 100%ige Sicherheit nicht gibt, ist das Problem bei diesem Vorgehen, dass dabei immer nur der Devise gefolgt wird, Befugten etwas zu gestatten, Unbefugten dagegen etwas zu verwehren. Damit sind Aktionen von Befugten eigentlich gar nicht kontrollierbar, d.h. die gesamte Insider-Problematik fällt aus dieser Form der Sicherheitsmaßnahme heraus. Gerade hier ist aber ein hohes Potenzial für den unerwünschten Abfluss von Daten (Data Leakage) vorhanden.[48] Um also Data Leakage möglichst perfekt zu entdecken bzw. zu vermeiden, muss daher neben dem Zugang zu Daten auch der Umgang mit Daten kontrolliert werden, was selbstverständlich rechtlich legitimiert sein muss.

5.2.4 Data Privacy Compliance Management als interdisziplinäre Aufgabe von IT und Recht

Das schon erwähnte Buch *'Innovativer Datenschutz'*[49] verdankt seine Entstehung nur und ausschließlich dem Ziel zu demonstrieren, dass es höchste Zeit ist, vom klassischen Datenschutzmanagement, das sich im Wesentlichen manueller Techniken wie Akteneinsicht, Einholung von Auskünften usw. bedient, zu einem automatisierten *Datenschutz-Engineering* zu avancieren. In diesem Sinne führte der Vorsitzende des Innenausschusses des Deutschen Bundestages aus: "Die Geschichte des Datenschutzes zeigt: Für den Schutz personenbezogener Daten sind Gesetze zwar ein sehr wichtiger, aber immer nur der erste Schritt. Denn letztlich entscheidet die Umsetzung der Datenschutznormen darüber, ob die alltägliche Praxis den gesetzgeberischen Zielvorstellungen entspricht.

Dabei gefährdet die fortschreitende automatisierte Verarbeitung in IT-Systemen personenbezogene Daten in besonderer Weise und verlangt signifikante Schutzmaßnahmen. Der beste und effektivste Schutz sind hier technische und organisatorische Maßnahmen, welche zu einem systemimmanenten Schutz personenbezogener Daten führen. Das Idealziel muss sein, eine rechtlich verbotene Datenverarbeitung unmöglich zu machen und im Rahmen eines IT-Systems nur eine solche Datenerfassung und -verarbeitung zuzulassen, die den Rechtsnormen entspricht."[50]

48 s. Fn. 2, S. 10
49 s. Fn. 40
50 s. aaO, S.9

6. Schlussbemerkung

Im Gegensatz zur internationalen Ebene ist auf nationaler Ebene Data Leakage Prevention durch technischen Datenschutz durchaus möglich. Dass die Politik dennoch bisher nichts in diese Richtung Weisendes unternommen hat, liegt sowohl an der Verhinderungsstrategie seitens der Management-Lobby, die eine IT-gestützte Kontrolle ihrer Tätigkeit scheut wie der Teufel das Weihwasser, als auch an der Ignoranz der zuständigen politischen Entscheidungsträger, was Organisation und Funktionsweisen der digitalen Welt betrifft.

[20.11.13]

Anschrift des Autors:

RA Dr. Falk Peters
Artemisstr. 9A
D – 13469 Berlin
ra.dr.falk.peters@t-online.de