**Deutscher Bundestag**
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)08

# Schriftliche Stellungnahme
# zum Fragenkatalog für das öffentliche Fachgespräch
# des Ausschusses Digitale Agenda des Deutschen Bundestages

zum Thema IT-Sicherheit
am Mittwoch, dem 7. Mai 2014

**Prof. Niko Härting** | Härting Rechtsanwälte

1. Eine „sichere Kommunikation“ war im Netz bei realistischer Betrachtung zu keinem Zeitpunkt möglich. Hacker haben bereits frühzeitig auf Schwachstellen aufmerksam gemacht. Der Akzeptanz des Internet als Kommunikationstool haben Berichte über nachgewiesene Sicherheitsdefizite zu keinem Zeitpunkt ernsthaft geschadet.

   Staatlicherseits hat es immer wieder Versuche gegeben, die digitale Kommunikation zur Gefahrenabwehr und zur Aufdeckung von Straftaten zu überwachen. Dies gilt für Versuche einer „Online-Durchsuchung“ ebenso wie für die gescheiterte Vorratsdatenspeicherung, aber auch für Bestandsdatenauskünfte. Der mit Abstand gewichtigste Beitrag, den der Staat zum Grundrechtsschutz leisten kann liegt darin, von Überwachungsmaßnahmen in größtmöglichem Maße Abstand zu nehmen.

2. Es ist zweifellos sinnvoll und angemessen, Nutzer über Sicherheitsdefizite aufzuklären und zu ermutigen, verschlüsselt zu kommunizieren. Hierzu kann unter anderem die Stiftung Datenschutz als unabhängige Stelle einen hilfreichen Beitrag leisten.

3. Datensicherheit und Datenschutz sind ein ungleiches Geschwisterpaar. Während in Deutschland und Europa intensiv über gesetzliche Maßnahmen zur Verbesserung und Modernisierung des Datenschutzes diskutiert wird, wird nicht immer in gleicher Intensität über regulatorische Maßnahmen zur Datensicherheit gesprochen. Dabei ist zu beachten, dass es nicht nur um die Sicherheit personenbezogener Daten geht, sondern beispielsweise auch um den Schutz bedeutsamer Betriebs- und Geschäftsgeheimnisse. Es ist sinnvoll und angemessen, den Anbietern von Kommunikations-Infrastruktur Sicherheitsstandards vorzugeben und die Einhaltung dieser Standards zu überwachen.

4. Alle Versuche, eine weite Verbreitung verschlüsselter Kommunikation durchzusetzen, sind bislang weitgehend fruchtlos geblieben. Digitale Signaturen haben sich am Markt nicht durchsetzen können, die Entwicklung und Verbreitung der De-Mail sollte abgewartet werden, bevor neue Systeme der Verschlüsselung und Zertifizierung entwickelt und regulatorisch verankert werden.

   Wie schwierig die Durchsetzung verschlüsselter Kommunikation ist, zeigt sich auch daran, dass Behörden in aller Regel Mails unverschlüsselt lassen. Jedwede weiteren Versuche einer regulatorischen Durchsetzung sollten daher Regelungen schaffen, die gewährleisten, dass staatliche Stellen den Weg der Verschlüsselung beschreiten und mit gutem Beispiel vorangehen.

5. Kleine und mittelständische Unternehmen sowie Privatpersonen bedürfen der Aufklärung über Sicherheitsrisiken durch Instanzen wie das BSI oder die Stiftung Datenschutz. Regulatorische Maßnahmen zur Verbreitung speziellen Verschlüsselungstechnik sind in der Vergangenheit oft fruchtlos geblieben.

6. Instant-Messenger-Dienste sind ein Beispiel dafür, dass unter den Gegebenheiten der digitalen Kommunikation die Reichweite des Telekommunikationsgeheimnisses und des Telekommunikationsrechts immer mehr an Trennschärfe verliert. Wie in der Stellungnahme des Deutschen Anwaltverein Nr. 55/2013 im einzelnen dargestellt, ist die Regulierungsdichte des Telekommunikationsrechts erheblich größer, als dies im Telemedienrecht der Fall ist. Auch die datenschutzrechtlichen Beschränkungen sind wesentlich tiefgreifender, wenn es um Telekommunikation geht, als dies bei Telemedien feststellbar ist. Regulatorisch sollte sich der Gesetzgeber entscheiden,

entweder Dienste wie WhatsApp vollständig dem Telekommunikationsrecht oder dem Telemedienrecht zu unterwerfen, um Rechtssicherheit für die Anbieter zu gewährleisten. Für eine Geltung des flexibleren Telemedienrechts könnte sprechen, dass bei einer allzu weitreichenden Geltung des Telekommunikationsgeheimnisses dessen Schutz schleichend ausgehöhlt werden könnte. Die Gefahr einer Aushöhlung lässt sich beispielsweise aus der Entscheidung des BVerfG zur Beschlagnahme von Mails beim Provider ableiten (BVerfG vom 16.6.2009, Az. 2 BvR 902/06). In dieser Entscheidung hat das BVerfG zwar einen Eingriff in das Fernmeldegeheimnis bejaht, zugleich jedoch sehr milde Anforderungen an einen solchen Eingriff postuliert.

7. Das Schengen-Routing und die Deutschland-Mail sind Vorschläge geschlossener Systeme, die – soweit praktikabel – ausländischen Behörden einen Zugriff erschweren könnten. Wie jedes geschlossene System würden derartige Verfahren den Zugriff durch inländische Stellen zugleich erleichtern, sofern keine Ende-zu-Ende-Verschlüsselung erfolgt. Ob dies gewollt ist, ist eine Frage, die nur politisch beantwortet werden kann. Soweit hierbei wirtschaftspolitische Erwägungen durch eine Förderung inländischer Anbieter eine Rolle spielen, sollte dies redlicherweise offen erörtert werden.

8. Für Messenger-Dienste bedarf es einer grundsätzlichen Entscheidung, welchem Regelungskomplex diese Dienste unterworfen werden. Auch bei der E-Mail-Kommunikation sind Regelungsdefizite feststellbar. So gibt es in den Unternehmen erhebliche Unsicherheiten über die Reichweite des Telekommunikationsgeheimnisses, wenn Mitarbeiter per Mail kommunizieren. Es fehlt an klaren rechtlichen Maßgaben und an höchstrichterlicher Rechtsprechung.

9. Das BSI und auch die Stiftung Datenschutz sollten weiter gestärkt werden als Instanzen, die zur Aufklärung und Beratung von Bürgern und Unternehmen wirken.

10. Für die Zertifizierung bietet es sich an, gesetzliche Grundlagen zu schaffen, die Anreize für Zertifizierungssysteme schaffen. Ein Vorbild könnten frühere Versuche gesetzlicher Grundlagen für Datenschutz-Audits liefern.

11. Die EU-Datenschutzgrundverordnung klammert den gesamten Bereich der nationalen Sicherheit aus und setzt daher europäischen Nachrichtendiensten keine Grenzen. Noch weniger ist damit zu rechnen, dass sich nicht-europäische Dienste durch eine europäische Verordnung daran hindern lassen werden, Überwachungsmaßnahmen gegen europäische Bürger zu richten. Soweit versucht wird, amerikanische Unternehmen an einer Zusammenarbeit mit ausländischen Diensten durch europäische Verbotsnormen zu hindern, verkennen die Brüsseler Entwürfe die Zwangslage und die Pflichtenkollision, die für die betroffenen Unternehmen entsteht. Wenn amerikanisches Recht Google zu Auskünften an amerikanische Dienste verpflichtet und europäisches Recht derartige Auskünfte zugleich untersagt, wird von den betroffenen Unternehmen Unmögliches verlangt. Im umgekehrten Verhältnis wird dies zurecht kritisiert, wenn beispielsweise deutsche Unternehmen in den USA verklagt werden und im Rahmen eines Discovery-Verfahrens zu Auskünften verpflichtet werden, die sie nicht ohne Verstoß gegen deutsches Datenschutzrecht erteilen können.