

## **Un-Begrenzte Möglichkeiten? Zur Krise ausgespähter und ausspähender Demokratien**

Sehr geehrter Herr Stöhr, sehr geehrter Herr Prof. Falke,

vielen Dank für die Einladung und die Organisation dieser Veranstaltung. Als Sie, sehr geehrter Herr Stöhr, im Oktober letzten Jahres unter dem Eindruck der Veröffentlichungen von Edward Snowden auf mich zukamen und meinten, dass viele Bürger die Frage nach der Sicherheit ihrer Daten beschäftige und in diesem Zusammenhang auch kritische Rückfragen nach dem Selbstverständnis westlicher Demokratien gestellt würden, wussten wir beide nicht, wie sich das Thema fortentwickeln würde. Als Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, zu dessen Aufgabenbereich es auch gehört, zu kontrollieren, ob und inwieweit bei Unternehmen der Datensicherheit Rechnung getragen wird, würde ich nach unseren Maßstäben sagen, dass bei der NSA eine Datenpanne in einem unvorstellbaren Ausmaß aufgetreten ist, so dass es Edward Snowden möglich war, eine ebenfalls offensichtlich unvorstellbare Menge von Daten abzugreifen und zu veröffentlichen. Ob man das unter politischen Gesichtspunkten als gut empfinden mag oder nicht, möchte ich nicht beurteilen. Nicht wohl fühle ich mich aber bei dem Gedanken, dass nicht nur Edward Snowden, sondern auch andere, d.h. andere Geheimdienste, Kriminelle oder Sonstige auf diese Daten Zugriff haben können. Das heißt, dass die Frage, ob es überhaupt begrenzte Möglichkeiten des Ausspähens und des Unter-Verschluss-Haltens ausgespähter Daten gibt, mehr als offen ist.

Ich freue mich darüber, dass entgegen der ursprünglichen Planung für diese Veranstaltung mit einem Einzelvortrag von mir, Sie, sehr geehrter Herr Moeller als Generalkonsul der Vereinigten Staaten von Amerika mit Sitz in München heute bei uns sind und mit mir und ich denke später auch den Zuhörerinnen und Zuhörern über diesen Themenkomplex sprechen.

Meine Mitarbeiterinnen und Mitarbeiter im Bayerischen Landesamtes für Datenschutzaufsicht und ich sind dafür zuständig, zu kontrollieren, ob und inwieweit bayerische Unternehmen, Verbände oder Vereine datenschutzrechtliche Vorschriften einhalten. Unsere Aufgabe ist es deshalb auch, zu prüfen, in welchem Umfang personenbezogene Daten aus Deutschland, unter anderem auch in die USA übermittelt werden, ob es dafür eine ausreichende Rechtsgrundlage gibt und ob sichergestellt ist, dass mit diesen personenbezogenen Daten im Ausland so umgegangen wird, wie es nach deutschem und europäischem Recht erforderlich ist. Ferner ist es unsere Aufgabe, zu prüfen, ob Unternehmen, Vereine, Verbände oder freiberuflich Tätige in Deutschland die gesetzlich

erforderlichen Anforderungen an die Datensicherheit einhalten und es damit „interessierten Stellen“, zu denen ich den chinesischen oder russischen Geheimdienst, die NSA, den englischen Geheimdienst, kriminelle Hacker, interessierte Informatikstudenten oder sonstige zähle, erschweren, auf einzelne personenbezogene Daten zuzugreifen oder gar diese personenbezogenen flächendeckend abzugreifen.

Wir haben durch die Aussagen von Edward Snowden, denen nach meiner Kenntnis bisher substantiiert nicht widersprochen wurde, wahrgenommen, dass durch amerikanische Geheimdienste eine flächendeckende Überwachung in einem Umfang auch in Deutschland stattfindet, den wir so nicht für möglich gehalten haben. Ob diese Überwachung dem Recht der USA entspricht, kann ich nicht beurteilen. Wir haben auch, zuletzt durch eine Entscheidung des Bezirksgerichts New York vom 25. April 2014, zur Kenntnis genommen, dass amerikanische Unternehmen verpflichtet sind, auch in sehr großem Umfang, d.h. nicht nur auf einen Einzelfall bezogen, personenbezogene Daten von - aus amerikanischer Sicht - Ausländern herauszugeben, selbst wenn diese auch nur durch europäische Tochterunternehmen der amerikanischen Unternehmen erhoben wurden und verarbeitet werden. Mit anderen Worten bedeutet dies, dass alle personenbezogenen Daten, die amerikanische Unternehmen, sei es Google, Apple, Facebook, Microsoft, Salesforce, Amazon, Yahoo oder wie sie alle heißen, über Deutsche gespeichert haben, herausgegeben werden müssen, ohne dass ein gerichtlich überprüfbarer Anlass Zweck Voraussetzung für eine Herausgabe wäre. Eine Kontrolle durch Datenschützer, zu welchem Zweck die Daten verwendet werden, findet nicht statt. Ferner erfolgt auch keine Informationen der Betroffenen, deren Daten übermittelt wurden.

Diese Situation bedeutet für uns Datenschützer in Deutschland eine sehr schwierige Situation, da wir, soweit wir es aufgrund unserer rechtlichen Möglichkeiten überhaupt können, ein derartiges Handeln dieser Unternehmen untersagen müssten.

Es gibt Rechtsgrundlagen, wie die Vereinbarung zwischen der Europäischen Kommission und dem amerikanischen Handelsministerium über Safe Harbour, wonach sich amerikanische Unternehmen selbst zertifizieren lassen können und sich zur Einhaltung europäischer Datenschutzstandards verpflichten. Tatsache ist aber, dass sich trotz dieser Verpflichtung die Unternehmen nach amerikanischem Recht nicht gegen die Herausgabe der Daten, die Nichtamerikaner betreffen, wehren können. Sie können sich nur entscheiden, ob sie gegen europäisches oder amerikanisches Recht verstoßen wollen. Ob deshalb diese Vereinbarung, die für die Wirtschaft eine enorm hohe Bedeutung hat, mittelfristig noch Bestand haben kann, wird derzeit von der Europäischen Kommission überprüft. Antwort aus den USA auf die Fragen aus Brüssel liegen bisher noch nicht vor.

Lassen Sie mich noch von einer anderen Seite auf dieses Thema blicken. Wir leben in einer globalisierten Welt, in der manche Grenzen verschwimmen oder, wenn man auf das Internet schaut, kaum mehr erkennbar sind. Wir haben in dieser globalisierten Welt aber unterschiedliche Bereiche, in denen unterschiedliches Recht gilt und auch eine zum Teil erheblich unterschiedliche Rechtskultur vorherrscht. Ich möchte diese Unterschiede zwischen USA und Deutschland bzw. Europa für den Bereich des Datenschutzes an zwei Beispielen deutlich machen.

- Heuhaufen
  - Wir hören immer wieder aus den USA: Wir suchen die Nadel im Heuhaufen. Mit anderen Worten, wir suchen in unseren Daten unter Verwendung entsprechender Algorithmen nach Merkmalen für Terroristen. Die Frage, wie der Heuhaufen zustande gekommen ist, spielt keine Rolle. Ob dieser Heuhaufen dann wirklich nur für die Suche nach Terroristen oder, wenn man ihn schon mal hat, auch für Wirtschaftsspionage genutzt wird, ist für mich jedenfalls nicht transparent.
  - Wir in Deutschland und Europa sagen: Wenn schauen auf eine grüne Wiese und suchen, wo Unkraut wächst. Dann beobachten wir diesen Bereich. Der große Datenstrom ist für uns zunächst unverdächtig und wird keiner anlasslosen Kontrolle unterzogen.
  
- Nutzungsdaten
  - Wenn ich es richtig sehe, dann dürfen und werden in den USA ohne jegliche rechtliche Beschränkung Nutzungsdaten der Telekommunikation gespeichert, weil sie als öffentliche Informationen gelten. Dies bedeutet konkret, dass gespeichert wird, wer mit wem, wie lange und auf welchem Kommunikationsweg verbunden war. Mit diesen Daten lassen sich sehr klare Erkenntnisse über Beziehungen und Netzwerke, Aufenthaltsorte und noch viel mehr für jeden einzelnen Menschen gewinnen.
  - In Europa unterliegen auch diese Daten dem Datenschutz. Der europäische Gerichtshof hat in seiner Entscheidung vom 8. April 2014, bekannt geworden unter dem Stichwort: Vorratsdatenspeicherung, sehr klar und deutlich ausgeführt, dass eine derartige flächendeckende und anlasslose Datenspeicherung nur unter gesetzlich genau festzulegenden Kriterien, für beschränkte Bereiche und einen beschränkten Zeitraum zulässig sind.

Wir haben in Europa in der seit dem 1. Dezember 2009 wirksamen Grundrechtecharta ein ausdrückliches europäisches Datenschutzgrundrecht. Wir haben darüber hinaus, abgeleitet aus Art. 1 Grundgesetz, der lautet: Die Menschenwürde ist unantastbar“ in Verbindung mit dem Recht auf freie Entfaltung der Persönlichkeit in Art. 2 Abs. 1 des Grundgesetzes ein deutsches Datenschutzgrundrecht, das vom Bundesverfassungsgericht als „Recht auf informationelle Selbstbestimmung“ bezeichnet wurde und auch immer noch bezeichnet wird. Dieses Datenschutzgrundrechts gilt nicht nur im Verhältnis des Bürgers zum Staat, sondern auch im Verhältnis Bürger zu Bürger bzw. Bürger zu Unternehmen. Es ist Aufgabe des Staates, sicherzustellen, dass die Grundrechte der Menschen, die sich in Deutschland aufhalten, beachtet werden. Deshalb ist es unsere Aufgabe als Datenschutzaufsichtsbehörde dafür Sorge zu tragen, dass durch Unternehmen, die in Bayern aktiv sind, Datenschutzgrundrechte nicht verletzt werden. Wenn diese Grundrechtsverletzung in einer Art und Weise stattfindet, dass wir als zuständige Behörde und auch keine sonstigen Behörden diese verhindern können, kann dies zu einer Krise der Demokratie werden, weil die Bürger das Vertrauen in die Fähigkeit ihres eigenen Staat, sie zu schützen, verlieren können.

Lassen Sie mich wieder zurückkommen zu unserer Aufsichtspraxis. Wir leben, wie gesagt, in einer globalisierten Welt und haben gerade zwischen Europa und USA eine sehr enge und sehr umfangreiche wirtschaftliche Verflechtung. Wir haben unterschiedliche rechtliche und auch datenschutzrechtliche Voraussetzungen diesseits und jenseits des Atlantiks. Ein ganz erheblicher Teil der wirtschaftlichen Betätigung wird mittlerweile über das Internet abgewickelt. Dabei spielt die Frage des Vertrauens eine zunehmend größere Rolle. Kann ich Firmen wie Microsoft, Facebook, Amazon, Apple, Google usw. vertrauen, dass sie mit unseren Daten nach unserem Verständnis rechtmäßig umgehen oder muss ich davon ausgehen, dass sie unter entsprechender Strafandrohung unsere Daten massenweise herausgeben müssen und ebenfalls unter entsprechender Strafandrohung uns nicht darüber informieren dürfen, welche Daten sie an wen herausgegeben haben.

Wir haben nicht nur in Europa rechtliche Grundlagen, sondern auch in Art. 12 der Allgemeinen Erklärung der Menschenrechte vom 10. Dezember 1948 eine weltweit geltende Regelung, die nach meinem Verständnis in diesem Zusammenhang Bedeutung haben kann. Art. 12 der Allgemeinen Erklärung der Menschenrechte lautet wie folgt:

Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

Ich betrachte es als einen willkürlichen Eingriff in mein Privatleben und in meine Familie, wenn meine Kommunikation und damit ich Bestandteil einer anlasslosen flächendeckenden Überwachung werde. Wir dürfen bei dieser Frage der Achtung der Menschenrechte auch keinen Unterschied machen, ob es sich um eigene Staatsangehörige oder „nur“ (ich sage dies mit großem Ausrufezeichen) Ausländer handelt.

Was bedeutet das nun für heute und die Zukunft. Wollen wir in dieser globalisierten Welt ein deutsches Internet oder auch nur ein europäisches Internet? Wollen wir ein deutsches oder ein europäisches Cloud-Computing? Wollen wir den deutschen Markt für Firmen wie Facebook, Apple und Co. schließen. Ich meine, dass dies keine wirklich gute Alternative ist. Ich meine aber auch, dass der bestehende Zustand nicht auf Dauer hingenommen werden soll. Ich wünsche mir deshalb, dass wir uns für die digitale Welt auf Standards einigen können, die dem amerikanischen und auch dem europäischen Recht angemessen Rechnung tragen, um für die bestehenden und für uns alle fruchtbaren wirtschaftlichen Beziehungen unter Beachtung der Grundrechte auf beiden Seiten des Atlantiks eine tragfähige Grundlage zu schaffen.