741.943.1

Alexander Dix

Vortrag beim 9. Europäischen Datenschutztag am 28.1.2015 in Berlin

Safe Harbor am Ende ? – Eine Betrachtung aus aufsichtsbehördlicher Sicht

Die englischsprachige Version von Wikipedia bezeichnet die europäische Datenschutzrichtlinie – ganz im Sinne des heutigen Themas - als Beispiel für eine „Safe-Harbor-Regelung". Europa war also ursprünglich der sichere Hafen im Sinne des Datenschutzes (auch heute noch ?) Das Safe Harbor Abkommen von 2000 zwischen Europa und den USA sollte den transatlantischen Datenverkehr in den europäischen sicheren Hafen einbeziehen und ihn gegenüber dem übrigen Datenexport aus Europa privilegieren.

Das Abkommen war von Anfang an ein problematischer Kompromiss. Weder in punkto Zweckbindung noch hinsichtlich des durch Verhältnismäßigkeit und Zumutbarkeit für die Datenverarbeiter eingeschränkten Auskunftsrechts oder bei der Weiterübermittlung in Drittstaaten entsprechen die Grundsätze des US-amerikanischen sicheren Hafens den Grundprinzipien des europäischen und deutschen Datenschutzrechts. Dennoch hat die Kommission sich vor allem aus wirtschaftspolitischen Gründen über die prinzipiellen und wiederholt geäußerten Einwände der Art. 29-Gruppe und des Europäischen Parlaments hinweggesetzt und das Abkommen mit der US-Regierung unterzeichnet. Damit ist allerdings keine prinzipielle Anerkennung des Datenschutzniveaus in den USA als angemessen im Sinne der Datenschutzrichtlinie von 1995 verbunden. Vielmehr beruht der sichere Hafen – und das ist wahrscheinlich seine zentrale Schwäche – auf einem System der Selbstzertifizierung, bei dem sich US-Unternehmen durch einen einfachen Brief an das Handelsministerium dem Safe Harbor-Konzept unterwerfen, anders ausgedrückt, sie bescheinigen sich selbst datenschutzkonformes Verhalten, ohne dass dies von einer unabhängigen Aufsichtsbehörde überprüft worden wäre oder später in jedem Fall überprüft wird. Das Fehlen einer unabhängigen Datenschutzaufsicht für die US-amerikanische Wirtschaft ist ein zentraler Mangel, der die Anerkennung der USA als sicheres Drittland bisher verhindert hat. Auch die Federal Trade Commission kann nur in bestimmten Wirtschaftsbereichen Beschwerden nachgehen und Fälle von Verbrauchertäuschung ahnden.

Nur aufgrund der nachdrücklichen Kritik, die die Art. 29-Gruppe vor Abschluss des Abkommens an dessen Grundkonzeption geübt hatte, hat sich die Kommission bereit gefunden (auch um Widerstände im Parlament auszuräumen), in ihrer Entscheidung vom 26. Juli 2000 die Kontrollbefugnisse

der nationalen Aufsichtsbehörden bei Datenexporten in die USA auch an Safe Harbor-Unternehmen einerseits zu betonen, sie andererseits aber an sehr hohe rechtliche Hürden zu knüpfen.

Zum einen haben die Aufsichtsbehörden auch bei einem Datenexport nach den Regeln des Safe Harbor weiterhin die Einhaltung nationaler Datenschutzregeln sicherzustellen. Eine Datenverarbeitung, die in Deutschland oder einem anderen europäischen Land unzulässig wäre, kann nicht durch den Export in die USA zu einem Safe-Harbor-zertifizierten Empfänger legalisiert werden. Die europäischen Regeln zum Datenexport sahen von Anfang an eine zweistufige Prüfung vor: zunächst muss die Rechtmäßigkeit nach deutschem Recht geprüft werden, bevor in einem zweiten Schritt die Angemessenheit des Datenschutzniveaus beim Empfänger untersucht wird.

Aber genau diese Angemessenheit des Datenschutzniveaus bei den zertifizierten US-Unternehmen wurde durch die australischen Galexia-Studien 2008 /2010 in Frage gestellt, nach denen eine Vielzahl von Unternehmen sich damit begnügten, eine einmalige Selbstzertifizierung beim Handelsministerium vorzunehmen und sich nicht um die vorgeschriebene jährliche Re-Zertifizierung zu kümmern. Dies führte zu Reaktionen auf beiden Seiten des Atlantiks: Die Federal Trade Commission intensiviert seitdem ihre Überprüfung, welche Unternehmen sich zu Unrecht auf die Safe Harbor-Grundsätze berufen, obwohl sie die Erneuerung der Zertifizierung unterlassen haben. Ein Teil der inzwischen fast 5000 auf der Liste des Handelsministeriums aufgeführten Safe-Harbor-Unternehmen ist deshalb mit dem Zusatz „nicht aktuell“ (not current) versehen. Die Federal Trade Commission hat aber nach wie vor keine Befugnis, bereits bei der ersten Anmeldung für die Safe Harbor-Liste zu überprüfen, ob die Selbsteinschätzung des Unternehmens, sich datenschutzkonform zu verhalten, tatsächlich zutrifft. Sie ist außerdem auf den Vebraucherschutz-Aspekt des irreführenden Verhaltens beschränkt. Datenschutz ist aber mehr als Verbraucherschutz. Für den in den USA ohnehin praktisch nicht-existenten Beschäftigtendatenschutz ist sie nicht zuständig.

In Deutschland führten die Galexia-Studien 2010 zu der Klarstellung des Düsseldorfer Kreises, dass der deutsche Datenexporteur der Behauptung des Importeurs, er sei Safe-Harbor-zertifiziert, nicht blind vertrauen darf. Der Exporteur muss sich vielmehr vom Importeur nachweisen lassen, dass die Zertifizierung noch aktuell ist und wie das US-Unternehmen seinen Informationspflichten gegenüber den Betroffenen nachkommt.

Mit den Snowden-Veröffentlichungen hat die Debatte über das Safe Harbor-Abkommen, aber auch über die Standardvertragsklauseln eine völlig neue Dimension erhalten. Zwar enthalten die Kommissions-Entscheidungen zu den Standardvertragsklauseln und zum Safe Harbor Vorbehalte zugunsten des Zugriffs von Sicherheitsbehörden. Diese Vorbehalte konnten aber von europäischer Seite von Anfang an nur so verstanden werden, wie sie nicht nur nach dem europäischen Grundrechtsver-

ständnis, sondern auch nach dem UN-Menschenrechtspakt für zivile und politische Rechte verstanden werden müssen: Sicherheitsbehörden dürfen nur anlassbezogen und in verhältnismäßigem Umfang in Grundrechte eingreifen. Die Art. 29-Gruppe hat deshalb im vergangenen Jahr (zuletzt im Dezember) in mehreren Stellungnahmen betont, dass weder die Standardvertragsklauseln noch die Safe Harbor-Prinzipien eine anlasslose, flächendeckende und unbegrenzte Übermittlung von personenbezogenen Daten für Zwecke der Sicherheitsbehörden rechtfertigen. Der Google-Chef Larry Page formulierte es im März 2014 so: „Ich glaube, es ist mit demokratischen Prinzipien unvereinbar, wenn wir die Nutzer vor Regierungshandeln schützen müssen, von dem nie die Rede war."

Deutsche Aufsichtsbehörden haben deshalb im Sommer 2013 erklärt, zum einen keine neuen Genehmigungen für Datenexporte in die USA erteilen zu wollen, solange keine politische Einigung zwischen der EU und der US-Regierung über eine Begrenzung der Geheimdienstaktivitäten erzielt worden ist; zum anderen wollen sie prüfen, ob Datentransfers nach Art. 3 Satz 1 Buchstabe b) der Safe Harbor-Entscheidung bzw. nach der entsprechenden Bestimmung der Entscheidungen zu Standardvertragsklauseln auszusetzen sind. Dies wurde in der Öffentlichkeit teilweise als Ankündigung missverstanden, deutsche Datenschutzbehörden wollten das Safe-Harbor-Abkommen aufkündigen. Dazu sind die Aufsichtsbehörden der Mitgliedstaaten nicht befugt. Sie können aber Genehmigungen versagen und den laufenden Datenexport zeitweise untersagen, wenn die Voraussetzungen des Art. 3 Satz 1 Buchstabe b) der Kommissionsentscheidung vom 26.7.2000 vorliegen. Entsprechende Verwaltungsverfahren laufen gegenwärtig in Berlin und Bremen, sind allerdings noch nicht abgeschlossen. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat sich ausdrücklich vorbehalten, entsprechende Anordnungen zu treffen. In diesem Zusammenhang ist auch auf die Entscheidung des irischen High Court vom Juli 2014 hinzuweisen, der dem Europäischen Gerichtshof die Frage vorgelegt hat, ob nationale Aufsichtsbehörden angesichts der bekannt gewordenen Praktiken der NSA die Frage der Angemessenheit des Datenschutzniveaus bei Safe Harbor-zertifizierten Unternehmen überprüfen muss. Der High Court selbst bejaht diese Frage.

Die Voraussetzungen für die Aussetzung des Datenexports sind relativ hoch. Ich erinnere daran, dass diese Befugnis von der Kommission erst auf Druck des Europäischen Parlaments und der europäischen Datenschutzbehörden aufgenommen und bewusst restriktiv formuliert worden ist. Daran muss man angesichts der aktuellen Bitte/Aufforderung der Kommission an die europäischen Datenschutzbehörden erinnern, jetzt verstärkt von den Aussetzungsbefugnissen Gebrauch zu machen. Dennoch spricht viel dafür, dass die Voraussetzungen der Aussetzung nach den Kommissionsentscheidungen gegeben sind. Solange die Vereinigten Staaten die Zugriffe ihrer Sicherheitsbehörden nicht auf das notwendige und erforderliche Maß beschränken, wie es die Europäische Kommission im November 2013 empfohlen hat, besteht eine hohe Wahrscheinlichkeit, dass die Grundsätze des sicheren Hafens verletzt werden und das unmittelbar bevorstehende Risiko eines schweren Scha-

dens für die betroffenen Personen besteht. Dieser Schaden muss kein materieller sein, er liegt vielmehr in der systematischen Verletzung des Grundrechts auf informationelle Selbstbestimmung.

Da die angekündigte Reform der Geheimdienste in den USA schon im Dezember (also noch bei demokratischer Mehrheit im Senat) zumindest vorerst gescheitert ist und auch Präsident Obama seine Befugnisse nicht dazu genutzt hat, die NSA-Aktivitäten zu beschränken, ist es umso wichtiger, dass deutsche und europäische Behörden bis zum Inkrafttreten der Datenschutz-Grundverordnung oder einer grundlegenden Überarbeitung des Safe Harbor-Abkommens ihre Befugnisse zum Schutz der Daten von Unionsbürgern nutzen, indem sie in geeigneten Fällen den Export von Kunden- und Beschäftigtendaten in die USA aussetzen.

Sie sollten darüber hinaus europäische Unternehmen dazu veranlassen, für ihre Datenverarbeitung europäische Cloud-Lösungen zu finden, statt sie an die marktbeherrschenden Anbieter in den USA auszulagern. Wir konnten bereits zwei große Berliner Unternehmen von der Notwendigkeit dieses Schritts überzeugen, ohne dass es einer Anordnung bedurft hätte. Ob die zunehmende Verlagerung von Rechenzentren amerikanischer Unternehmen nach Europa deren Angebote wieder datenschutzrechtlich interessant machen kann, hängt vom Ausgang des Rechtsstreits zwischen Microsoft und der CIA zur Frage der Zugriffsrechte von US-Behörden auf in Europa belegene Server unter der Kontrolle von US-Unternehmen ab.

Langfristig ist zu hoffen, dass auch in den Vereinigten Staaten ein allgemeines Datenschutzgesetz für den privaten Sektor in Kraft tritt. Dazu hat es mehrere Anläufe gegeben. Zuletzt hat Präsident Obama am 12. Januar dieses Jahres angekündigt, noch im Februar einen Gesetzentwurf zum besseren Verbraucherdatenschutz vorlegen zu wollen. Entsprechende Ankündigungen hatte er bereits 2012 gemacht. Auch wenn er hofft, dafür parteiübergreifende Unterstützung im Kongreß zu erhalten, ist der Ausgang angesichts der neuen Mehrheiten völlig ungewiss.

Allerdings muss bei dem Stichwort „Europa: Sicherer Hafen des Datenschutzes ?“ auch die Frage angesprochen werden, inwieweit die Zusammenarbeit europäischer Nachrichtendienste, insbesondere des britischen GCHQ, mit den US-Behörden den innereuropäischen Datenverkehr gefährdet. Die Datenschutzrichtlinie von 1995 geht davon aus, dass in allen Mitgliedstaaten der Union ein gleichwertiges grundrechtskonformes Datenschutzniveau herrscht. Daran bestehen jedoch in Bezug auf Großbritannien nach dem Bekanntwerden des TEMPORA-Programms Zweifel. Gegenwärtig berät der Europäische Gerichtshof für Menschenrechte über eine Beschwerde mehrerer Bürgerrechtsorganisationen. Sollte der Gerichtshof zu dem Ergebnis kommen, dass der britische Auslandsgeheimdienst mit seinen Praktiken und der Kooperation mit der NSA die Menschenrechtskonvention verletzt, müsste die Europäische Kommission informiert werden und Konsequenzen ziehen.

Letztlich betrifft dies aber alle europäischen Geheimdienste: die Snowden-Veröffentlichungen über den nachrichtendienstlich-industriellen Komplex in den USA haben deutlich gemacht, dass die Europäische Kommission sich nicht darauf zurückziehen kann, sie habe im Bereich der Geheimdienste oder der nationalen Sicherheit keine Kompetenzen. Sie muss auf die Einhaltung der Grundrechte-Charta in allen Mitgliedstaaten dringen.

Ich fasse zusammen:

Wenn es nicht gelingt, zwischen Europa und den USA in Kürze zu einer politischen Einigung über die nachprüfbare Begrenzung der Datensammlung durch US-Nachrichtendienste zu kommen und die übrigen Mängel des Safe Harbor-Abkommens zu beheben, muss die Kommissionsentscheidung zu Safe Harbor aufgehoben werden. Generell gilt: Exzessive Überwachung durch unzureichend kontrollierte Geheimdienste gefährdet das Datenschutzniveau und den freien Datenverkehr weltweit.