Untersuchung des LIBE-Ausschusses

zur massenhaften elektronischen Überwachung von EU-Bürgern

Öffentliche Anhörung, Straßburg, 7. Oktober 2013

Beitrag von Peter Hustinx (EDSB)

- Vielen Dank für die Einladung. Im Mittelpunkt unseres heutigen Programms stehen zwar das US Safe Harbour-Konzept und andere Instrumente für internationale Datenübermittlungen, doch möchte ich die Gelegenheit nutzen und auch ein paar allgemeine Anmerkungen zu dem vortragen, was auf dem Spiel steht und was im Hinblick auf die diversen Enthüllungen über die massenhafte elektronische Überwachung von EU-Bürgern getan werden sollte.

- Wir hatten gleich nach der Veröffentlichung der ersten Folge der NSA-Story unsere Bedenken bezüglich möglicher Auswirkungen auf den Datenschutz und andere Grundrechte von EU-Bürgern geäußert. Wir haben um ausführliche Erklärungen und eine Klarstellung des Sachverhalts gebeten, wir haben auf sofortiges und angemessenes Handeln gedrängt, und wir haben seitdem die noch immer nicht beendete Geschichte weiterverfolgt.

- Vizepräsidentin Reding danke ich für die Schritte, die sie im Namen der Europäischen Kommission unternommen hat, und ich weiß auch die sehr

Postanschrift: rue Wiertz 60 – B-1047 Brüssel
Dienststelle: rue Montoyer 30
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel: 02-283 19 00 - Fax: 02-283 19 50

deutlichen Worte zu schätzen, die Frau Merkel und andere führende europäische Politiker gefunden haben.

- Wie Sie wissen, arbeitet die Artikel 29-Datenschutzgruppe derzeit an einer Bewertung der verschiedenen Überwachungsprogramme, der Folgen, die diese für den Datenschutz von EU-Bürgern haben könnten, sowie der Implikationen, die sie für internationale Übermittlungen haben können. Unsere Mitarbeiter leisten einen aktiven Beitrag zu dieser Analyse und beschäftigen sich beispielsweise mit der Anwendbarkeit des EU-Rechts und den in diesem Zusammenhang auftretenden Fragen.

- Während ihrer letzten Plenarsitzung, also erst vor einigen Tagen, erteilte die Artikel 29-Datenschutzgruppe ihren einschlägigen Untergruppen ein Mandat zur Fortsetzung der Analyse der verschiedenen Programme und zur Berichterstattung hierüber im Plenum im Dezember. Danach dürfte die Artikel 29-Datenschutzgruppe in der Lage sein, sich zu allen wichtigen Aspekten des Themas zu äußern.

- Auch wenn noch keine ausreichende Klarheit über alle Fakten besteht – und vielleicht auch nie bestehen wird –, wird uns dies nicht davon abhalten, alle einschlägigen Szenarios zu untersuchen und ihre Folgen zu analysieren. Wir hoffen natürlich auch, irgendwann die Ergebnisse und Schlussfolgerungen anderer laufender Arbeiten nutzen zu können.

- Beim EDSB beschäftigt uns vor allem die Frage, wie unter Umständen Organe und Einrichtungen der EU betroffen waren, und wir werden prüfen, ob es erforderlich sein wird, das derzeitige Informationssicherheitsniveau anzuheben, ganz gewiss auch mit Blick auf die jüngsten Ereignisse bei Belgacom. In diesem Zusammenhang intensivieren wir unsere Kontakte zu allen einschlägigen Dienststellen.

- Nach unseren bisherigen Erkenntnissen sind am auffälligsten i) der Umfang der vorgenommenen Überwachung, ii) die Zahl der privaten Akteure, zu denen auch wohlbekannte Internetriesen gehören, die aktiv oder passiv anscheinend daran beteiligt waren, und iii) die Entwicklung von Schwachstellen und Hintertüren in der Verschlüsselung, die weit reichende nachteilige Wirkungen haben und dem Vertrauen der Öffentlichkeit sehr großen Schaden hinzugefügt haben.

- Derzeit dürfte nur geringer Zweifel daran bestehen, dass wir vor einer existenziellen Herausforderung für unsere Grundrechte und Grundfreiheiten stehen. Wir müssen daher bereit sein, eine Grenzlinie zu ziehen.

- Es müssen starke Garantien für unseren Datenschutz ausgehandelt und angenommen werden. Falls dies nicht gelingt, müssen wir die Aussetzung von Datenübermittlungen in Erwägung ziehen und uns überlegen, ob wir bestehende Abkommen über den Datenaustausch aussetzen.

- Gleichzeitig bietet sich vielleicht aber auch die Möglichkeit, intelligentere Antworten zu finden und die Krise in Chancen zu verwandeln und sie so zu unserem Vorteil zu nutzen.

- Eine erste Schlussfolgerung für mich lautet, dass nunmehr noch mehr Gründe für eine rasche Annahme der Allgemeinen Datenschutzverordnung bestehen, die uns die Möglichkeit geben wird, sehr viel wirksamer als mit dem derzeitigen Rechtsrahmen gegen die privaten Akteure vorzugehen.

- Sie bedeutet mehr Regelungen für Verantwortung und Rechenschaftspflicht und für eine stärkere und kohärentere Aufsicht und Durchsetzung in der gesamten EU. Sie wird auch von wesentlicher Bedeutung für eine Ausdehnung des Anwendungsbereichs des EU-Rechts sein, damit für alle auf dem europäischen Markt Tätigen gleiche Bedingungen herrschen.

- Die Verordnung sollte ferner einen Mechanismus wie den berühmten Artikel 42 einer früheren Fassung vorsehen, mit dem sich die durchaus reale Möglichkeit eines völkerrechtlichen Konflikts bewältigen lässt, dass nämlich Rechtsordnungen widersprüchliche Ansichten über ihre öffentlichen Interessen haben. Grundsätzlich sollte gelten, dass alle Datenübermittlungen im Einklang mit dem EU-Recht zu stehen haben, sofern nicht in einem verbindlichen internationalen Abkommen anderes vorgesehen ist oder eine Justiz- oder Aufsichtsbehörde eine Ausnahme gewährt hat.

- Zu bedenken wäre auch, dass ein Zusatzprotokoll zum Übereinkommen über Cyber-Kriminalität, wie es derzeit beim Europarat diskutiert wird, durchaus Raum für unberechtigten Zugriff durch Geheimdienste auf in anderen Rechtsordnungen gespeicherte Daten bietet. Dieses Thema wurde auch in der Stellungnahme des LIBE-Ausschusses für ITRE zur Strategie für das Cloud-Computing angesprochen. Wir sollten uns nach Kräften dafür einsetzen, dass dieses Zusatzprotokoll nicht angenommen wird.

- Die NSA-Story hat aber noch andere Implikationen, auf die ich jetzt nur kurz eingehen kann. Wenn wir denn eine Grenzlinie ziehen sollen, dann, um damit unsere europäische Datenschutzkultur durchzusetzen, die eine Diskriminierung aufgrund der Staatsangehörigkeit nicht kennt. Wir können daher eine Unterscheidung zwischen US-Personen und Nicht-US-

Personen nicht akzeptieren, weil damit alle EU-Bürger ohne angemessenen gesetzlichen Schutz dastehen.

- Ein weiteres Problem ist die augenscheinlich in großem Maßstab erfolgende *Erhebung* von Daten, bei denen nur für die *Verwendung* Beschränkungen bestehen. Dies ist vollkommen unvereinbar mit der Tatsache, dass wir bei Einschränkungen von Grundrechten so großes Gewicht auf Notwendigkeit und Verhältnismäßigkeit legen.

- Ich sage es daher ganz deutlich: Wir müssen uns jetzt wehren, es geht tatsächlich um „jetzt oder nie".

- Es wäre in diesem Zusammenhang gar nicht so schwierig, für künftige transatlantische Gespräche und gegebenenfalls auch Verhandlungen eine solide Agenda aufzustellen. Darauf komme ich aber am Ende meiner Ausführungen noch einmal zurück.

- Nun möchte ich mich dem US Safe Harbour-Konzept zuwenden, einem der Themen dieser Anhörung. Bei diesem Thema möchte ich meine Ausführungen in drei Teile gliedern: erstens das Konzept der „Angemessenheit", zweitens das „normale" US Safe Harbour, und drittens die Ausnahme aus Gründen der „nationalen Sicherheit" und ähnlicher Interessen.

- Mit der Einführung des Begriffs eines „angemessenen" Schutzniveaus in Artikel 25 der Richtlinie sollte gewährleistet werden, dass Datenübermittlungen an Drittländer nur vorbehaltlich eines ausreichenden Schutzes erfolgen, der von den Gegebenheiten des Einzelfalls abhängt, aber nicht zwangsläufig dem Schutzniveau innerhalb der EU gleichwertig

ist. Dies ist ein pragmatischer Ansatz, der die Vielfalt der Rechtskulturen in der Welt wiederspiegelt.

- Der Begriff der „Angemessenheit“ wurde in einer 1998 angenommenen Stellungnahme der Artikel 29-Datenschutzgruppe näher ausgeführt, die die Grundlage aller Angemessenheitsentscheidungen der Kommission war, und dies auch im Fall US Safe Harbour. Angemessener Schutz erfordert die Einhaltung eines Kerns von „inhaltlichen“ Grundsätzen und „verfahrensrechtlichen“ bzw. mit der „Durchsetzung im Zusammenhang stehenden“ Erfordernissen, damit eine gute Befolgungsrate der Vorschriften, Unterstützung und Hilfe für betroffene Personen und angemessene Entschädigung gewährleistet sind. Mit anderen Worten: ein „objektiver“ oder „funktionaler“ Ansatz.

- Im Abschnitt über inhaltliche Grundsätze werden in der Stellungnahme die Beschränkung der Zweckbestimmung, die Datenqualität und -verhältnismäßigkeit, die Transparenz, die Sicherheit der Daten, das Recht auf Zugriff und Berichtigung sowie Beschränkungen der Weiterübermittlung aufgeführt. In der Stellungnahme heißt es aber auch, dass Ausnahmen *„mit Artikel 13 der Richtlinie in Einklang zu stehen haben“* (siehe S. 7). Gemäß diesem Artikel 13 sind Ausnahmen zum Schutz der Sicherheit des Staates und der öffentlichen Sicherheit möglich, sofern sie notwendig sind. Diese Bestimmung gilt zwar nicht in einem Drittland, doch verlässt man sich sinngemäß auf sie.

- Im Zusammenhang mit den vertraglichen Bestimmungen, die Angemessenheit herbeiführen sollen, wird in der Stellungnahme auch das Problem des „vorrangigen Rechts“ erörtert (siehe S. 22f.). Eine der Schlussfolgerungen lautet: *„Länder, in denen beim Informationszugang die Befugnisse der staatlichen Behörden über das hinausgehen, was*

durch die weltweit angenommenen Normen des Schutzes der Menschenrechte erlaubt ist, sind keine sicheren Bestimmungsorte für Übermittlungen auf der Grundlage von Vertragsklauseln“ (siehe S. 25). Dasselbe würde natürlich auch auf Angemessenheitsbefunde zutreffen.

- Die US Safe Harbour-Regelung war von Anfang an umstritten. Im Verlauf der Verhandlungen zwischen der Kommission und dem US-Handelsministerium hat die Artikel 29-Datenschutzgruppe eine Reihe äußerst kritischer Stellungnahmen angenommen. Nach dem Abschluss der Verhandlungen jedoch und nach der Annahme der Safe Harbour-Entscheidung durch die Kommission hat sich die Artikel 29-Datenschutzgruppe sehr dafür engagiert, sie mit Leben zu erfüllen und ihre Funktionsweise zu verbessern.

- Gestatten Sie mir den deutlichen Hinweis, dass das Gros der Safe Harbour-Arbeiten für die EU-Datenschutzbehörden auf nationaler Ebene stattfindet. Organe und Einrichtungen der EU übermitteln zwar gelegentlich auch personenbezogene Daten an Drittländer, doch ist davon Safe Harbour nicht betroffen. Aus strategischer Sicht fällt die Beurteilung jedoch ganz anders aus. Wir waren daher in die verschiedenen Phasen des Prozesses eng eingebunden.

- Man kann mit Fug und Recht behaupten, dass Safe Harbour nur langsam angelaufen ist, dann aber kontinuierlich an Fahrt gewonnen hat. Wir glauben, dass wesentliche Verbesserungen erreicht worden und die meisten Probleme nunmehr gelöst sind. Dies gilt insbesondere für die aktivere Rolle des US-Handelsministeriums bei der Selbstzertifizierung sowie für die Rolle der *Federal Trade Commission* bei der Durchsetzung. Safe Harbour bietet also durchaus gewisse Vorteile.

- Problematisch ist nach wie vor, dass es weder einen umfassenden Überblick über SH-Praktiken und Erfahrungen, noch ausreichend zuverlässige Statistiken gibt. Aus diesem Grund wurde eine Datenschutzkontaktgruppe aus Vertretern beider Seiten eingerichtet, die über eine ganze Reihe von Jahren aktiv war. Derzeit wartet die Artikel 29-Datenschutzgruppe auf den von der Europäischen Kommission angekündigten Bewertungsbericht.

- Die Einleitung zu den Grundsätzen des „sicheren Hafens“ (siehe Anhang I der Entscheidung der Kommission vom 26. Juli 2000) besagt, dass die Geltung dieser Grundsätze begrenzt werden kann, *„insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss…“*. Eine ähnliche Bestimmung befasst sich mit dem vorrangigen Recht. Es sollte jedoch immer berücksichtigt werden, dass wir es in diesem Zusammenhang mit Ausnahmen von Grundrechten zu tun haben, die der Gerichtshof und der Europäische Gerichtshof für Menschenrechte immer restriktiv auslegen.

- Außerdem ist der zitierte Wortlaut sorgsam formuliert (es heißt dort „*insoweit*“), während wir es zur Zeit offenbar in allen Fällen, in denen Unternehmen durch eines der Massenüberwachungsprogramme ausgespäht wurden, mit einer systematischen Nichteinhaltung der SH-Grundsätze zu tun haben.

- Vermutlich sind sich die beiden Seiten nicht darüber einig, ob diese Ausnahme tatsächlich galt. Diese Frage sollte auf jeden Fall verneint werden, wenn wir davon ausgehen, dass die einschlägigen Überwachungsprogramme tatsächlich über ihr Ziel hinausschossen. Auch

hier ist zu vermuten, dass sich die beiden Seiten bezüglich dieser Schlussfolgerung nicht einig sind.

- Hier könnte ein Anlass gegeben sein, sich auf Artikel 4 der Entscheidung der Kommission zu berufen, der besagt: *„Diese Entscheidung kann jederzeit im Licht der Erfahrungen mit ihrer Anwendung angepasst werden und/oder dann, wenn das durch die Grundsätze (…) gewährte Schutzniveau in die Rechtsvorschriften der USA übernommen wird“*. Entsprechende Nachweise könnten beispielsweise in einem Bewertungsbericht der Kommission vorgelegt werden, wie er bis zum Jahresende erwartet wird.

- Alle weiteren Schritte sollten dann von der Kommission in Absprache mit den Vertretern der Mitgliedstaaten im Artikel 31-Ausschuss unternommen werden. In diesem Fall würde der Schwerpunkt eher auf der Frage *„Wie ist mit übermäßiger Überwachung umzugehen?“* oder auf *„fehlender Einigung bei diesem Thema“* und weniger auf der Wirksamkeit des SH als einem Instrument zur Gewährleistung angemessenen Schutzes liegen. Der Bericht der Kommission könnte allerdings auf beides eingehen und damit einen inhaltlichen Beitrag zu Gesprächen und Verhandlungen mit der US-Seite leisten. Gestatten Sie mir in diesem Zusammenhang die Bemerkung, dass wir Safe Harbour nicht einfach wegwerfen sollten, ohne zu prüfen, ob nicht Raum für Verbesserungen besteht.

- Eine Agenda für Verbesserungen des SH *„im Licht der Erfahrungen“* könnte mit anderen Fragen und Bedenken kombiniert werden, entweder im Rahmen der Zusammenarbeit in der Strafverfolgung oder im Handel, oder langfristig im Hinblick auf ein neues internationales Abkommen mit Grundsätzen für eine rechtmäßige Überwachung.

- Wir sollten vor diesem Hintergrund auch nicht vollständig ausschließen, dass ein erheblicher Teil der Lösung vielleicht aus den USA kommt. Dabei kann es sich um Empfehlungen des *US Privacy and Civil Liberties Oversight Board* oder der von der US-Administration eingesetzten internen Expertengruppe zu mehr Transparenz oder um andere sinnvolle Garantien handeln.

- Es wäre auf jeden Fall klug, sich alle Optionen offen zu halten und gleichzeitig alle Möglichkeiten für ein konstruktives Engagement auszuloten.

* * * * *