Mit Europarecht gegen die amerikanischen und britischen Abhöraktionen? Teil 1: NSA

verfassungsblog.de/mit-europarecht-gegen-amerikanischen-und-britischen-abhoeraktionen-teil-1-nsa/

Franz C. Mayer Mo 18 Nov 2013

Mo 18 Nov 2013

Ob die NSA wirklich so mächtig ist? Wochenlang sollen die Digitalschlapphüte unbescholtene Bürger in Washington DC abgehört haben bis sie merkten, dass man die Vorwahl von Washington DC mit der Ländervorwahl von Ägypten verwechselt hatte. Wochenlang – das macht doch stutzig. Vielleicht hat die NSA längst den Überblick verloren.

Wer sich darauf nicht verlassen will und doch lieber auf das Recht vertraut hat ein Problem: Auf welches Recht? Mit dem deutschen Straf- oder gar Verfassungsrecht wird man gegen das durch Edward Snowden bekannt gewordene flächendeckende anlasslose Ausspähen von privaten Daten durch die NSA nicht sehr weit kommen. Eine bessere Antwort: Europarecht.

Nun sind die USA bekanntlich nicht Mitglied der Europäischen Union. Es ist kein europäisches Recht im engeren oder weiteren Sinne in Sicht, welches unmittelbar gegen die Maßnahmen der NSA („PRISM“, „XKeyscore“und anderes) in Stellung gebracht werden könnte. Auch wenn sie die Cybercrime Convention des Europarates ratifiziert haben, so sind die USA bei der Europäischen Menschenrechtskonvention nicht dabei.

Es bestehen aber eine Reihe von EU-bezogenen rechtlichen Hebeln, mit denen man auf die USA einwirken kann.

Das Europäische Parlament hat im Oktober 2013 einen Entschließungsantrag angenommen, in dem gefordert wird, das SWIFT-Abkommen von 2009 auszusetzen. Es geht dabei um die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der EU an die USA um die Finanzierung des Terrorismus aufzuspüren. Und auch die Gespräche über eine EU-US Freihandelszone („TAFTA“ oder „TTIP-Abkommen“) sollten – so EP-Präsident Schulz – auf Stop gestellt werden, solange die Datenschutzfrage ungeklärt ist. Das EP hat sich freilich schon einmal mit seiner Echelon-Untersuchung ohne großen Erfolg gegen die US-amerikanischen Geheimdienstpraktiken gestellt. Zweifler werden zudem betonen, dass die USA ja gerade nicht mehr auf das SWIFT-Abkommen und die Datenübermittlung auf dessen Grundlage angewiesen sind, wenn die NSA sich einen direkten Zugang zu den SWIFT-Servern erschlichen hat. Und nicht wenige meinen, dass das ökonomische Interesse am transatlantischen Freihandel auf europäischer Seite sehr viel höher ist als auf amerikanischer Seite.

Einen wirksameren rechtlich-ökonomischen Hebel verspricht vor diesem Hintergrund die Thematisierung der sogenannten Safe harbor-Absprache zwischen den USA und EU. Nach der Datenschutz-Richtlinie 95/46/EG ist die Übermittlung personenbezogener Daten in ein Drittland nur zulässig, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet. Die Kommission kann feststellen, dass ein Drittland ein angemessenes Schutzniveau gewährleistet. Darum geht es in der Safe harbor-Absprache. Es handelt sich dabei genau besehen nicht um ein echtes Abkommen, sondern eine aus juristischer Perspektive einigermaßen skurrile Konstruktion von Selbstverpflichtung, bei der eine Verständigung über ein Verfahren erfolgte, in dem sich die US-amerikanische Seite im Kern selbst attestieren kann, dass sie europäische Datenschutzstandards einhält. Safe harbor ist die Grundlage für ökonomische Aktivitäten zahlreicher US-amerikanischer Unternehmen. Diese Grundlage lässt sich aus zwei Richtungen in Frage stellen.

Einmal könnte die Europäische Kommission tätig werden. Sie hat für die USA im Kontext des Safe-harbor-Mechanismus und auf Grundlage der Datenschutz-Richtlinie durch eine Entscheidung im Jahre 2000 (2000/520/EG) festgelegt, dass in den USA unter bestimmten Bedingungen aus EU-Sicht ausreichende Datenschutzstandards bestehen. Diese Entscheidung 2000/520 kann von der Kommission jederzeit überprüft und aufgehoben werden. Schließlich haben sich grundlegend neue Tatsachen ergeben.

Zum anderen könnten die Datenschutzbehörden der Mitgliedstaaten hier tätig werden. Die Entscheidung der Kommission verleiht diesen Behörden nämlich Befugnisse, zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung an eine Organisation auszusetzen (Art. 3 Abs. 1 Entscheidung 2000/520, Art. 25 Abs. 6 Datenschutz-Richtlinie). Dies kann dann geschehen, wenn „eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden“; wenn Grund zur Annahme besteht, dass die jeweilige Durchsetzungsinstanz – auf US-amerikanischer Seite – „nicht rechtzeitig angemessene Maßnahmen ergreift bzw. ergreifen wird, um den Fall zu lösen“; „wenn die fortgesetzte Datenübermittlung für die betroffenen Personen das unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde, und wenn die zuständigen Behörden in den Mitgliedstaaten die Organisation unter den gegebenen Umständen in angemessener Weise unterrichtet und ihr Gelegenheit zu Stellungnahme gegeben haben“.

Es kommt hier freilich auf die Befugnisse der jeweiligen Datenschutzbehörde an, die Kommissions-Entscheidung verweist ja auf diese. Wie sieht es in Deutschland aus?

Auf Bundesebene findet sich wenig. Im Kern bestehen für die zuständige Behörde, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, lediglich Kontrollbefugnisse und das Mittel der Beanstandung nach § 25 BDSG. Für das TKG verweist § 115 Abs. 4 TKG auf die allgemeinen Befugnisse des Bundesbeauftragten. Hierbei handelt es sich um die Feststellung eines Datenschutzverstoßes gegenüber der zuständigen Aufsichtsstelle und die Aufforderung der Stellungnahme. Das klingt nicht gerade furchteinflößend.

Auf Länderebene sieht es anders aus. Die zuständigen Länderbehörden können nach § 38 Abs. 5 BDSG zur „Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz“ „Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen“. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann die Behörde sogar die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen. Nach § 43 BDSG besteht für die Länder auch die Möglichkeit Bußgelder zu verhängen, und zwar bis zu 300.000 Euro.

Was heißt das konkret? Einem großen Konzern mit Sitz in Deutschland, der seine Personaldaten in den USA lagert oder verarbeiten lässt, könnte genau dies durch die zuständige Datenschutzbehörde untersagt werden. Oder konkreter: Unternehmen und öffentlichen Stellen, die einen amerikanischen Cloud-Dienst wie Dropbox oder iCloud einsetzen, könnte die Übermittlung von Daten in diese Dienste untersagt werden. Und soweit die Nutzung von Facebook sich mit der Übermittlung von Daten verbindet, könnte auch dies untersagt werden. Anderes Beispiel: Einer deutschen Universität, die ihren gesamten Email-Dienst auslagern und über Gmail abwickeln möchte – dieses Outsourcing des eigenen Email-Dienstes für sämliche Universitätsangehörigen an Gmail haben mehrere große US-Universitäten wie die NYU oder die Columbia University jüngst unternommen – wird dies untersagt.

Auch in anderen Mitgliedstaaten bestehen Befugnisse der jeweiligen nationalen Datenschutzbehörde, die für die Umsetzung von Art. 3 Abs. 1 Entscheidung 2000/520 eingesetzt werden könnten. In Frankreich beispielsweise verfügt die CNIL (Commission nationale de l’informatique et des libertés) über weitreichende Befugnisse. Sie ist u.a. befugt, Normen für die Erstellung und Benutzung von besonderen Kategorien von Datenbanken, die persönliche Dateien beinhalten, zu erlassen. Und es können Bußgelder ebenfalls bis zu 300.000 Euro verhängt werden. In Spanien hat die AEPD (Agencia Española de Protección de Datos) ähnliche Befugnisse. Die höchsten Bußgelder dort können bis zu 600.000 Euro betragen.

Die Datenschutzbeauftragten des Bundes und der Länder haben auf die Verbotsmöglichkeiten in einer gemeinsamen Erklärung im Juli 2013 hingewiesen. Und im August 2013 hat es einen Brief der Art. 29 Working Party, der Arbeitsgruppe nach Art. 29 der Datenschutz-Richtlinie, an die Kommission gegeben, der ebenfalls auf die Überprüfung der Safe harbor-Prinzipien drängt.

All dies klingt ermutigend. Aber es ist gut möglich, dass es bei wechselseitigen Briefen und Hinweisen bleibt und die Entscheidungsverantwortung schlicht zwischen Kommission und nationalen Behörden hin- und hergeschoben wird. Die Gründe dafür wären nicht schwer auszumachen:

Wieviel kann man von einer Kommission erwarten, die sich in den letzten Monaten ihrer Amtszeit befindet und deren Präsident offenbar die Vorstellung einer weiteren Amtszeit noch nicht aufgegeben hat, dementsprechend kein Interesse daran haben dürfte, bei den Regierungen der Mitgliedstaaten – die den Kommissionspräsidenten vorschlagen – durch besonders eigenständiges Handeln aufzufallen. Auf die Regierungen sollte man schon gar nicht zählen in der NSA-Frage, weil deren Haltung nicht selten weniger von der Sorge um dem Grundrechtsschutz der Unionsbürger getragen scheint ist als eher von einem neidischen „Hätten wir auch gerne“, wenn es um die Kapazitäten der NSA geht.

Und die nationalen Datenschutzbehörden? Diese können sich die Sache einfach machen und auf die Verantwortung der Kommission verweisen, die Entscheidung zu überprüfen. Die Kommission hat aber möglicherweise das besagte politische Problem. Daneben erscheint die Position nicht völlig abwegig, der zufolge die Entscheidung lediglich einen Rechtsrahmen abgibt, auf dessen Grundlage die nationalen Behörden schon heute entscheiden könnten. So lässt sich der Ball wieder zurück zu den nationalen Behörden spielen.

In Irland – vielleicht nicht ganz zufällig europäischer Sitz einer Reihe von IT-Unternehmen – hat es bereits Beanstandungen auf nationaler Ebene gegeben, die irische Datenschutzbehörde hat aber keinen Anlass gesehen einzugreifen. Bei Untätigkeit der Datenschutzbehörden lässt sich über eine Verpflichtungsklage vor den zuständigen Gerichten – in Deutschland den Verwaltungsgerichten – nachdenken.

In Deutschland erscheint die parzellierte Zuständigkeit der einzelnen Länder und des Bundes nicht nur unübersichtlich, sondern wahrscheinlich kontraproduktiv, eigentlich nicht mehr zeitgemäß: Wären die Datenschutzbehörden der Länder mit ihren jeweils paar Leuten überhaupt von ihrer Größe her in der Lage für einen in dem jeweiligen Bundesland belegenen multinationalen Konzern beispielsweise die Personaldatenverarbeitung in den USA zu überprüfen? Und wäre man bereit, den politischen Druck auszuhalten, der entstünde, wenn Unternehmen bei Verboten wie sie oben skizziert sind ihren Wegzug aus einem Bundesland androhen, verbunden mit einem entsprechenden Verlust von Arbeitsplätzen?

Zusammenfassend: Ja, das Europarecht kann gegen die NSA helfen. Besser als der hilflose Nationalstaat könnte die EU „Datensouveränität“ der Unionsbürger wirksam schützen, es reicht eben nicht aus, auf die „Klugheit der Nutzer“ zu verweisen. Der Ansatz ist dabei letztlich ein indirekter. Durch Einwirkung auf politische und ökonomische Interessen der USA und in den USA könnte im Ergebnis ein besserer Grundrechtsschutz für Unionsbürger gegen Maßnahmen der amerikanischen Regierung erreicht werden. Es besteht mit Blick auf die technologische Entwicklung (insbes. Cloud Computing) an sich ja ein allseitiges Interesse an einer politischen und rechtlichen Klärung der Situation, auch in den USA gibt es eine Diskussion. Die EU kann dabei ihre Marktmacht gegenüber den USA einsetzen. Eine belastbare rechtliche Klärung verspricht am ehesten perspektivische Stabilität.

Wie oben gezeigt gäbe es sogar unter dem derzeitigen unscharfen Hybridregime eines Safe-harbor-Ansatzes wirksame rechtliche Hebel. Safe harbor wäre schlicht anzuwenden, jedenfalls aber zu überprüfen und möglicherweise sogar auszusetzen, gefordert sind die Kommission und die nationalen Behörden.

Werden diese Möglichkeiten nicht genutzt, dann muss der rechtliche Rahmen wohl doch besser geklärt und gefestigt werden. Das Ziel wären dann „binding treaties“, hartes Recht in einem völkerrechtlichen Abkommen mit hohen Standards und klaren Regeln. Minimalziel aus europäischer Sicht wäre dabei mit Blick auf die NSA-Aktivitäten mindestens das auch sonst im Freihandel verbreite Prinzip der Inländerbehandlung: Unionsbürger und EU-Unternehmen müssen in Datenschutzbelangen mindestens Gleichbehandlung mit US-Bürgern in Sachen Datenschutz gegen Geheimdienste bekommen. Bestenfalls wird man damit aber zu einem Zustand kommen, in dem vielleicht dann eines Tages die Vorwahl von Wuppertal mit der Ländereinwahl von Ägypten verwechselt wird.

Diese Fragen sollen auch in der neuen EU-Datenschutzgrundverordnung angesprochen werden. Ein intensiv umkämpfter Art. 42, eine „Lex NSA“ aus einem früheren Entwurf, der wohl nicht zuletzt auf amerikanischen Druck zunächst aus dem Kommissions-Entwurf verschwand, spielt hier eine wichtige Rolle. Diese Bestimmung findet sich als Art. 43a in der im EP am 21. Oktober 2013 beschlossenen Ausschussfassung der EU-Datenschutzverordnung.

Diese Bestimmung besagt, dass keine Entscheidung eines Gerichts oder einer Verwaltungsbehörde eines Drittstaats, die private Datenhalter zur Preisgabe personenbezogener Daten von Unionsbürgern verpflichtet, anerkannt oder durchgesetzt werden kann, wenn dafür kein völkerrechtlicher Vertrag mit diesem Drittstaat auf Ebene der EU oder eines Mitgliedstaates besteht. Dies richtet sich gegen die Praxis der USA, insbesondere aufgrund sogenannter „National Security Letters“ Internet- oder Telekommunikationsanbieter in den USA zu verpflichten, Daten der Bürger von Drittstaaten an Bundesbehörden weiterzugeben, ohne dass diese Weitergabe offen gelegt werden darf. Die amerikanischen Internetkonzerne müssten sich dann entscheiden, ob sie gegen europäisches oder amerikanisches Recht verstoßen, dies sollte einen politischen Druck entfalten, der zu völkerrechtlichen Verträgen in diesen Fragen führt. Art. 43a dürfte indessen nicht weiterhelfen, so die Kritik, wenn die NSA die Daten von Google oder Yahoo-Nutzern außerhalb der USA abfischt , etwa vom britischen Partnerdienst bezieht. Oder womöglich vom BND? Gleichwohl wird die Position der Bundesregierung zu Art. 43a in den Beratungen im Ministerrat Aufschluss darüber geben, wie ernst man es mit dem Datenschutz meint. Der Rat beschließt hier mit qualifizierter Mehrheit, Großbritannien und Deutschland könnten also überstimmt werden.

Auf die gutwillige Kooperationswilligkeit der amerikanischen Akteure sollte man bis auf weiteres so oder so nicht allzu viel Hoffnung setzen. Dies gilt auch für die privaten Akteure. Symptomatisch dürfte die Position sein, die derzeit Google in einem beim EuGH anhängigen Verfahren (Rs. C-131/12) einnimmt. Danach ist das europäische Recht sowieso gar nicht mehr einschlägig, sobald eine Google-Abfrage auf Server in Kalifornien zugreift. Diese Argumentation von Google ist entlarvend.

Vielleicht muss Teil einer Lösungsstrategie deswegen tatsächlich auch sein, dass Cloud Computing deutlicher territorial verortet wird, zumindest entsprechende Angebote bestehen, weil man selbst für den Fall, dass es rechtliche Zusagen der USA gibt, auf deren Einhaltung nicht mehr vertrauen kann. Technisch ist hier auch beim Email-Verkehr durch gezieltes Routing, beispielsweise auf Schengen-Staaten beschränkt, mehr möglich als es die landläufige Vorstellung vom Internet als unregulierbarem Medium nahe legt. Auch in der Schutzgewährleistungsdimension bestätigt sich Larry Lessigs These „Code is law“: die technischen Weichenstellungen zur Netzarchitektur sind im Kern vielfach bereits Entscheidungen von rechtlicher Tragweite.

Hier geht es auch um Fragen der gezielten Förderung von Forschung und Industrien, bei der auf europäischer Seite ganz offenbar Boden verloren worden ist. Auch hier besteht europapolitischer Handlungsbedarf.

Abschließend muss man bei alledem freilich auch sehen, dass die amerikanische Seite es nicht verstehen wird, wenn einerseits hohe Anforderungen an die USA gerichtet werden, zugleich auf der anderen Seite der Mitgliedstaat Großbritannien mit seinen Geheimdiensten flagrante Verletzungen von Datenschutzrechten in der EU begeht und damit durchkommt. Dies führt zu einem zweiten Teil meiner Überlegungen: Mit dem Europarecht gegen den GCHQ?

Der Beitrag beruht auf Vorträgen bei einem Fachgespräch „Möglichkeiten des Rechtsschutzes gegen Abhörprogramme der USA und Großbritanniens (PRISM und TEMPORA)“ bei der Bundestagsfraktion Bündnis 90/Die Grünen am 20.8.2013 und auf einem Workshop der „Glienicker Gruppe” am 31.8.2013.

SUGGESTED CITATION Mayer, Franz C.: *Mit Europarecht gegen die amerikanischen und britischen Abhöraktionen? Teil 1: NSA, VerfBlog,* 2013/11/18, http://verfassungsblog.de/mit-europarecht-gegen-amerikanischen-und-britischen-abhoeraktionen-teil-1-nsa/.