

**Interview von Gudrun Seidl, cenjur,
zum SWIFT II-(TFTP)Abkommen mit der ehemaligen
Bundesjustizministerin Professor Dr. Herta Däubler-Gmelin**

Berlin/Brüssel, 29.07.2010, [cen] Frau Däubler-Gmelin, Ihnen liegt das EU/USA-Abkommen (SWIFT-oder auch TFTP-Abkommen genannt) vom 24.06.2010 nebst den Ratsdokumenten dazu vor.

Hätte das Abkommen in dieser Form verabschiedet werden dürfen?

HDG: Nein, ich halte die Verabschiedung für einen großen Fehler. Zwar hat das Europäische Parlament, das nach dem Lisabonner Vertrag ja solchen Vereinbarungen zustimmen muss, Verbesserungen gegenüber dem früheren Vertrag, den die EU-Regierungen abgesehnet hatten, erreicht. Aber, das Parlament als Vertreter der Bürgerinnen und Bürger in Europa, hätte nicht zustimmen dürfen. Es hätte zunächst darauf drängen müssen, dass die Voraussetzungen für den Grundrechts- und Datenschutz innerhalb der EU abgestimmt werden. Erst dann hätte es zu einem Abkommen zwischen der EU und den USA kommen dürfen, in dem dann auch die Grund- und Freiheitsrechte geschützt sind. Das ist nicht geschehen – und so werden diese Versäumnisse für zu Unrecht Betroffene in den nächsten fünf Jahren der Geltung dieses Abkommens sehr problematisch werden; sie werden den

Schutz der Persönlichkeitsrechte insgesamt schwächen und die Stellung der Datenschutzbehörden der Mitgliedsstaaten der EU unterminieren. Kurz: der Datenschutz beim Transfer von persönlichen Daten über die Grenzen bleibt mindestens für fünf Jahre weitestgehend auf der Strecke.

Was ist/wäre die Alternative zu diesem Abkommen (gewesen), bilaterale Verträge, angepasst an den jeweiligen Zustand des Staates?

HDG: In dem Abkommen geht ja um ein an sich vernünftiges Anliegen, nämlich die gemeinsame Verhinderung der Finanzierung international agierender Terrorgruppen durch die Überwachung von Überweisungen über Landesgrenzen. Diese Überwachung hätte die EU mit den entsprechenden Grundrechts- und Verfahrenssicherungen selbst regeln können und müssen. Im Anschluss daran hätte die EU mit den USA dann einen Vertrag schließen

können, der berechtigten US-Behörden auf berechnete Einzelanforderung und unter Vorlage der notwendigen datenschutzrechtlichen Garantien die Möglichkeit gibt, Informationen zu erhalten.

Das SWIFT-Abkommen jedoch lässt den schlichten Transfer riesiger Datenmengen mit dem großen Staubsauger durch US-Behörden zu, wobei man ja weiß, wie in den USA mit Daten umgegangen wird. Das geht in rechtlich zulässiger Weise nicht.

Das Trostpflaster der EU-Kommission, sie plane jetzt ein eigenständiges europäisches Verfahren zur Bekämpfung der Finanztransaktionen zur Terrorunterstützung, reicht nicht aus. Dieses Verfahren hätte die EU längst einrichten können; das EU-Parlament hätte darauf bestehen können und müssen.

Wie beurteilen Sie unter dem Gesichtspunkt der Freiheit und des Rechts das Zustandekommen des Abkommens und seinen Inhalt?

HDG: Ganz offensichtlich stand die EU stark unter dem politischen Druck, den USA nicht zu viele ihrer Forderungen abzuschlagen. Das ist bedauerlich, zumal der Schutz von Bürgerrechten bei der Terrorbekämpfung ja auch von EU-Politikern in ihren Sonntagsreden als wichtig herausgestellt wird. Dieser Schutz entspricht den europäischen Werten und den Forderungen des letzten Winter in Stockholm beschlossenen EU-Programms zur Umsetzung der Grundrechte in der EU. Es ist bedauerlich, dass auch das EU-Parlament sich letztlich dem Druck gebeugt oder angepasst hat: die erreichten Verbesserun-

gen reichen nicht aus und die vereinbarte fünfjährige Dauer ist zu lang.

Instanzzüge – Rechtsmittel – US-amerikanisches Recht - EU-Recht - Gerichtshof der EU – können Sie erklären, wie das alles zusammenhängt, was damit gemeint ist und was ich tun kann / tun muss?

HDG: Das SWIFT-Abkommen betrifft nicht Handlungen deutscher Behörden, deshalb gibt es auch keinen – deutschen – Rechtsweg gegen solche Handlungen.

Das Abkommen hat den Datentransfer zwischen der EU und den USA geregelt und dabei auf EU-Seite Handlungen und Bewertungen von Europol vorgesehen. In den USA geht es dann um das, was die US-Behörden, die die Informationen erhalten, mit diesen Daten machen.

Wie kann sich nun ein Betroffener gegen seiner Meinung nach unrechtmäßiges Vorgehen von Europol wehren? Nun, die Rechtmäßigkeit des Verhaltens von Europol im Klageweg kann auf dem Klageweg grundsätzlich nach EU-Recht beim EuGH in Luxemburg überprüft werden – insoweit sind die Aussagen von BMI und BMJ korrekt. Was beide Ministerien jedoch nicht ausführen ist, dass das den Betroffenen im Regelfall wenig nutzt. Im Zweifel sind ja ihre Daten und die mit ihnen verbundenen Informationen, z.B. über Geschäftsbeziehungen oder persönliche Verbindungen längst transferiert. Sie sind im Zweifel in den USA weg, verteilt und verwendet. Die Betroffenen EU-Bürger könnten vor dem EU-Gericht nur im Nachhinein die Unrechtmäßigkeit des Verhaltens von Europol feststellen lassen. Dass auf diesem Weg im konkreten Fall überhaupt Schadensersatzforderungen durchgesetzt wer-

den könnten, halte ich für überaus zweifelhaft.

Auch die Möglichkeiten der Betroffenen, in den USA gegen dortige Verletzungen des Datenschutzes, also von Grundrechten, zu klagen, sind trotz des Wortlauts des Abkommens mehr als ungewiß. Zum Einen müssen die Betroffenen ja wissen, wo und wie sie vorgehen können. Das geht nur entsprechend der US-Regeln in englischer Sprache mit Unterstützung (teurer) US-Anwälte. Außerdem ist es unklar, ob das US-Recht im Zeitpunkt des Inkrafttretens des SWIFT–Abkommens überhaupt eine Klagebefugnis für betroffene Nicht-US-Staatsbürger vorsieht; darauf haben die europäischen Datenschutzbeauftragten mit Recht hingewiesen. Die Einschätzung des Bundesministeriums der Justiz halte ich in diesem Punkt mindestens für außerordentlich optimistisch – bisher entspricht sie der US-Rechtssituation nicht und gibt auch keine Auskunft darüber, wo, wie und inwieweit bei Schäden eine Haftung der US-Behörden durchgesetzt werden könnte.

Wie sehen Sie den datenschutzrechtlichen Standard des Abkommens, gemessen an dem, was wir in Deutschland gewohnt sind?

HDG: Er ist ungenügend. Das Bundesverfassungsgericht hat in zahlreichen Grundsatzentscheidungen klargestellt, dass Datenschutz Persönlichkeitsschutz und Schutz der Menschenwürde bedeutet. Deshalb sind wir in Deutschland hier zu Recht sehr streng. Das Bundesverfassungsgericht hat jetzt in seiner sog. Online-Entscheidung zusätzlich ausgeführt, dass der Staat auch gewährleisten muss, dass die IT- und Kommunikationssysteme

vor Zugriffen geschützt sind, weil sonst unsere freiheitliche Gesellschaftsordnung in sich zusammenbricht.

Das ist sehr wichtig, weil damit klargestellt ist, dass jeder Bürger sich im täglichen Leben darauf verlassen können muss, dass er auch bei der Nutzung der IT- und Kommunikationssysteme unseres Alltags **n i c h t** überwacht wird. Vielmehr sind Eingriffe auch in die IT- und Kommunikationssysteme nur bei Vorliegen klarer Hinweise auf Straftaten und anderer gesetzlicher Voraussetzungen und dann nur gleichzeitig mit klaren Schutzverfahren zulässig.

Auch diese Verfassungsgrundsätze respektiert die SWIFT–Vereinbarung zwischen EU und USA leider nicht. Gerade deshalb ja unser Ärger darüber, dass das EU-Parlament nun doch zugestimmt hat.

Wie praxistauglich ist dieses Abkommen zur Überprüfung der Abläufe durch individuell betroffene Dritte (selbst der Bundesdatenschutzbeauftragte geht auf Anfrage von cenjur davon aus, dass über ihn kein tauglicher Rechtsschutz zu erlangen ist)?

HDG: Leider definiert das SWIFT–Abkommen die Praxistauglichkeit aus der Sicht der US-Geheimdienste, nicht aus dem Interesse des Schutzes der Grund- und Freiheitsrechte der Bürger. Das ist das Problem.

Diese Frage wurde von cenjur an den Bundesdatenschutzbeauftragten (BfDI) gerichtet:

§ Bestehen für die SWIFT-Mitarbeiter straf- oder bußgeldrechtliche Risiken aufgrund des de facto ungeschützten

Datentransfers in der USA, der die Schutzpositionen nach dem BDSG leerlaufen de facto leerlaufen lässt?

§ *Bestehen darüber hinaus Teilnahmerisiken i.S.v. §§ 26, 27 StGB bzw. § 14 OWiG für Behördenmitarbeiter, die diesen ungeschützten Datentransfer fördern?*

Antwort des BfDI: Die SWIFT-Mitarbeiter, die Banktransaktionsdaten (auch) deutscher Bankkunden nach Prüfung und Freigabe durch Europol (Art. 4 Abs.4 des am 27.7. im EU-Amtsblatt L 195/5 ff. veröffentlichten Abkommens) für das US-Finanzministerium gemäß Art. 4 Abs. 5

Satz 2 "bereitstellen", also die Übermittlung vom niederländischen Server in die USA veranlassen, tun dies entweder von der belgischen SWIFT-Zentrale aus oder am Serverstandort in den Niederlanden, so dass eine evtl. Strafbarkeit zunächst nach Maßgabe des belgischen bzw niederländischen Strafrechts zu prüfen wäre...vollständige Antwort siehe unten

HDG: Ich halte die Beantwortung durch den BfDI für korrekt, beantworte sie deshalb nicht

Frau Däubler-Gmelin, ich danke für das Interview

Die vollständigen Antworten des BfDI, BMJ und BMI sowie Antworten von Europa-Abgeordneten zum SWIFT (TFTP)-Abkommen finden Sie hier:

<http://www.cenjur.de/europa/swift/swiffraant.htm>

Sie berichten:



<http://rsw.beck.de/rsw/shop/default.asp?docid=306689&docClass=NEWS&site=MMR&from=mmr.root>

Ganz besonders möchte ich mich bei Herrn Rechtsanwalt Dr. Carsten Wegner bedanken, der sehr interessante Fragen zum SWIFT-Abkommen stellte und meine neugierigen Fragen beflügelte. Vielen wird Dr. Wegner – wie mir - durch seine wirtschaftsstrafrechtlichen Nachrichten bekannt sein, mit deren Herausgabe er bei Professor Hans Achenbach begann und diese bis heute fortführt.

Herta Däubler-Gmelin danke ich, die sich sofort – im Gegensatz zum Deutschen Richterbund – zu diesem Interview bereitfand. Mögen die von cenjur zusammengetragenen Fakten und Informationen zu einem EU-eignen Abkommen Grundlage und Ansporn sein. Europa ist die Zukunft unserer Kinder, die wir bauen. Verlernen wir nie, mit den Augen eines Kindes zu sehen: von unten nach oben.
Gudrun Seidl, cenjur

