

# SWIFT: Europa „befreit“ Banktransaktionsdaten vom Grundrecht auf Datenschutz

Grundrechte-Report 2010, Seite 35

Eigentlich war der Fall klar: In der Koalitionsvereinbarung von CDU/CSU und FDP vom Oktober 2009 heißt es, die Bundesregierung werde sich bei den Verhandlungen zum SWIFT-Abkommen „für ein hohes Datenschutzniveau (strikte Zweckbindung, Löschung der Daten, klare Regelungen bezüglich Weitergabe an Drittstaaten) und einen effektiven Rechtsschutz einsetzen“. Die Übermittlung der Daten werde „an Tatbestandsvoraussetzungen geknüpft und aufgrund einer Bedrohungs- und Gefährdungsanalyse eingegrenzt“. Das zugrunde liegende Abkommen müsse vom Bundestag ratifiziert werden. Danach hätte sich die Bundesregierung am letzten Tag vor Inkrafttreten des Lissabon-Vertrages am 1. Dezember 2009 beim SWIFT-Abkommen nicht der Stimme enthalten dürfen. Das hat sie aber, was im Ergebnis auf einen Verzicht auf ihr Veto-Recht und auf ein Inkrafttreten des Abkommens hinauslief. Damit wird deutscher und europäischer Datenschutz, also unser Grundrecht auf informationelle Selbstbestimmung, bei internationalen Finanztransaktionen im Hinblick auf US-Behördenanfragen weiterhin verletzt.

## Die Vorgeschichte

Wie kam es zu diesem Verfassungsverstoß? Im Jahr 2006 wurde bekannt, dass sich US-Sicherheitsbehörden nach den Terroranschlägen am 11. September 2001 Zugang zu sämtlichen internationalen Banktransaktionsdaten verschafften, indem sie den Monopolisten für derartige Transaktionen, den in Belgien beheimateten Dienstleister „Society for Worldwide Interbank Financial Telecommunication“ (SWIFT) zwangen, das Abschöpfen der Daten über einen in den USA befindlichen, sämtliche globale Transaktionsdaten enthaltenden Rechner zu dulden (vgl. Grundrechtreport 2007, S. 46 ff.). Die Empörung hierüber verbreitete sich von der Presse, über die europäischen Datenschutzbehörden, die Finanzinstitute und SWIFT bis zu den nationalen Parlamenten und dem Europaparlament. Europäische Unternehmen äußerten die nicht unbegründete Befürchtung, dass die abgezogenen Daten zum Zweck der Wirtschaftsspionage genutzt würden. Die Kritik führte schließlich zu einem begrenzten Eingeständnis durch die Europäische Kommission und die deutsche Bundesregierung, dass die Vorgehensweise problematisch ist. Der öffentliche Druck veranlasste zudem den Finanzdienstleister SWIFT, sein Spiegelrechenzentrum von den USA in die Schweiz zu verlegen und die US-Rechner nur noch für den lokalen und nicht mehr für den innereuropäischen Datenverkehr zu verwenden. Diese Änderung wurde für den Jahreswechsel 2009/2010 angekündigt und tatsächlich auch umgesetzt. So war schon frühzeitig erkennbar, dass den US-Behörden bisher verfügbare Daten entzogen würden.

Dies veranlasste die US-Regierung Kontakt mit dem Rat der Europäischen Union (EU) aufzunehmen, um den drohenden Datenverlust zu verhindern. Anstatt den Sieg des Datenschutzes zu feiern, ließen sich der EU-Kommission und -Rat mit ausdrücklicher Zustimmung der damaligen schwarz-roten deutschen Bundesregierung auf das Ansinnen der USA ein. Geplant wurde ein Abkommen, das den US-Behörden weiterhin die Bankdaten von völlig unverdächtigen Menschen und Unternehmen zur Verfügung stellt. Der Vertrag sollte vor Inkrafttreten des Lissabon-Vertrages geschlossen werden, um die nach diesem Vertrag bestehende Zuständigkeit des Europaparlaments zu vermeiden.

Im Vorfeld der Unterzeichnung des SWIFT-Abkommens kam es zu einem Konflikt zwischen den Koalitionspartnern der Bundesregierung. Nachdem aber sämtliche anderen EU-Staaten ihre Vorbehalte gegen das Abkommen zurückgestellt hatten, verzichtete auch Deutschland mit der Stimme des Innenministers auf ein Veto, so dass der Vertrag mit den USA am 1. Februar 2010 in Kraft treten konnte. Außer Deutschland enthielten sich Österreich, Ungarn und Griechenland. Das Europaparlament reklamierte schließlich, dass ohne dessen Zustimmung das Abkommen nicht umgesetzt werden dürfe.

## **Das neue SWIFT-Abkommen**

Zunächst die positive Botschaft: Das Abkommen soll nach 9 Monaten Ende Oktober 2010 und nach Ersetzung durch ein nach den neuen Lissabon-Regeln zustande gekommenes Vertragswerk ersetzt werden. Doch der Inhalt des Abkommens ist skandalös: Die EU-Staaten verpflichten sich, im Rahmen des „Terrorist Finance Tracking Programme“ (TFTP) des US-Finanzministeriums Banktransferdaten von in Europa ansässigen internationalen Finanzdienstleistern, also v.a. von SWIFT, auf Anfrage zu liefern. Die Formulierung des Vertrages führt dazu, dass nicht nur Transaktionen mit Drittländern, sondern auch innerhalb Europas erfasst sind. Hierunter können auch die des neuen innereuropäischen Überweisungssystems SEPA fallen, ebenso innereuropäische Bargeldauszahlungen und sogar innerdeutsche Eilüberweisungen. Voraussetzung ist, dass die spezifischen Recherchen an Transaktionsart, Raumbezug und vermuteten terroristischen Gefahren anknüpfen. Es genügt, dass diese Recherchen den Zwecken der Prävention, der Ermittlung, des Aufspürens oder der Verfolgung des Terrorismus oder der Terrorfinanzierung dienen können. Der Zugriff soll nicht mehr, wie bisher, direkt erfolgen, sondern auf Nachfrage und nach Prüfung durch die national zuständige Behörde, die sich aber auf die Feststellung der Vertragskonformität der Anfrage beschränkt. Sämtliche Maßnahmen werden „als Eilsache durchgeführt“. Übermittelt werden darf alles, was als Transaktionsdaten anfällt.

Die im Abkommen verabredeten Datenschutzvorkehrungen sind ungenügend: Es würde kein Data Mining betrieben, also kein Suchlauf mit offenen Fragestellungen. Der Datenumfang solle so eng wie möglich sein. Die Bestände würden sicher gespeichert und deren Nutzung auf den Zweck der Terrorismusbekämpfung beschränkt – was immer dies auch nach Ansicht der USA sei. Aus der Datenanalyse erlangte Hinweise sollen mit Verfolgungs- und Sicherheitsbehörden in den USA, Europa und dritten Staaten zum Zweck der Terrorismusbekämpfung ausgetauscht werden können. Die Grunddaten würden spätestens nach 5 Jahren gelöscht.

Als Gegenleistung - und dies ist ein vergiftetes Geschenk - bietet die USA Europa an, aus den Daten erlangte Hinweise mitzuteilen und selbst Daten aus den USA anzuliefern, sollte die EU vergleichbare Auswertungen vornehmen wollen. Entgegen der Ankündigung des Bundesinnenministers im Deutschen Bundestag ist in dem Abkommen in Europa kein gerichtlicher Rechtsschutz gewährleistet, weil Europa auf die Datennutzung in den USA keinen Einfluss nehmen darf und kann. Selbst ein nachschauendes Kontrollrecht wird der EU nicht eingeräumt. Nach 6 Monaten soll lediglich eine Evaluation erfolgen, an der auch zwei europäische Datenschützer teilnehmen, wobei nur die Konformität mit den Vertragsbestimmungen geprüft wird, in denen aber keine substantziellen Datenschutzgarantien enthalten sind.

Die Betroffenenrechte sind unzureichend geregelt: Betroffene können bei ihren in Europa liegenden nationalen Datenschutzbehörden nachfragen, ob ihre Rechte nach dem Abkommen beachtet wurden. Nur: das Abkommen gewährt gerade keine Datenschutzrechte, und die europäischen Datenschutzbehörden dürfen in den USA die Nutzung der Daten nicht überprüfen. Eine unabhängige Kontrolle in den USA gibt es nicht.

# Was bleibt

Die EU über deren Rat durften ohne parlamentarische Beteiligung zu einem derartigen Eingriff in die Grundrechte der Betroffenen überhaupt nicht verpflichtet. Unstreitig ist, dass die in Deutschland wie in der EU geltenden Standards für effektiven Grundrechtsschutz unterlaufen werden. Angesichts der Verteidigung des Abkommens durch das Bundesinnenministerium, wonach „Verbesserungen“ durchgesetzt worden seien und die Lösungsfrist der verdachtslos übermittelten Daten erst nach 5 Jahren „nicht völlig abwegig“ sei, ist zu befürchten, dass keine wesentlichen Verbesserungen im Fall eines langfristigen Abkommens zu erreichen sind.

Unklar bleibt, was mit den Daten in den USA in der Vergangenheit passiert ist und passieren wird. Unklar ist auch, was der millionenfache Datenabgleich gebracht hat. Angeblich wurden bisher 1.450 Hinweise aus dem TFTP-Programm an Sicherheitsbehörden in der EU gegeben und 800 an Behörden anderer Staaten. Was tatsächlich an sicherheitsrelevanten Erkenntnissen herausgekommen ist, wurde weder überzeugend noch überprüfbar dargelegt. Das deutsche Bundeskriminalamt jedenfalls meint, die Datenauswertung bringe nichts. Statt darauf zu dringen, dass Nicht-EU-Staaten hohe Datenschutzstandards einführen, werden ohne Not die europäischen Standards auf dem Altar der Sicherheitspolitik geopfert - zum Schaden der Menschen in der EU. Europäische Sicherheitsbehörden scharren schon mit den Füßen, selbst von Grundrechtsbindungen befreit ermitteln zu können.

So wurde am Tag vor dem Inkrafttreten des Grundrechtes auf Datenschutz in der Grundrechtecharta - einem Bestandteil des Lissabonvertrags - dieses Grundrecht diskreditiert - kein guter Start für die EU-Grundrechte!

---

<https://www.humanistische-union.de/publikationen/grundrechte-report/2010/publikation/swift-europa-befreit-banktransaktionsdaten-vom-grundrecht-auf-datenschutz/>

Abgerufen am: 05.12.2021