

**Veröffentlicht in TELOS, Revista de Pensamiento sobre Comunicación,  
Tecnología y Sociedad  
Februar-Mai 2014**

---

## **Wiederherstellung des Vertrauens in die transatlantischen Beziehungen\***

*Peter Hustinx\*\**

*Europäische Datenschutzbeauftragte (EDSB)*

Die jüngsten Enthüllungen über die massenhafte Überwachung im Internet durch die Geheimdienste der USA und anderer Staaten hat eine Schockwelle rund um den Globus ausgelöst, aber auch ein ernsthaftes, vielschichtiges Problem zwischen der EU und den USA offengelegt. Es wurde nicht nur bekannt, dass Bürger ohne Unterschied bei ihrer täglichen Arbeit exzessiv, großflächig und strukturell überwacht wurden, sondern auch, dass diese massenhafte Überwachung eine Infrastruktur kostenloser Dienste nutzt, die insbesondere von US-amerikanischen Unternehmen beherrscht werden. Bei der Nutzung dieser Dienste werden die personenbezogenen Daten der Bürger kontinuierlich überwacht und erzielen durch Werbung im Internet riesige Gewinne. Diese Infrastruktur entstand schrittweise über die letzten zehn Jahre, offensichtlich nicht ohne Zutun der Bürger, doch ohne ein wirkliches öffentliches Bewusstsein für die Folgen, die nun offen zutage treten. Vor allem aber lässt sich ein besorgniserregendes Ungleichgewicht in Bezug auf den bestehenden Rechtsrahmen auf beiden Seiten des Atlantiks feststellen.

Die Europäische Kommission hat vor kurzem einen Aktionsplan zur Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA vorgestellt.<sup>1</sup> In diesem Aktionsplan wird auch die Regierung der USA

---

\* Veröffentlicht in TELOS, Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad, nr. 97, Februar-Mai 2014, S. 80-82.

\*\* Peter Hustinx ist der Europäische Datenschutzbeauftragte (EDSB). E-Mail: [edps@edps.europa.eu](mailto:edps@edps.europa.eu); Website: [www.edps.europa.eu](http://www.edps.europa.eu).

<sup>1</sup> Mitteilung der Kommission an das Europäische Parlament und den Rat vom 27. November 2013, *Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA*, KOM(2013) 846 endgültig.

aufgerufen, ihren Teil beizutragen, das Vertrauen wiederherzustellen und die entstandene Kluft zu überbrücken. Dabei darf jedoch nicht übersehen werden, dass die aufgetretenen Probleme tief in der Geschichte und der Rechtskultur der Länder verwurzelt sind und es ein langer Prozess sein wird, diese zu beheben. Auf jeden Fall sollte das Problem der „exzessiven Bespitzelung“ getrennt von den anderen, stärker strukturell bedingten Problemen behandelt werden, wobei die Zusammenhänge jedoch nicht außer Acht gelassen werden dürfen.

Es lassen sich aber auch einige Gemeinsamkeiten zwischen der EU und den USA feststellen. Erste Überlegungen zum Schutz personenbezogener Daten kamen sowohl in der EU als auch den USA in den frühen 1970er Jahren auf. Die vom Europarat im Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 festgehaltenen Grundsätze beruhen in der Tat auf den US-amerikanischen Fair Information Practice Principles<sup>2</sup>, an denen sich auch die OECD-Richtlinien über Datenschutz von 1980 orientieren. Im weiteren Verlauf gingen die Entwicklungen diesseits und jenseits des Atlantiks allerdings auseinander: Abgesehen von einigen Einzelgesetzen beruht das US-amerikanische System auf dem Grundsatz der Selbstregulierung, während sich in der EU die Bemühungen um einen gesetzlichen Rahmen in der Umsetzung der Richtlinie 95/46/EG in nationales Recht niederschlugen. Dies führte schließlich zur Anerkennung des Rechts auf den Schutz personenbezogener Daten als eigenständiges Grundrecht in Artikel 8 der Charta der Grundrechte der Europäischen Union, die mit dem Inkrafttreten des Vertrags von Lissabon Ende 2009 rechtsverbindlich wurde.

Dieser Unterschied in der rechtlichen Infrastruktur geht letztlich auf einen bedeutenden Unterschied auf Ebene der Verfassung zurück. So hat der 4. Zusatzartikel zur Verfassung der Vereinigten Staaten von Amerika<sup>3</sup>, der willkürliche Durchsuchung, Verhaftung und Beschlagnahme verbietet, einen wesentlich begrenzteren Geltungsbereich als das Recht auf Schutz des Privatlebens,

---

<sup>2</sup> US Department of Health, Education and Welfare, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers and the Rights of Citizens*, Washington D. C. 1973.

<sup>3</sup> Wortlaut des 4. Zusatzartikels zur Verfassung der Vereinigten Staaten von Amerika: *„The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.“* (Übersetzung der amerikanischen Botschaft: *„Das Recht des Volkes auf Sicherheit der Person und der Wohnung, der Urkunden und des Eigentums, vor willkürlicher Durchsuchung, Verhaftung und Beschlagnahme darf nicht verletzt werden, und Haussuchungs- und Haftbefehle dürfen nur bei Vorliegen eines eidlich oder eidesstattlich erhärteten Rechtsgrundes ausgestellt werden und müssen die zu durchsuchende Örtlichkeit und die in Gewahrsam zu nehmenden Personen oder Gegenstände genau bezeichnen.“*)

das in Artikel 7 der Charta der Grundrechte der Europäischen Union verankert ist.<sup>4</sup> In der Tat bezieht sich der 4. Zusatzartikel nur auf *Inhalte*, nicht auf andere Kommunikationsdaten (wie den Anrufer, die Zeit und den Standort), und schützt zudem im Prinzip nur US-Bürger. Außerdem genießen Informationen, die einem Dienstleister übermittelt wurden, nicht mehr diesen Schutz, während der Ausgangspunkt des EU-Rechts die Vertraulichkeit der Kommunikation ist.

Im Laufe der Jahre wurden kreative Lösungen zur Überbrückung der Kluft zwischen dem EU-Recht und der US-amerikanischen Selbstregulierung entwickelt. Ein gutes Beispiel hierfür ist die Safe-Harbor-Entscheidung<sup>5</sup>, die die Übermittlung von Daten aus der EU in die USA gestattet, wenn die Organisationen die Grundsätze des „sicheren Hafens“ zum Datenschutz (Safe Harbor Privacy Principles) beachten und der Zuständigkeit der US Federal Trade Commission (FTC) gemäß dem US Fair Trade Act unterliegen. Obwohl inzwischen mehr als 3 000 Unternehmen dem Abkommen beigetreten sind, bleiben einige zentrale Probleme ungelöst. Die Europäische Kommission<sup>6</sup> hat 13 Ansatzpunkte für Verbesserungen ermittelt und eine eingehende Überprüfung angekündigt, die bis Sommer 2014 abgeschlossen sein soll.

Unterdessen hat die EU viel Energie in die eingehende Überprüfung des bestehenden Rechtsrahmens für den Datenschutz investiert, um diesen im Hinblick auf die Herausforderungen neuer Technologien und der Globalisierung sicherer und wirksamer zu gestalten.<sup>7</sup> Vorgesehen ist eine Stärkung der Rechte der betroffenen Personen, größere Verantwortungen der für die Datenverarbeitung Verantwortlichen sowie eine konsequentere Überwachung und Durchsetzung durch unabhängige Stellen. Der Vorschlag für eine Datenschutz-Grundverordnung<sup>8</sup> – die in allen Mitgliedstaaten direkt anwendbar ist – wird für eine größere Konsistenz der rechtlichen Regelungen und Verfahren in der Europäischen Union sorgen. Ein starker Rahmen mit klaren Regeln, die auch dann durchsetzbar sind, wenn Daten in Drittländer übermittelt werden, ist heute mehr denn je eine Notwendigkeit.

Ein wichtiger Aspekt dieses Vorschlags ist, dass er für alle Unternehmen gelten soll, die auf dem europäischen Markt tätig sind, unabhängig davon, wo sie ihren Sitz

---

<sup>4</sup> Artikel 7 der Charta der Grundrechte der Europäischen Union: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.“

<sup>5</sup> Entscheidung der Kommission 2000/520/EG vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, S. 7.

<sup>6</sup> Siehe die in Fußnote 1 zitierte Mitteilung.

<sup>7</sup> Siehe das von der Europäischen Kommission im Januar 2012 vorgestellte Datenschutz-Reformpaket.

<sup>8</sup> Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig.

haben. Der neue Rahmen wird folglich auch für Unternehmen gelten, die in den USA oder anderen Drittländern niedergelassen sind und dort keinen vergleichbaren Vorschriften unterliegen. Davon werden vermutlich auch einige bekannte Diensteanbieter im Internet betroffen sein, die bei der Erbringung von Dienstleistungen für Verbraucher aus der EU möglicherweise einer massenhaften Überwachung unterlagen. Mit den neuen Vorschriften soll ein Instrument gegen die unlauteren Praktiken von Unternehmen geschaffen werden, die ihre Kunden derzeit systematisch überwachen und das Verbraucherverhalten ausnutzen. Allein die Größe des europäischen Marktes trägt dazu bei, dass der neue Rahmen zu einer realistischen Option wird.

Im Rahmen der neuen Vorschriften könnte auch ein Mechanismus<sup>9</sup> zur Lösung von Konflikten bei kollidierenden (inter)nationalen Rechtsnormen entwickelt werden, wenn verschiedene Staaten ihre öffentlichen Interessen unterschiedlich auslegen. Dieser Mechanismus sollte auf dem Grundsatz basieren, dass jeder Datenaustausch dem EU-Recht entsprechen muss, sofern nicht in einer bindenden internationalen Vereinbarung etwas anderes festgelegt wurde oder eine Justiz- oder Aufsichtsbehörde eine Sondergenehmigung erteilt hat. Ein solcher Mechanismus könnte sich in verschiedenen Bereichen als nützlich erweisen, nicht zuletzt in solchen, die zurzeit möglicherweise einer massenhaften Überwachung unterliegen.

In diesem Zusammenhang ist von Bedeutung, dass in dem kürzlich von der Europäischen Kommission vorgestellten Aktionsplan auch Maßnahmen in Bezug auf internationale Übereinkommen mit den USA vorgesehen sind.<sup>10</sup> Abgesehen von der bereits erwähnten Safe-Harbor-Regelung ist die Europäische Kommission bestrebt, die Datenschutzgarantien im Bereich der Strafverfolgung zu stärken. In diesem Rahmen soll ein Abkommen über die Datenübermittlung im Zusammenhang mit der polizeilichen und justiziellen Zusammenarbeit geschlossen werden, das ein hohes Schutzniveau für die Bürger auf beiden Seiten des Atlantiks gewährleistet. Dazu gehört auch, dass EU-Bürger, die nicht in den USA ansässig sind, Zugang zu Rechtsmittelverfahren erhalten sollen. Die Datenübermittlung zu Zwecken der Strafverfolgung soll über die offiziellen Kanäle erfolgen. Direkte Auskunftersuchen bei EU-Unternehmen sollen nur in klar festgelegten und gerichtlich überprüfbaren Ausnahmefällen gestattet sein.

Die Europäische Kommission verlangte außerdem nachdrücklich, dass europäische Belange im laufenden US-Reformprozess berücksichtigt werden. Sie nahm dabei

---

<sup>9</sup> Siehe Änderungsanträge des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (LIBE) vom 21. Oktober 2013.

<sup>10</sup> Siehe die in Fußnote 1 zitierte Mitteilung.

Bezug auf die von Präsident Obama angekündigte Überprüfung der Tätigkeiten der nationalen Sicherheitsbehörden der USA auch mit Blick auf den geltenden Rechtsrahmen. Zu den wichtigsten Neuerungen, die die Europäische Kommission dabei anstrebt, gehört die Ausweitung der für US-Bürger und Gebietsansässige geltenden Garantien auf nicht in den USA ansässige EU-Bürger, mehr Transparenz bei den Tätigkeiten der Nachrichtendienste und eine Stärkung der Aufsicht. Die Notwendigkeit und Angemessenheit der derzeitigen Überwachungsprogramme soll ebenfalls gründlich geprüft werden.

Die Europäische Kommission wies zudem auf die steigende Bedeutung internationaler Datenschutznormen, insbesondere im Internet, hin. In diesem Zusammenhang führte sie einige Initiativen aus der jüngeren Vergangenheit an, wie den Entwurf einer Resolution zum Schutz der Privatsphäre online und offline, den Deutschland und Brasilien der UN-Generalversammlung vorgelegt haben und der sich auf Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte von 1966 stützt.

Hinsichtlich des Datenaustauschs über den Atlantik und darüber hinaus wäre eine Stärkung des nationalen Rechtsrahmens in den USA einschließlich der Annahme des von Präsident Obama im Februar 2012 als Teil einer umfassenden Strategie für einen verbesserten Schutz der Privatsphäre von Verbrauchern angekündigten Rechtenkatalogs für den Verbraucherdatenschutz (Consumer Privacy Bill of Rights) mit eindeutigen Vorteilen verbunden.<sup>11</sup> Das Bestehen eines Katalogs strenger und durchsetzbarer Datenschutzvorschriften, die in der EU und in den USA verankert sind, würde eine solide Grundlage für den grenzüberschreitenden Datenverkehr bilden.

Schließlich sollte nicht vergessen werden, dass auch EU-Mitgliedstaaten bei der massenhaften Überwachung vermutlich eine wichtige Rolle gespielt haben oder noch spielen. Die Tatsache, dass die nationale Sicherheit in die ausschließliche Zuständigkeit<sup>12</sup> der einzelnen Mitgliedstaaten fällt, ist kein Grund, nicht so frühzeitig wie möglich und auf der richtigen Ebene die richtigen Fragen zu stellen und geeignete Maßnahmen zu ergreifen.

---

<sup>11</sup> Siehe „*Consumer Data Privacy in a Networked World: a framework for protecting privacy and promoting innovation in the global digital economy*“, Februar 2012, Washington D. C.

<sup>12</sup> Siehe Artikel 4 Absatz 2 des Vertrags über die Europäische Union (EUV).