

„Zeitenwende“ im Datenschutz?

Über Grundrechtsschutz und mehr digitale Souveränität

| ALEXANDER ROSSNAGEL | Joybrato Mukherjee, der Präsident der Justus-Liebig-Universität in Gießen, forderte in Forschung & Lehre 10/22 (S. 761) dazu auf, auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA zu verzichten. In der „Zeitenwende“, die durch den Krieg Putins in Europa ausgelöst wurde, sei es nicht mehr zeitgemäß, den USA zu misstrauen. Er forderte auf, offen darüber zu sprechen. Eine Replik.

Ein Rechtsstaat zeichnet sich dadurch aus, dass er auch und gerade in Zeiten der Krise rechtsstaatliche Errungenschaften schützt. Datenschutz ist Freiheitsschutz. Datenschutz ist ein Grundrecht – geschützt durch die Europäische Grundrechtecharta und das Grundgesetz. Datenschutz schützt auch andere Grundrechte wie – insbesondere mit Blick auf US-amerikanische Nachrichtendienste – die Meinungsfreiheit oder die Reisefreiheit. Dieser Schutz der Grundrechte kann in einem Rechtsstaat nicht beliebig – abhängig von aktuellen politischen Entwicklungen – relativiert werden.

Ausgangspunkt für die gegenwärtige Diskussion über die Zeitgemäßheit des Datenschutzes muss das Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 („Schrems II“) sein. In diesem hat der EuGH die Anerkennung der US-Regelungen zur Übermittlung

personenbezogener Daten aus der EU in die USA („Privacy Shield“) durch die Europäische Kommission für rechtswidrig und ungültig erklärt. Ausschlaggebend waren zwei Gründe: Zum einen ist die Datenerhebung und -auswertung durch die US-Nachrichtendienste – ins-

»Es ist sehr kurzsichtig, allein die gegenwärtige Haltung des demokratischen US-Präsidenten gegenüber Europa zu berücksichtigen.«

besondere die Massenverarbeitung im Internet – unverhältnismäßig. Zum anderen kann niemand aus der EU gegen die unzulässige Verarbeitung seiner Daten in den USA klagen. Daher verursacht jeder, der personenbezogene Daten in die USA übermittelt, dass die jeweils betroffene Person ihre Grundrechte auf Datenschutz und Rechtsschutz nicht mehr wahrnehmen kann. Um diesen Grundrechtsverlust zu verhindern, hat der EuGH die Datenschutzaufsichtsbehörden verpflichtet, solche Übertragungen zu unterbinden.

Freiheit und Demokratie

Putins Krieg ist kein Grund, auf Grundrechte zu verzichten. Europa und Deutschland sind in der Unterstützung der Ukraine und der Verteidigung der westlichen Welt zwar näher mit den USA zusammengedrückt. Aber – um was geht es denn in diesem Kampf? Verteidigt werden Freiheit und Demokratie. Daher ist es unverständlich, wie-

so wir dafür auf Freiheit, auf den Schutz von Grundrechten verzichten sollten – auch wenn diese Grundrechte nicht von Putin, sondern von US-amerikanischen Nachrichtendiensten verletzt werden. Auch unter befreundeten Staaten sind anlasslose Massenüberwachungen der Bürgerinnen und Bürger eines anderen Staates nicht akzeptabel.

Hinzu kommt noch ein historisches Argument gegen den Verzicht auf eine kritische Haltung gegenüber der Praxis US-amerikanischer Nachrichtendienste: Es ist sehr kurzsichtig, allein die gegen-

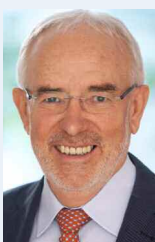
wärtige Haltung des demokratischen US-Präsidenten gegenüber Europa zu berücksichtigen. Bis vor zwei Jahren hat ein republikanischer Präsident eine

America-First-Politik mit geopolitischem Isolationismus betrieben. In zwei Jahren kann im Weißen Haus wieder ein republikanischer Präsident regieren, der die gleiche Politik verfolgt. Dann haben wir wieder eine „Zeitenwende“.

EuGH und Videokonferenzsysteme

Das Urteil des EuGH gilt z.B. auch für Videokonferenzsysteme. Wer solche Systeme einsetzt, die personenbezogene Daten den US-Nachrichtendiensten zugänglich machen, verletzt seine Fürsorge- und Schutzpflicht für die Grundrechte seiner Studierenden und Lehrenden. Dabei geht es nicht darum, Videokonferenzsysteme aus den USA zu verhindern, sondern Grundrechte zu schützen. Daher können auch US-amerikanische Systeme genutzt werden, wenn dabei die Übertragung personenbezogener Daten in die USA verhindert wird. Eine solche Nutzung hat die hessische Aufsichtsbehörde unter ausrei-

AUTOR



Alexander Roßnagel ist der Hessische Beauftragte für Datenschutz und Informationsfreiheit und Seniorprofessor für Öffentliches Recht mit dem Schwerpunkt Recht mit dem Umweltschutz an der Universität Kassel.

chenden Schutzmaßnahmen z.B. für „Zoom“ anerkannt. Bei der datenschutzrechtlichen Bewertung von Videokonferenzsystemen wird somit keine amerikafeindliche protektionistische Politik umgesetzt. Auch verhindert sie nicht die Arbeitsfähigkeit der Hochschulen und die Erfüllung ihres Lehrauftrags. Auf beides hat die Aufsichtsbehörde jetzt über zwei Jahre Rücksicht genommen. Sie hat während dieser Zeit immer wieder darauf hingewiesen, dass die Hochschulen nicht auf Videokonferenzsysteme angewiesen sind, die personenbezogene Daten in die USA übertragen. Vielmehr können sie auch leistungsfähige Systeme einsetzen, die die Daten nur in der EU verarbeiten.

Dies führt zu einem zweiten Argument, das in dieser Diskussion beachtet werden muss: Wenn wir aus der „Zeitenwende“ etwas gelernt haben, dann ist es die Erkenntnis, dass wir technische und wirtschaftliche Abhängigkeiten soweit wie möglich vermeiden müssen. Dies gilt nicht nur für die Energieab-

hängigkeit, sondern in der digitalen Transformation mindestens ebenso für die Abhängigkeit von fremder Informationstechnik. Daher verfolgen die Europäische Kommission, die Bundesregierung und alle Landesregierungen das Ziel digitaler Souveränität. Um diese als Voraussetzung und Folge digitaler Selbstbehauptung zu verbessern, sind koordinierte Anstrengungen in vielen Politikbereichen wie der Wirtschafts- und Industrie-, Wettbewerbs-, Forschungs-, Bildungs-, Rechts- und Digitalpolitik erforderlich. Die Zielsetzung digitaler Souveränität kann auch in einem rechtsstaatlichen Sinn verstanden werden: Es geht um den Einsatz von Informationstechnik, die es den Verantwortlichen ermöglicht, ihre rechtlichen Verpflichtungen – auch im Datenschutz – zu erfüllen.

Mehr digitale Souveränität anstreben

Auch wenn eine vollständige digitale Souveränität nicht zu erreichen sein

wird, sind Anstrengungen notwendig, die bestehenden Abhängigkeiten im Rahmen des Möglichen abzubauen. Dies soll vor allem durch Stärkung der eigenen IT-Wirtschaft und durch den Einsatz von Open Source-Systemen erreicht werden. Viele Maßnahmen, die sich an dem Ziel digitaler Souveränität orientieren, sind inzwischen auf den Weg gebracht – wie etwa auf Bundesebene die Souveräne Verwaltungscloud, der Souveräne Arbeitsplatz, der Sovereign Tech Fund und das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS). Auf Länderebene werden z.B. in Hessen die Schulen künftig ihre Videokonferenzen mit dem Open Source-System „BigBlueButton“, betrieben von German Edge Cloud, durchführen und die Landesverwaltung wird ihre Videokonferenzen mit dem Open Source-System „Jitsi“, betrieben durch T-Systems, abhalten. Die Hochschulen, gerade in Hessen, sollten nicht die letzten sein, die diesen Weg zu mehr digitaler Souveränität beschreiten.

Anzeige

„Das Studium in Osnabrück ermöglichte mir neue Blickwinkel auf das Management von Hochschulen und Wissenschaft.“

Michael G.



HOCHSCHULE OSNABRÜCK
UNIVERSITY OF APPLIED SCIENCES

ZERTIFIKATSPROGRAMM – CAS

Certificate of Advanced Studies

PERSONALMANAGEMENT IN HOCHSCHULEN UND WISSENSCHAFT

Berufsbegleitende Weiterbildung im Umfang von **15 ECTS**

Individuell & flexibel – **Zertifikatsstudium Hochschul- und Wissenschaftsmanagement** an der Hochschule Osnabrück

- Human Resource Management
- Diversity Management
- Personalentwicklung und Karriere im Wissenschaftssystem

Wir bieten ein kompaktes Studienkonzept ausgerichtet auf Berufstätige, Kontaktphasen in Blöcken an Wochenenden und integrierten Online-Phasen mit individueller Betreuung und Beratung.



Neugierig geworden? Informieren Sie sich auf www.hs-osnabrueck.de/cas-wissenschaftsmanagement