Hände weg vom Datengold

Die Europäische Union muss persönliche Daten effektiv schützen

AXEL VOSS

Geboren 1963 in Hameln, Mitglied der EVP-Fraktion und Mitglied des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres im Europäischen Parlament.

Bald zwanzig Jahre, fast zwei Dekaden ist sie alt, die europäische Datenschutzrichtlinie. Für die Entwicklung moderner Technologien wie der des Internets ist das eine Ewigkeit. Im „Geburtsjahr" der Richtlinie 95/46/EG, 1995, gab es kein WhatsApp, keine sozialen Netzwerke, Smartphones, Googlemaps und Wikipedia. Es war die Ära der Telefone und des Videotextes. Informationen wurden gefaxt, kopiert und in Bibliotheken nachgeschlagen. Das Internet zog zwar schon per lärmendem Modem in den Alltag ein, doch von der heutigen dauerhaften Erreichbarkeit jeder Person und jeglicher Information überall war noch wenig zu spüren. Für die unter Zwanzigjährigen sind das Erzählungen aus einer anderen Zeitrechnung.

Die gesamte Kommunikation hat eine Revolution durchlaufen, im privaten Bereich ebenso wie in Unternehmen und in der öffentlichen Verwaltung. Daten sind durch die Omnipräsenz und Dauernutzung digitaler Dienste zum „Gold des 21. Jahrhunderts“ geworden. Je mehr Menschen von sich preisgeben, desto mehr wird der Einzelne durch seine Daten zu einem attraktiven Faktor im Wirtschaftskreislauf – der Absatzmarkt für das Produkt „personenbezogene Daten“ floriert.

DOMINANTE AMERIKANER

Für den Datenschutz ergeben sich in der Europapolitik aus diesen Entwicklungen heute drei grundsätzliche Probleme.

Erstens hinken die Gesetze der Realität hinterher – wie das Eingangsbeispiel der Datenschutzrichtlinie zeigt. Oft mangelt es jedoch weniger an den Gesetzen als an deren konsequenter und effektiver Durchsetzung: So kann ein europäischer Datenschutz nicht greifen, wenn beispielsweise E-Mails von Würzburg nach Mailand durch die USA geleitet werden. Territorial begrenzte Gesetze treffen auf grenzenlose, globalisierte Problemlagen.

Zweitens gibt es eine zunehmende Aushöhlung unserer Privatsphäre sowohl auf nachrichtendienstlicher als auch auf kommerzieller Ebene. Einerseits schockten die Enthüllungen des Ex-NSA-Mitarbeiters Edward Snowden die Öffentlichkeit, als er die massenhafte Ausspähung von Bürgern durch amerikanische und britische Geheimdienste publik machte. Andererseits sind es aber digitale Dienste kommerzieller Anbieter, die das Konsumverhalten „vernetzter“ Bürger ausspionieren und ihnen Daten entlocken. Vielen ist immer noch nicht bewusst, wie viel Information sie tagtäglich – etwa durch den intelligenten Fernseher mit Internetanschluss oder die ferngesteuerte Heizung – von sich preisgeben. Die Befürchtung, dass heute tatsächlich nichts mehr privat ist, scheint vor diesem Hintergrund mehr als begründet.

Drittens agieren als Treiber und Gestalter dieser gesamten Entwicklung nicht die Europäische Union (EU) oder ihre Mitgliedsstaaten. Es sind die USA und die US-Unternehmen wie Google, Apple oder Facebook, die den Takt für Europa bestimmen. Obwohl sie einen riesigen Markt mit 450 Millionen Bürgern darstellt, ist es der EU nicht gelungen, eine dominante Rolle auf dem Gebiet der digitalen Kommunikation einzunehmen. Stattdessen richtet sie sich nach den amerikanischen Angeboten aus. Es wird für Europa Zeit, dies zu ändern.

„DATENVERKEHRSREGELUNG“

Der weltweite Datenverkehr benötigt, dem Straßenverkehr vergleichbar, eine globale „Datenverkehrsregelung“. Da diese jedoch auf absehbare Zeit nicht erreichbar sein wird, wird zunächst an europäischen Lösungen gearbeitet. Der Schutz personenbezogener Daten ist ein Grundrecht der Bürger Europas. Besonderes Augenmerk muss deshalb der Wahrung der Sicherheit des Bürgers und der Privatsphäre des Einzelnen, also der Durchsetzung dieses Rechts, gelten. Das heißt, dass überall dort, wo Daten europäischer Bürger verarbeitet werden, auch europäisches Recht gelten muss. Dennoch gilt: Kein Datenschutzrecht kann den Einzelnen von seiner eigenen Verantwortung freisprechen. Die verstärkte Aufklärung im Umgang mit Daten, insbesondere an Schulen, muss deswegen ein wichtiges Ziel der europäischen Datenschutzpolitik sein.

Die Novellierung der bestehenden Datenschutzrichtlinie ist ein erster und entscheidender Schritt für den Schutz der Persönlichkeitsrechte im wachsenden digitalen Markt. Zugleich muss das neue Recht der digitalen Wirtschaft die dringend benötigten Innovationen und Wachstum ermöglichen. Das ist eine schwierige Balance. Mit der neuen „Datenschutzgrundverordnung“ konnte nach langen und zähen Verhandlungen im Europäischen Parlament eine gemeinsame Position gefunden werden. Es hängt nun vom Ministerrat ab, dieses starke Signal für einen besseren Datenschutz in Europa im Parlament als Gesetz zu verabschieden.

Das Ziel ist eine vollständige Harmonisierung des Datenschutzrechts in Europa, damit sich die Bürger in allen EU-Staaten auf ein einheitliches hohes Datenschutzniveau verlassen können und die Unternehmen gleiche Wettbewerbsbedingungen vorfinden. Das deutsche Datenschutzniveau darf dabei selbstredend nicht verwässert werden.

Klare und übersichtliche Informationen sind ein zentrales Element dieser Bestrebung: Jeder muss erfahren können, wer seine Daten wann und wofür verarbeitet und auf welcher Rechtsgrundlage dies geschieht. Jeder muss das Recht haben, seine Daten zu löschen und zu berichtigen. Daten von Kindern und Jugendlichen bedürfen eines besonderen Schutzes und sollten nur mit der Einwilligung der Erziehungsberechtigten verarbeitet werden dürfen. Wichtig sind angemessene und effektive Sanktionen für die, die dieses Recht ignorieren – unabhängig davon, von welchem Staat aus sie sich an die europäischen Bürger wenden.

Während die Verhandlungen zur neuen Datenschutzgrundverordnung auf Hochtouren liefen, stellten die Snowden-Enthüllungen über die tägliche Praxis der US-amerikanischen und britischen Geheim-

dienste sowie über das mögliche Abgreifen privater Kommunikationsdaten die Datenschutzpolitik vor vollkommen neue Fragen. Das Europäische Parlament hat noch im Sommer 2013 einen Untersuchungsausschuss eingerichtet, lange bevor nationale Parlamente darüber entschieden.

Seither hat der „NSA-Untersuchungsausschuss" in über fünfzehn Sitzungen getagt und Experten aus EU-Institutionen, US-Vertreter, Vertreter der nationalen Parlamente, Journalisten, Sicherheits-, Computer- und IT-Experten, Whistleblower sowie Experten aus der Zivilgesellschaft angehört und die beunruhigenden Erkenntnisse in einem Bericht zusammengefasst.

DER NÄCHSTE GOOGLE-KONZERN SOLL AUS EUROPA KOMMEN

Da Geheimdienste per se nicht viel über ihre Aktivitäten aussagen, muss davon ausgegangen werden, dass die NSA-Untersuchungsarbeit keine vollkommene Aufklärung der Tätigkeiten der NSA leisten kann. So lehnte zum Beispiel Keith B. Alexander, ehemaliger General der US-Armee und bis Januar 2014 Direktor der NSA, die Einladung des Europäischen Parlaments zu einer Aussage ab. Die Tatsache allerdings, dass die NSA die im Raum stehenden Gerüchte über Aktivitäten nicht widerlegt hat, läßt vermuten, dass tatsächlich alle Daten permanent im Internet abgefangen und gespeichert werden. Es wäre aber durchaus naiv, zu glauben, dass die NSA ein Einzelfall ist und andere Geheimdienste keine personenbezogenen Daten kumulieren. Es ist davon auszugehen, dass auch andere Nachrichtendienste EU-Bürger, Wirtschaftskonzerne sowie staatliche Strukturen datenbasiert intensiv ausspähen.

Was also können wir tun? Um einer hundertprozentigen IT-Sicherheit näherzukommen, müssten die EU und die Mitgliedsstaaten ihre eigenen Anstrengungen enorm verstärken. Die Bereiche E-Mail und Telekommunikation müssen sicherer und besser verschlüsselt werden. Zentral ist die Forderung nach einer EU- beziehungsweise einer Schengen-Cloud. Diese könnte als Schutzschild gegen externe Gefahren dienen und somit einen vertrauenswürdigen Datenspeicher bilden – insbesondere dann, wenn auch die Server in Europa aufgestellt würden.

Ähnlich verhält es sich mit dem EU-Routing sowie der Gesprächsdatenerfassung und -verarbeitung innerhalb der EU oder auch mit europäischen Suchmaschinen. Die Daten müssten nicht wie bislang EU-Territorium und somit den Unions-Rechtsraum verlassen. Dies wären veritable Schritte in Richtung IT-Unabhängigkeit, ohne Protektionismus zu betreiben. Die vorhandenen IT-Strukturen können besser ausgebaut,

sicherer gemacht und Datenströme besser kontrolliert werden. Dazu ist eine Europäische IT-Offensive notwendig: Der nächste Google-Konzern soll aus Europa kommen!

Mit einer einheitlichen Datenschutzgrundverordnung könnte der europäische Markt den USA auf der Basis eines starken Gesetzes gegenübertreten. Die USA haben ein massives Interesse an dem Absatzmarkt der Europäischen Union und an den EU-Bürgern als Nutzer der von ihren Unternehmen angebotenen digitalen Dienste. Diesen Hebel kann sich das europäische Vorgehen zunutze machen.

Der Datenaustausch zwischen den USA und der EU wird rechtlich derzeit über das „Safe Harbor-Abkommen" abgewickelt. Dieser „Sichere Hafen" soll garantieren, dass Unternehmen privaten Daten in den USA ein zum europäischen Schutz äquivalentes Datenschutzniveau bieten. Der NSA-Skandal hat allerdings die Illusion über die Umsetzbarkeit einer solchen Praxis endgültig platzen lassen.

EINE ZUKUNFT FÜR DIE PRIVATSPHÄRE

Die EU sollte deshalb von ihrer Option zur Aussetzung des „Safe Harbor-Abkommens", das in den USA die Geschäfte mit den persönlichen Daten der EU-Bürger vereinfacht, Gebrauch machen, auch wenn die Amerikaner genau dieses fürchten. Auf der Grundlage der EU-Datenschutzverordnung könnte dann selbstbewusst neu verhandelt werden.

Das wäre ein klares Signal an die USA und an die großen datensammelnden Unternehmen – nämlich, dass die massenhafte Ausspähung europäischer Bürger sowohl kommerzielle als auch sicherheits- oder strafrechtsrelevante Grenzen hat und dass gemeinsame Standards in dieser Frage unumgänglich sind. Solange sich aber unsere amerikanischen Partner an diesem Punkt verweigern, müssen die Europäer einen eigenen Weg gehen. Obwohl eine Aussetzung des „Safe Harbor-Mechanismus" ernsthafte Konsequenzen für die Unternehmen zur Folge haben kann, ist Europa bereit, diesen Weg einzuschlagen, damit der Schutz der Privatsphäre noch eine Zukunft hat.