



Arbeitsgruppe Europäische Integration*

Bürgerrechte, Sicherheit und Verbraucherschutz in der EU

Grundrecht Datenschutz als Basis für eine europäische Innenpolitik

- Die kriminelle Nutzung des Internets nimmt zu. Der Staat muss daher die notwendigen Instrumente zum Austausch von Daten und die Überwachung von Kommunikation erhalten. Auf Ebene der EU ist ein verstärkter Datenaustausch aufgrund des Schengenraums erforderlich.
- Die Legitimität europäischer wie auch nationaler Maßnahmen ist allerdings immer nur dann sichergestellt, wenn die erweiterte Verfügbarkeit persönlicher Daten in einem angemessenen Verhältnis zur Freiheit der Persönlichkeit, dem Schutz der Privatsphäre und der informationellen Selbstbestimmung steht. Hierzu sind strikte Bedingungen zu stellen.
- In der EU wird der Datenschutz mit dem Lissabonner Vertrag endlich Grundrechtsstatus erhalten. Ferner hat die EU versucht, mit einem Rahmenbeschluss im Bereich polizeilicher und justizieller Zusammenarbeit, den Datenschutz zu stärken. Viele Bestimmungen sind jedoch ungenau und überlassen den nationalen Behörden die Interpretationshoheit bei der Weitergabe und Nutzung von personenbezogenen Daten.
- Neben der hoheitlichen Datennutzung ist Datenmissbrauch im privaten Sektor ein wachsendes Problem. Auch hier sind stärkere Grenzen zu ziehen und strafrechtliche Maßnahmen vorzusehen. Die Vorratsdatenspeicherung erzeugt ein weiteres Vertrauensproblem an der Schnittstelle zwischen hoheitlicher Datennutzung und privatwirtschaftlicher Datenspeicherung.

JUNI 2009

Inhalt

1	Einleitung.....	2
2	Sicherheit und Bürgerrechte.....	2
3	Grundrecht Datenschutz.....	3
4	Der private Sektor: Datenschutz ist Verbraucherschutz	3

1 Einleitung

Die europäische Öffentlichkeit wurde in den letzten Jahren in immer kürzeren Abständen von Datenschutzskandalen erschüttert, die zum einen durch Fehler öffentlicher Institutionen (Großbritannien), zum anderen durch geradezu kriminellen Missbrauch von Mitarbeiter- und Kundendaten in Unternehmen (Deutschland) ausgelöst wurden. Diese Skandale begleiteten und diskreditierten diverse Gesetzesinitiativen auf Ebene der Mitgliedstaaten wie auch auf EU-Ebene, die die Zugriffsmöglichkeiten von Polizei und Justiz auf die Daten der Bürgerinnen und Bürger erweitern und den Datenaustausch zwischen den Polizeibehörden verbessern sollen. Die Ziele dieser Gesetzesvorhaben, die Bekämpfung von Kriminalität und Terrorismus, sind dabei auch in der breiteren Öffentlichkeit ein durchaus akzeptiertes Anliegen. Doch in welchem Umfang gefährden diese Maßnahmen die Privatsphäre und die Grundrechte der Bürger und Bürgerinnen?

2 Sicherheit und Bürgerrechte

Die Debatte über die Grenzen des staatlichen Zugriffs auf Internet- und Kommunikationsdaten entzündete sich vor allem in Deutschland an der Vorratsdatenspeicherung, wobei der deutsche Innenminister mit seinen Forderungen nach erweiterten Möglichkeiten zur Onlinedurchsuchung bereits erheblich zur Verunsicherung der Bevölkerung beigetragen hatte. Unstrittig ist, dass Polizei und Ermittlungsbehörden in einer zunehmend technisierten und globalisierten Welt stärker auf den Austausch von Daten und die Überwachung von Kommunikation über das Internet oder andere Netze angewiesen sind als je zuvor. Mit Blick auf die Zunahme der Nutzung des Internets für kriminelle Machenschaften bzw. die enorme Zunahme der im Internet verübten Straftaten muss der Staat die notwendigen Instrumente erhalten, um die Menschen auch online angemessen schützen zu können. Laut einer forsa-Umfrage sind bereits über vier Millionen Deutsche Opfer von Internetkriminalität geworden, wobei die meisten der Betroffenen durch Phishing, Kreditkartenbetrug oder Virentacken einen finanziellen Schaden erlitten.

Auf Ebene der EU ist die Notwendigkeit zu einem verstärkten Datenaustausch schon aufgrund des Schengenraums gegeben. In einem Gebiet der offenen Grenzen und zusammenwachsender Wirtschaftsräume ergeben sich für die organisierte Kriminalität grenzenlose Betätigungsfelder. Nationale Polizeibehörden und isolierte Fahndungsdatenbanken allein werden mit dieser Internationalisierung der Kriminalität nicht mehr fertig werden. Das Schengener-Informationssystem (SIS), Europol, das Visa-Informationssystem (VIS), die Abfrage von DNA-Daten (Prümer Vertrag) und auch die Vorratsdatenspeicherung sind Antworten auf diese Problemstellung. Die Legitimität dieser Maßnahmen ist aber immer nur dann sichergestellt, wenn die erweiterte Verfügbarkeit persönlicher Daten in einem angemessenen Verhältnis zur Freiheit der Persönlichkeit, dem Schutz der Privatsphäre und der informationellen Selbstbestimmung steht.

Daher müssen für alle Maßnahmen, die die Speicherung, Verarbeitung oder Weitergabe von persönlichen Daten beinhalten, folgende Bedingungen erfüllt sein:

1. Die Erfassung von persönlichen Daten erfolgt ausschließlich zu einem klar definierten und begrenzten Zweck. Umfang und Verwendung der erfassten Daten müssen im Hinblick auf den Zweck der Maßnahme und die Stärke des Eingriffs in die Persönlichkeitsrechte verhältnismäßig sein. Die Verhältnismäßigkeit ist umfassend darzustellen.
2. Die Speicherung, Verarbeitung und Weitergabe der Daten muss einen wirklichen Fortschritt für die spezifische Verbrechensbekämpfung versprechen und für die Ermittlungsarbeiten unbedingt notwendig sein. Die Notwendigkeit sowie die Verhältnismäßigkeit des Eingriffs sind regelmäßig vom Gesetzgeber zu überprüfen.
3. Der Betroffene muss die gespeicherten Daten einsehen und fehlerhafte Informationen löschen lassen können.
4. Die Sicherheit der Daten muss jederzeit gewährleistet sein.
5. Die Weitergabe an andere Dienststellen oder Drittstaaten darf nur erfolgen, wenn das Datenschutzniveau ebenso hoch ist wie in der EU.
6. Es ist gesetzlich zu gewährleisten, dass die gespeicherten Daten nicht für zweckfremde Maßnahmen genutzt werden (sog. Datamining). Eine abweichende oder ausgeweitete Nutzung vorhandener Datenbestände darf nur aufgrund einer neuen gesetzlichen Grundlage erfolgen. Et-

* Die Arbeitsgruppe »Europäische Integration« des Europabüros der FES in Brüssel besteht seit mehr als zehn Jahren. Mitglieder sind Fachleute aus den europäischen Institutionen, Bundesministerien, Ländervertretungen sowie aus Verbänden und Wissenschaft.

waiges Anzapfen von Datenbeständen durch die Hintertür – Komitologieverfahren, ministerielle Verordnungen – muss ausgeschlossen werden.

Die Anforderungen zur Begründung der Notwendigkeit und der Verhältnismäßigkeit sind von Beginn an in Gesetzesinitiativen und Vorschläge von Regierungsvertretern einzubeziehen. Zu oft haben Minister und Kommissare aufgrund der Medienberichterstattung neue Überwachungsmaßnahmen angekündigt, die sich weder als geeignet noch als grundrechtskonform erwiesen haben. So hat der damalige EU-Kommissar Frattini mit einer Reihe von angekündigten Initiativen, wie z. B. der Überwachung der Ein- und Ausreise sowie der Seegrenzen oder zu einem europäischen System der Fluggastdatenerfassung, für erhebliche Verunsicherung gesorgt. Dabei wird der Nutzen solcher Systeme für die Sicherheit der Bürger und Bürgerinnen stark in Zweifel gestellt. In Großbritannien, wo die Fluggastdatenerfassung in einem Pilotprojekt läuft, sind bis jetzt vorwiegend illegal Einreisende »Opfer« dieser Maßnahmen geworden. Einen Schub im Hinblick auf die Bekämpfung schwerer Verbrechen oder terroristischer Aktionen hat es nicht gegeben. Bevor die Bevölkerung mit der Ankündigung neuer Eingriffe in ihre Privatsphäre beunruhigt wird, sollten an die Initiativen von Europäischer Kommission und nationalen Ministerien von Beginn an hohe Ansprüche bei der Begründung von Grundrechtseingriffen gestellt werden.

3 Grundrecht Datenschutz

In der Europäischen Union erhält der Datenschutz mit Inkrafttreten des Lissabonner Vertrags nun endlich Grundrechtsstatus, da der Schutz persönlicher Daten in Artikel 8 der Grundrechtecharta verbrieft ist. Im Bereich des Binnenmarktes ist der Datenschutz durch die Richtlinie 95/46/EG geregelt, die vor allem durch die Einrichtung der sog. Artikel 29 Datenschutzgruppe einen erheblichen Beitrag zur Verbesserung des Datenschutzes auf EU-Ebene geleistet hat. Dieses unabhängige Expertengremium bewertet ebenso wie der Europäische Datenschutzbeauftragte alle Maßnahmen der EU, die die persönlichen Daten von EU-Bürgern betreffen und nimmt so Einfluss auf die Gesetzesinitiativen der Europäischen Kommission sowie auf die Debatten des Europäischen Parlaments.

Der dritten Säule der EU-Zuständigkeiten im Bereich polizeiliche und justizielle Zusammenarbeit (PJZ) fehlte es lange an einem Rahmen für den

Datenschutz. Zwar beinhalten die einzelnen Maßnahmen jeweils spezifische Datenschutzvorschriften, doch mangelte es an grundsätzlichen Vorschriften für die Speicherung, Verarbeitung und Weitergabe von Daten im Rahmen der Strafverfolgung. Nun wurde der Rahmenbeschluss über Datenschutz im Bereich der PJZ im letzten Jahr nach über dreijährigen Verhandlungen endlich durch den Ministerrat verabschiedet. Er wird jedoch von Datenschützern aus verschiedenen Gründen kritisiert. Viele Bestimmungen sind sehr ungenau und überlassen den nationalen Behörden die Interpretationshoheit bei der Weitergabe und Nutzung von personenbezogenen Daten. Daneben müsste die Weitergabe von Daten an Drittstaaten wesentlich stärker begrenzt werden. Dieser Punkt war bereits bei der Debatte über die Weitergabe von Fluggastdaten (sogenannte PNR-Daten) an die USA von entscheidender Bedeutung, da sensible persönliche Daten von EU-Bürgern hier regelmäßig und für bis zu 15 Jahre an einen Drittstaat weitergegeben werden. Die Bürger und Bürgerinnen müssen sich darauf verlassen können, dass solche Vorgänge ihre Privatsphäre respektieren und ausreichender Rechtsschutz besteht. Daran besteht bei dem Abkommen mit den USA erheblicher Zweifel. Darüber hinaus zeigt die Weitergabe von Bankdaten Europäischer Bürgerinnen und Bürger durch das Unternehmen SWIFT an amerikanische Behörden, dass die EU sich im Rahmen des transatlantischen Dialogs stärker gegen solche Begehrlichkeiten wehren muss. Der Schutz der Grundrechte der Menschen in Europa muss Vorrang haben vor diplomatischen Freundschaftsdiensten. Die Anforderung und Weitergabe von Daten darf nur auf Grundlage rechtsstaatlich einwandfreier Verfahren unter Beachtung der Verfahrensrechte der Betroffenen erfolgen.

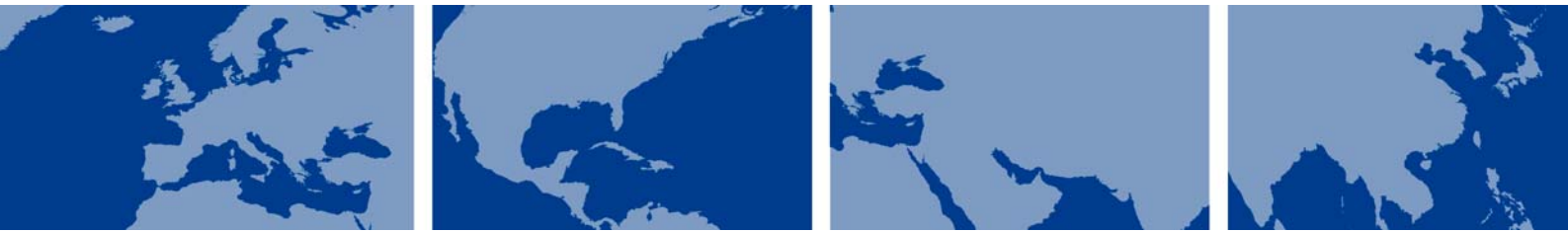
4 Der private Sektor: Datenschutz ist Verbraucherschutz

Doch nicht nur die polizeiliche Zusammenarbeit hat Mängel im Bereich des Datenschutzes. Viele bekannt gewordene Datenschutzprobleme der letzten Monate sind im privaten Sektor und insbesondere in Firmen erfolgt. Die Sicherheit von Mitarbeiter- und Kundendaten ist daher neu zu bewerten und europaweit restriktiver zu regeln. Ebenfalls muss der Schutz der Privatsphäre im Internet stärker in den Fokus rücken. Dazu gehört die Frage, inwieweit Provider und andere Anbieter Kunden- und Benutzerdaten für kommerzielle Zwecke verwenden dür-

fen und wo hier Grenzen zu ziehen sind (siehe Telekom, Microsoft, Google, Facebook). Sollten das Europäische Parlament und der Rat der Europäischen Union im Vermittlungsausschuss eine Einigung beim Telekompaket erzielen, ist mit einigen Verbesserungen beim Datenschutz im Rahmen der elektronischen Kommunikation zu rechnen. Welche weiteren konkreten Maßnahmen notwendig sind, hängt vom endgültigen Verhandlungsergebnis ab.

Die Problematik der Nutzung von Kundendaten bei Telekommunikationskonzernen und Internet Providern hat durch die Vorratsdatenspeicherung eine neue Dimension erhalten. Um den Staat und vor allem die Polizei nicht dem Verdacht auszusetzen, man wolle jetzt sämtliche Lebensbereiche der Bevölkerung systematisch erfassen, sieht die entsprechende Richtlinie die Speicherung der Daten bei den privaten Dienstleistern vor. Erst aufgrund einer richterlichen Verfügung erhalten die Strafverfolgungsbehörden Zugang zu den Daten. Die Vorratsdaten sollen dem Gesetze nach zwar getrennt von anderen Firmendaten gespeichert und dürfen nicht von den Unternehmen genutzt werden – die Datenschutzskandale der letzten Jahre lassen aber stark daran zweifeln, dass die betriebliche Praxis sich an dieses Gebot halten wird. Diese Missbrauchsgefahr ist aufgrund ihrer Dimension auf europäischer Ebene neu zu bewerten. Alternative Lösungen sollten gesucht werden – im Zweifelsfall ist auf die Vorratsdatenspeicherung zu verzichten. In jedem Fall sind die Mitgliedstaaten aufgefordert, bei Verstößen gegen den innerbetrieblichen Datenschutz auch strafrechtliche Maßnahmen vorzusehen. Finanzielle Sanktionen allein, wenn auch wie im Fall Lidl in Millionenhöhe, scheinen bei den Dimensionen der Datenskandale nicht abschreckend genug zu sein.

Abschließend sollte auch über Maßnahmen nachgedacht werden, die den Online-Nutzer vor unabsichtlicher Weitergabe persönlicher Daten schützen. Denn der Datenschutz im Internet ist häufig durch unreflektiertes und uninformiertes Verhalten der Benutzer bedingt und nicht allein durch Datenschutzlecks bei Unternehmen. So werden private Informationen in offene Bereiche von sozialen Netzwerken oder anderen Plattformen eingestellt, in der Annahme, diese stünden nur einer begrenzten Personenzahl zur Verfügung. Dieser Entwicklung wird man nicht nur durch Informationskampagnen begegnen können, es werden auch Maßnahmen von Seiten der Anbieter nötig sein, die die Benutzer darauf aufmerksam machen. Denn für neue wie ungeübte Anwender darf das Internet nicht zu einer Gefahr für ihre Privatsphäre werden.



Impressum

Friedrich-Ebert-Stiftung
Internationale Politikanalyse
Abteilung Internationaler Dialog
D-10785 Berlin

www.fes.de/ipa
E-Mail: info.ipa@fes.de

ISBN: 978-3-86872-118-8

Bestellungen

Friedrich-Ebert-Stiftung
Internationale Politikanalyse
Nora Neye
D-10785 Berlin

E-Mail: info.ipa@fes.de
Fax: +49 (30) 26935-9248

Alle Texte sind online verfügbar:

www.fes.de/ipa

Die in dieser Publikation zum Ausdruck kommenden Meinungen sind die des Autors/der Autorin und spiegeln nicht notwendigerweise die Meinung der Friedrich-Ebert-Stiftung wider.