

Sicherheit und Preis persönlicher Daten



Bericht von Mathias Bug

Bevölkerungsvertrauen in digitalisierte Sicherheitspolitik 783

Interview mit Mathias Bug

»Vorratsdatenspeicherung wird kritisch beurteilt« 792

Bericht von Nicola Jentzsch

Monetarisierung der Privatsphäre:
Welchen Preis haben persönliche Daten? 793

Am aktuellen Rand Kommentar von Marcel Fratzscher

Deutschlands Schwäche ist selbst verschuldet 800



DIW Berlin – Deutsches Institut
für Wirtschaftsforschung e.V.
Mohrenstraße 58, 10117 Berlin
T +49 30 897 89 -0
F +49 30 897 89 -200
81. Jahrgang
20. August 2014

Herausgeber

Prof. Dr. Pio Baake
Prof. Dr. Tomaso Duso
Dr. Ferdinand Fichtner
Prof. Marcel Fratzscher, Ph.D.
Prof. Dr. Peter Haan
Prof. Dr. Claudia Kemfert
Prof. Karsten Neuhoff, Ph.D.
Dr. Kati Schindler
Prof. Dr. Jürgen Schupp
Prof. Dr. C. Katharina Spieß
Prof. Dr. Gert G. Wagner

Chefredaktion

Sabine Fiedler
Dr. Kurt Geppert

Redaktion

Renate Bogdanovic
Andreas Harasser
Sebastian Kollmann
Dr. Claudia Lambert
Dr. Anika Rasner
Dr. Wolf-Peter Schill

Lektorat

Prof. Dr. Martin Kroh
Isabel Teichmann

Textdokumentation

Manfred Schmidt

Pressestelle

Renate Bogdanovic
Tel. +49-30-89789-249
presse@diw.de

Vertrieb

DIW Berlin Leserservice
Postfach 74
77649 Offenburg
leserservice@diw.de
Tel. (01806) 14 00 50 25
20 Cent pro Anruf
ISSN 0012-1304

Gestaltung

Edenspiekermann

Satz

eScriptum GmbH & Co KG, Berlin

Druck

USE gGmbH, Berlin

Nachdruck und sonstige Verbreitung –
auch auszugsweise – nur mit Quellen-
angabe und unter Zusendung eines
Belegexemplars an die Serviceabteilung
Kommunikation des DIW Berlin
(kundenservice@diw.de) zulässig.

Gedruckt auf 100 % Recyclingpapier.



Der DIW Wochenbericht wirft einen unabhängigen Blick auf die Wirtschaftsentwicklung in Deutschland und der Welt. Er richtet sich an die Medien sowie an Führungskräfte in Politik, Wirtschaft und Gesellschaft. Wenn Sie sich für ein Abonnement interessieren, können Sie zwischen den folgenden Optionen wählen:

Standard-Abo: 179,90 Euro im Jahr (inkl. MwSt. und Versand).

Studenten-Abo: 49,90 Euro.

Probe-Abo: 14,90 Euro für sechs Hefte.

Bestellungen richten Sie bitte an leserservice@diw.de oder den DIW Berlin Leserservice, Postfach 74, 77649 Offenburg; Tel. (01806) 14 00 50 25, 20 Cent/Anruf aus dem dt. Festnetz, 60 Cent maximal/Anruf aus dem Mobilnetz. Abbestellungen von Abonnements spätestens sechs Wochen vor Laufzeitende

NEWSLETTER DES DIW BERLIN



Der DIW Newsletter liefert Ihnen wöchentlich auf Ihre Interessen zugeschnittene Informationen zu Forschungsergebnissen, Publikationen, Nachrichten und Veranstaltungen des Instituts. Wählen Sie bei der Anmeldung die Themen und Formate aus, die Sie interessieren. Ihre Auswahl können Sie jederzeit ändern, oder den Newsletter abbestellen. Nutzen Sie hierfür bitte den entsprechenden Link am Ende des Newsletters.

>> Hier Newsletter des DIW Berlin abonnieren: www.diw.de/newsletter

RÜCKBLIQUE: IM WOCHENBERICHT VOR 50 JAHREN

Die Leistungen der privaten Hypothekenbanken zur Wohnungsbaufinanzierung 1964/65

Die in der letzten Zeit angekündigten bzw. durchgeführten kreditpolitischen Maßnahmen haben zu einer Erhöhung der Pfandbriefrendite und damit auch zu einer Verteuerung der Wohnungsbaufinanzierung geführt. Da die Wohnungsbauinvestitionen auf Änderungen der Kreditkonditionen trotz intensiver staatlicher Förderung nachweisbar zu reagieren pflegen, ist damit zu rechnen, daß die Nachfrage nach Wohnungsbaudarlehen und damit die Zusagen und Leistungen der Kapitalsammelstellen nennenswert abnehmen werden.

Allerdings werden die kreditpolitischen Maßnahmen die institutionellen Träger des Realkredits sehr ungleichmäßig treffen. Besonders stark wird das Kreditgeschäft der privaten Hypothekenbanken beeinträchtigt werden; da diese Institute sich fast ausschließlich durch die Emissionen von Pfandbriefen refinanzieren, werden die Konditionen, zu denen die Hypothekenbanken neue Wohnungsbaudarlehen zusagen können, weitgehend durch die Pfandbriefrendite bestimmt. Dagegen wird das Mittelaufkommen der Versicherungen und Sparkassen von den bisherigen kreditpolitischen Maßnahmen nahezu unbeeinflusst bleiben. Zwar werden sich alle Institute in ihren Darlehenskonditionen der Entwicklung der Pfandbriefrendite tendenziell angleichen, die Sparkassen und insbesondere die Versicherungen können aber ihren Darlehensnehmern günstigere Konditionen als die Hypothekenbanken gewähren. Ein hoher Pfandbriefsatz wirkt sich daher in mehrfacher Hinsicht auf die Zusagen und damit letztlich auch auf die Leistungen der privaten Hypothekenbanken aus: Aufgrund der Zinselastizität des Wohnungsbaus verringert sich allgemein die Nachfrage nach Darlehen, aber zusätzlich wird diese verminderte Nachfrage sich teilweise auf andere Institute verlagern und damit das Ausmaß der Auszahlungen von Wohnungsbaudarlehen durch Hypothekenbanken weiter abnehmen.

aus dem Wochenbericht Nr. 34 vom 21. August 1964

Bevölkerungsvertrauen in digitalisierte Sicherheitspolitik

Von Mathias Bug

Sowohl die Wirtschaft als auch die Sicherheitspolitik bauen mehr und mehr auf die Nutzungs- und Analysemöglichkeiten von personenbezogenen Daten. Diese Möglichkeiten der Nutzung werden in der Bevölkerung allerdings nicht uneingeschränkt positiv bewertet. Das betrifft insbesondere digitale Überwachungsmaßnahmen. Das DIW Berlin hat analysiert, welches Vertrauen Überwachungsmaßnahmen wie die Vorratsdatenspeicherung oder die Speicherung von Fluggastdaten in der Bevölkerung genießen und inwieweit dieses Vertrauen von den an der Überwachung beteiligten Akteuren beeinflusst wird. Außerdem wurde untersucht, wie die Bevölkerung den Datenaustausch personenbezogener Daten zwischen deutschen Sicherheitsbehörden, zwischen den EU-Mitgliedstaaten und mit Drittstaaten wie den USA bewertet. Dazu wurde das Bevölkerungsvertrauen auf Basis von repräsentativen Daten des Forschungsprojektes Sicherheit im öffentlichen Raum (SIRA) analysiert. Die zugrundeliegende Befragung wurde im November und Dezember 2011 durchgeführt.

Große Unterschiede zeigen sich in der Akzeptanz der verschiedenen Überwachungsmaßnahmen. Die Übermittlung von Fluggastdaten wird positiver beurteilt als die Vorratsdatenspeicherung. Die an der Speicherung von Vorratsdaten und Fluggastdaten beteiligten Unternehmen genießen in der Bevölkerung hingegen nur bedingtes Vertrauen. Kritisch werden vor allem deren Umgang und der Schutz der erhobenen Daten gesehen. Personen, die den Austausch personenbezogener Daten positiv bewerten, haben auch eher Vertrauen in die Arbeit der Sicherheitsbehörden und der privaten Sicherheitsunternehmen.

Die Digitalisierung aller Lebensbereiche, der Wirtschaft und der gesamten Grundversorgung der Bevölkerung zieht seit Jahren Kritik und Hoffnung gleichermaßen an.¹ Wo auf der einen Seite ganz neue Wirtschaftszweige entstehen, sehen andere die Entwicklung einer kritischen Infrastruktur² oder die Aufgabe jeglicher Privatheit, derer sich niemand entziehen kann. Dieses ambivalente Meinungsbild zeigt sich auch in Bevölkerungsbefragungen zum Thema.³ Die grundsätzlich positive Einschätzung der Potentiale der technologischen Entwicklung wurde durch zahlreiche Veröffentlichungen zu den Überwachungsmöglichkeiten von US-amerikanischen und britischen, aber auch kontinentaleuropäischen Geheimdiensten vorerst nicht beeinträchtigt. In der Bevölkerung besteht jedoch ein großes Misstrauen in den Umgang mit persönlichen Daten durch staatliche Stellen und Unternehmen (wie zum Beispiel Kommunikationsdienstleister und Flugverkehrsunternehmen).⁴

Dieses Misstrauen dürfte sich nach den medial stark aufgearbeiteten Fällen von Datendiebstahl Anfang 2014⁵ und schließlich aktuell durch vermeintlich russische Hacker⁶ eher noch vergrößern. Da die Auswertung digitaler personenbezogener Daten aber eine zwingend notwen-

¹ Das Projekt wurde im Zuge der Bekanntmachung *Gesellschaftliche Dimensionen der Sicherheitsforschung* im Rahmen des Programms *Forschung für die zivile Sicherheit* der Bundesregierung vom Bundesministerium für Bildung und Forschung (BMBF) gefördert. Es wurde an der Universität der Bundeswehr München durchgeführt.

² Dabei wird das Netz in einem doppelten Sinne als kritische Infrastruktur gesehen: Einerseits direkt als zentrale Kommunikationsinfrastruktur, andererseits mittelbar durch die Vernetzung weiterer kritischer Infrastrukturen wie Wasser oder Energieversorgung.

³ Institut für Demoskopie Allensbach (2014): Die Zukunft der digitalen Gesellschaft. Allensbach, www.digitalhist.de/index.php?id=201, abgerufen am 5. August 2014.

⁴ Institut für Demoskopie Allensbach (2013): Wirkungslose Aufregung. www.ifd-allensbach.de/uploads/tx_reportsdocs/August21_Aufregung.pdf, 19 f., abgerufen am 5. August 2014.

⁵ Tagesschau.de (7. April 2014): BSI stellt Sicherheitstest online. www.tagesschau.de/inland/sicherheitstest-bsi100.html, abgerufen am 6. August 2014.

⁶ Perlroth, N., Gelles, D. (5. August 2014): Russian Gang Amasses Over a Billion Internet Passwords. www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?hp&action=click&pgtype=Homepage&version=LedeSum&module=first-column-region%2%AEion=top-news&WT.nav=top-news&_r=0, abgerufen am 5. August 2014.

Kasten 1

Datenbasis

Die Datenbasis entstand im Rahmen des Teilprojektes 7 *Der Einfluss Institutioneller Regimes auf die Akzeptanz von Sicherheitsmaßnahmen* im Verbundprojekt *Sicherheit im öffentlichen Raum (SIRA)*, gefördert vom Bundesministerium für Bildung und Forschung (BMBF) an der Universität der Bundeswehr München.

Im November und Dezember 2011 wurden dafür 1 257 Personen repräsentativ in Deutschland durch das Zentrum für empirische Sozialforschung der HU Berlin telefonisch befragt. Im Rahmen eines Dual Frame Ansatzes wurden 15 Prozent der Befragten über Mobilfunknummern erreicht. Sowohl die Festnetz- als auch die Mobilnummern wurden nach dem ADM-Design für Telefonstichproben gezogen.¹ Telefonnummernstämme wurden regional geschichtet gezogen und die letzten Nummern randomisiert. Eine Gewichtung der Stichprobe fand nicht statt.

¹ Gabler, S., Häder, S. (2009): Die Kombination von Mobilfunk- und Festnetzstichproben in Deutschland. In: Weichbold, M., Bacher, J., Wolf, C. (Hrsg.): *Umfrageforschung: Herausforderungen und Grenzen*. Österreichische Zeitschrift für Soziologie Sonderheft 9, Wiesbaden, 239-252.

Folgende Fragewortlaute sind für diesen Wochenbericht relevant:

Beurteilung Vorratsdatenspeicherung (C5.1, C5.2)

- C5.1: Wie gut oder wie schlecht finden Sie diese Maßnahme, sehr gut, eher gut, eher schlecht, sehr schlecht?
- C5.2: Aus den Daten geht hervor mit wem Sie wann und wie lange telefoniert haben und mit wem Sie wann E-Mail- oder SMS-Kontakt hatten. Bei Handynutzung wird auch der Standort festgehalten. Halten Sie die Vorratsdatenspeicherung für sehr gut, eher gut, eher schlecht, sehr schlecht?

Deutschland – Vorratsdatenspeicherung – Vertrauen in Maßnahme und Akteure (C51 A–C):

- A. Fühlen Sie sich durch diese Maßnahme sicher?
- B. Gehen Sie davon aus, dass Kommunikationsunternehmen im Rahmen der Vorratsdatenspeicherung mit Ihren Telefon- und Internetdaten mit Ihren Daten vertrauenswürdig umgehen?
- C. Gehen Sie davon aus, dass Behörden im Rahmen der Vorratsdatenspeicherung mit Ihren Telefon- und Internetdaten vertrauenswürdig umgehen?

dige Voraussetzung für die Verbrechensbekämpfung im und mit Hilfe des Internets ist, müssen Bedenken in der Bevölkerung entsprechend ernst genommen werden.

Ganz konkret engt sich mit einer steigenden Skepsis gegenüber dem Umgang mit persönlichen Daten bei Unternehmen und Staat demnach auch der Spielraum für staatliche Sicherheitsmaßnahmen ein. Die Urteile zur Vorratsdatenspeicherung des Bundesverfassungsgerichts⁷ und des Europäischen Gerichtshofs⁸ weisen in diese Richtung.⁹

⁷ BVerfG, 1 BvR 256/08 vom 2. März 2010, Absatz-Nr. (1 – 345), www.bverf.de/entscheidungen/rs20100302_1bvr025608.html, abgerufen am 5. März 2014.

⁸ EuGH (2014): Urteil in den verbundenen Rechtssachen C-293/12 und C-594/12: Digital Rights Ireland und Seitlinger u. a. curia.europa.eu/jcms/jcms/P_125953/, abgerufen am 5. August 2014.

⁹ In Richtung einer solchen Eingrenzung argumentieren auch Böhm, F., Cole, M. D. (2014): *Data Retention after the Judgement of the Court of Justice of the European Union*. Insbesondere Kapitel D, E, publications.uni.lu/handle/10993/17500, abgerufen am 5. August 2014. Einen Überblick über die Rolle des Bundesverfassungsgerichts insbesondere bei der Fortentwicklung digitaler Sicherheitsmaßnahmen bieten Schmid, V. (2011): 2. SIRA Conference Series: Innere Sicherheit – auf Vorrat gespeichert?; Bug, M., Münch, U., Schmid, V. (Hrsg.): *Innere Sicherheit – auf Vorrat gespeichert?* Tagungsband 2. SIRA Conference Series. München 2011, nbn-resolving.de/urn/resolver.pl?urn:nbn:de:bvb:706-020, abgerufen am 11. August 2014, 3; Hornung, G., Schnabel, C. (2009): *Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention*. *Computer Law & Security Review* 25: 115–122, tinyurl.com/pgxqk6j, abgerufen am 4. Januar 2012.

Die Studie untersucht, wie die weitreichende verdachtsunabhängige Speicherung und der Austausch persönlicher Daten in der Bevölkerung beurteilt werden und welche Faktoren diese Bewertung beeinflussen. Dabei wird der Datenaustausch zwischen deutschen Sicherheitsbehörden, zwischen EU-Mitgliedstaaten und mit Drittstaaten wie zum Beispiel den USA in den Blick genommen.

Die hier vorgestellte Studie wurde vor dem Skandal rund um die Snowden-Bekanntmachungen und die jüngsten Fälle von Datendiebstahl durchgeführt. Das Antwortverhalten der Befragten ist damit unbeeinflusst von der anhaltenden Medienberichterstattung (Kasten 1).

Vorratsdatenspeicherung wird kritisch beurteilt

Die Vorratsdatenspeicherung gilt als die wohl bekannteste und weitreichendste digitale Überwachungsmaßnahme in Deutschland.¹⁰ Aus den Daten geht hervor,

¹⁰ Eine ausführlichere Analyse zur Entwicklung der Vorratsdatenspeicherung Bukow, S. (2011): *Vorratsdatenspeicherung in Deutschland. Symbol des sicherheitspolitischen Wandels und des zivilgesellschaftlichen Protests?* In: Bug, M. et al. (Hrsg.), a. a. O., 22–55. Eine weiter führende Analyse des SIRA-Datensatzes in

Beurteilung Passagierdaten (E 14.1, E 14.2)

E 14.1: Wie finden Sie diese Maßnahme? Finden Sie sie sehr gut, eher gut, eher schlecht, sehr schlecht?

E 14.2: Zu diesen Daten gehören unter anderem Name, Geschlecht, Staatsangehörigkeit und Daten zum genauen Reiseverlauf. Wie finden Sie diese Maßnahme?

Beurteilung – Passagierdaten –

Vertrauen in Maßnahme und Akteure (E 14.1 A–C):

- A. Fühlen Sie sich durch diese Maßnahme am Flughafen sicher?
- B. Gehen Sie davon aus, dass Verkehrsunternehmen mit Ihren Ausweis- und Passagierdaten vertrauenswürdig umgehen?
- C. Gehen Sie davon aus, dass Behörden mit Ihren Ausweis- und Passagierdaten vertrauenswürdig umgehen?

Bewertung Datenaustausch zwischen Polizeien/Verfassungsschutz/Geheimdienst (H1): Wie bewerten Sie den Datenaus-

tausch zwischen deutschen Polizeien, Verfassungsschutz und Geheimdienst? Halten Sie ihn für sehr gut, eher gut, eher schlecht, sehr schlecht?

Bewertung Datenaustausch mit europäischen Mitgliedsstaaten (H2):

- Wie ist das mit dem Datenaustausch zwischen den Mitgliedstaaten der Europäischen Union? Halten Sie ihn für sehr gut, eher gut, eher schlecht oder sehr schlecht?
- Bewertung Datenaustausch mit außereuropäischen Staaten wie USA (H3): Wie ist das mit dem Datenaustausch mit Staaten außerhalb der EU, wie z. B. den USA. Halten Sie ihn für sehr gut, eher gut, eher schlecht oder sehr schlecht?

Wahlpräferenz Innere Sicherheit (G 5A, G 5B)

- A. Wie wichtig sind bei Ihrer Wahlentscheidung die Forderungen einer Partei zur Inneren Sicherheit?
- B. Wie wichtig wären bei Ihrer Wahlentscheidung die Forderungen einer Partei zur Inneren Sicherheit?

wer mit wem, wann und wie lange telefoniert hat, E-Mail- oder SMS-Kontakt hatte, und wer wann online war. Bei Handynutzung wird auch der Standort festgehalten. Die Daten wurden in Deutschland für sechs Monate bei den Kommunikationsunternehmen gespeichert und konnten bei begründetem Verdacht von Sicherheitsbehörden abgefragt werden. Diese vollumfängliche Speicherung von Kommunikationseckdaten (oder auch Metadaten) erlaubt Rückschlüsse über das grundsätzliche Kommunikationsverhalten, Kontaktpersonen aber auch die Analyse persönlicher Kontaktnetzwerke und Bewegungsprofile. Die Reichweite der Vorratsdatenspeicherung hat Gerichte auf bundesdeutscher wie auf EU-Ebene dazu bewegt, die gesetzlichen Regelungen der Maßnahmen ohne zeitlichen Aufschub außer Kraft zu setzen. Die grundsätzliche Einschätzung der Bevölkerung zur Vorratsdatenspeicherung in Deutschland ist

entsprechend kritisch.¹¹ Insgesamt weist das Antwortverhalten der Befragten darauf hin, dass die Vorratsdatenspeicherung lediglich von einer Minderheit der Bevölkerung uneingeschränkt mitgetragen wird. Fast zwei Drittel der Bevölkerung stehen dieser Maßnahme hingegen ablehnend gegenüber (Abbildung 1).

Neben der geringen Akzeptanz trägt die Vorratsdatenspeicherung zudem nur bei wenigen Befragten zu einem erhöhten Sicherheitsgefühl bei. Das Vertrauen in den Datenumgang fällt dabei ebenso kritisch aus, hängt aber stark von den beteiligten Akteuren ab. Behörden genießen gegenüber privaten Kommunikationsunternehmen ein deutlich höheres Vertrauen im Umgang mit den Daten. In diesem Zusammenhang fällt insbesondere der Anteil an Befragten mit dezidiert positiver oder negativer Bewertung auf (Abbildung 2). Demnach können Kommunikationsunternehmen auf eine verschwindend kleine Gruppe an Befragten (drei Prozent) bauen, die ein uneingeschränktes Vertrauen in ihren Umgang mit personenbezogenen Daten haben. Dem gegenüber steht ein knappes Drittel der Befragten, das entschie-

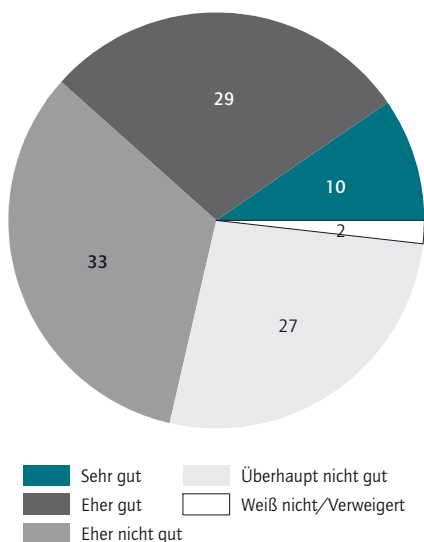
Bezug auf Vorratsdatenspeicherung unter Bug, M. (2014 b): Innere Sicherheit – digital und vernetzt. In: Röllgen, J.: „Wie die Statistik belegt...“ 3. SIRA Conference Series, 45–70, athene.bibl.unibw-muenchen.de:8081/node?id=92194, abgerufen am 18. August 2014; Bug, M. (2013): Societal Divide Regarding Attitudes towards Digitised Security Measures? British versus German Perspectives. In: Löblich, M., Pfaffrüdiger, S.: Communication and Media Policy in the Era of Digitization and the Internet. Book Series of the Center on Governance, Communication, Public Policy and Law at Ludwig-Maximilians-Universität München, 159–174.

¹¹ In der parallel durchgeführten Befragung in Großbritannien fiel die Bewertung der Maßnahme ähnlich kritisch aus – Deutschland spielt hier insofern keine Sonderrolle innerhalb der EU. Siehe dazu Bug, M. (2013), a. a. O.; Bug, M. (2014 b), a. a. O.

Abbildung 1

Beurteilung der Vorratsdatenspeicherung

In Prozent (N = 1 058)



Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

© DIW Berlin 2014

Nur wenige Befragte befürworten die Vorratsdatenspeicherung uneingeschränkt.

ne Zweifel an den Kommunikationsanbietern meldet. In Anbetracht dieser Verteilung wirkt es fast verwunderlich, dass von Seiten der Politik die Speicherung bei den Kommunikationsanbietern direkt anstatt bei Sicherheitsbehörden selbst, als unterstützendes Argument für die Wiedereinführung der Maßnahme über mehrere Jahre hinweg angeführt wurde.

Fluggastdatenspeicherung steigert das Sicherheitsgefühl

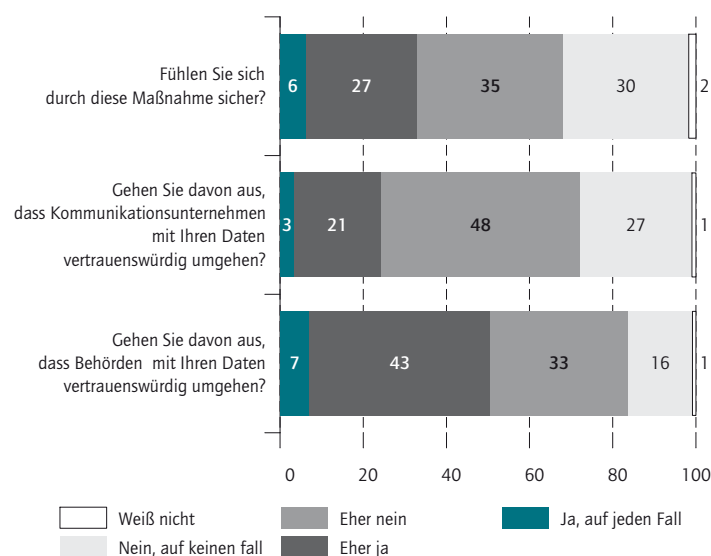
Die Fluggastdatenspeicherung und insbesondere die direkte Übermittlung der gesammelten Daten an die USA (aber auch an weitere Länder wie Kanada und Australien)¹² ist ein Kristallisationspunkt im Ringen um transatlantische Übereinkünfte zur Datenübermittlung.¹³ Die Fluggastdaten geben Auskunft über die Eckpunkte der Flug- oder Schifffreise, was Zahlungsmodalitäten und Daten rund um die Reise wie beispielsweise Hotelbuchungen mit einschließen kann. Dabei werden die Daten automatisiert über die Buchungssysteme der Verkehrsunternehmen an die Sicherheitsbehörden der Länder übermittelt, mit denen ein entsprechendes Abkommen besteht. Der Umfang der Maßnahme erweitert sich insbesondere durch das erklärte Ziel einer EU-weiten Einführung (und dem entsprechenden automatisierten Austausch zwischen den EU-Mitgliedstaaten);¹⁴ aber auch am Interesse an den Daten seitens Ländern wie Russland.¹⁵

Die Maßnahme wird von der Bevölkerung im Vergleich zur Vorratsdatenspeicherung deutlich weniger kritisch bewertet (Abbildung 3).

Die positivere Einschätzung liegt wohl einerseits an der lediglich punktuellen Betroffenheit im Falle einer Reise und andererseits an einem erhöhten Sicherheitsgefühl durch die Maßnahme bei einer Mehrheit der Befragten. In diese Richtung könnte zumindest das positive Sicherheitsgefühl

Abbildung 2

Vorratsdatenspeicherung – Vertrauen in Akteure und Sicherheitsgefühl

In Prozent¹


1 Nur Internetnutzer mit Vorwissen zur Vorratsdatenspeicherung, N = 854.

Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

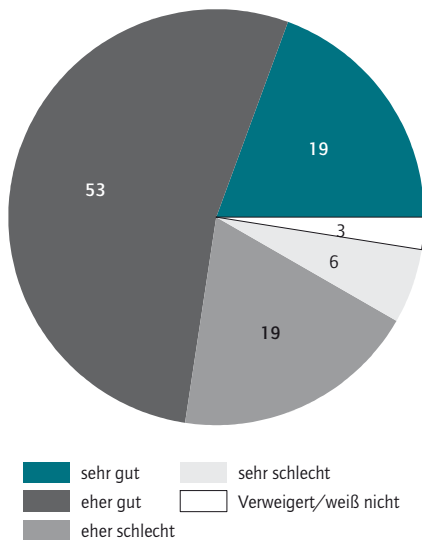
© DIW Berlin 2014

Vorratsdatenspeicherung steigert nur bei wenigen Befragten das Sicherheitsgefühl.

Abbildung 3

Beurteilung der Fluggastdatenspeicherung

In Prozent (N = 799)



Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

© DIW Berlin 2014

Knapp drei Viertel der Befragten bewerten die Speicherung von Fluggastdaten als positiv.

das mit der Maßnahme verbunden wird, interpretiert werden (Abbildung 4).¹⁶ Dennoch vertrauen auch bei der Übermittlung von Fluggastdaten ein Drittel der Befragten dem Datenmanagement privater Akteure wenig oder gar nicht. Die Unterschiede im Vergleich zum Vertrauen in das behördliche Datenmanagement fallen dabei jedoch deutlich geringer aus als im Falle der Vorratsdatenspeicherung.

Vertrauen in Datenaustausch hängt von der Reichweite der ausgetauschten Daten ab

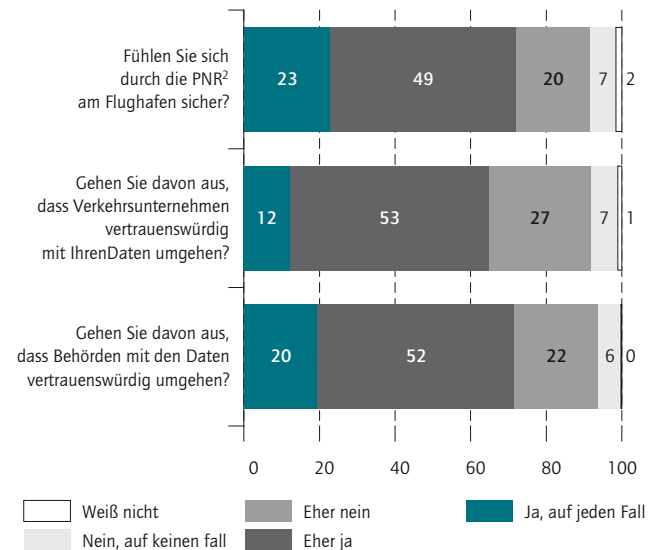
Im Folgenden wird dargestellt, welche Bedeutung die Befragten der Weitergabe von persönlichen Informationen beimessen. Aufgrund mangelnder Transparenz und politischer Aufklärung ist die Reichweite des Datenaustauschs den Betroffenen oft nicht bewusst. Mit dem Datenaustausch ergeben sich Möglichkeiten der Verknüpfung verschiedener Datenquellen, deren Wirkung weit über den originären Bestimmungszweck der Datenspeicherung (zum Beispiel in den Be-

¹⁶ Bug, M. (2014 b), a. a. O., 60.

Abbildung 4

Fluggastdaten – Vertrauen in Akteure und Sicherheitsgefühl

In Prozent¹



¹ Nur Flugpassagiere mit Vorwissen zur Maßnahme, N = 378.

² Passenger Name Record.

Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

© DIW Berlin 2014

Fast drei Viertel der Befragten fühlen sich durch die Übermittlung von Fluggastdaten sicher.

reichen Onlinebanking, Reisen oder Kommunikation) hinausgeht. Der Datenaustausch ist somit für die Befragten weniger fassbar als die Speicherung von Vorrats- oder Fluggastdaten.

Welche Faktoren können Unterschiede in der Bewertung des Datenaustauschs erklären? Hierzu wurden drei aufeinander aufbauende Regressionsmodelle geschätzt. Aus Platzgründen beschränkt sich die Analyse auf die Reichweite des Datenaustauschs.¹⁷ Unter Reichweite wird verstanden, ob die Daten innerhalb Deutschlands oder über die Staatsgrenzen hinaus weiter gegeben werden (Kasten 2).

Datenaustausch zwischen deutschen Sicherheitsbehörden weitgehend akzeptiert

Dem Austausch anlassunabhängig gespeicherter, personenbezogener Daten zwischen deutschen Sicherheitsbehörden stehen zwei Drittel der Befragten eher oder

¹⁷ Die Befunde für die Speicherung von Fluggastdaten und Vorratsdaten werden nicht gezeigt, die Zusammenhänge weisen allerdings in eine vergleichbare Richtung.

Kasten 2

Modell

Die Bewertung des Datenaustausches mit verschiedenen Reichweiten wurde in einem weiteren Analyseschritt als jeweils unabhängige Variable in drei aufeinander aufbauenden Regressionsmodellen auf den Zusammenhang hin mit den Erklärungsmodellen überprüft. Dabei wurden die Antwortkategorien binarisiert und ein Probit-Verfahren angewandt. Ein Probit-Modell schätzt, welche Faktoren die Beurteilung des Datenaustauschs positiv oder negativ beeinflussen.

In einem ersten Modell werden klassische soziodemographische Merkmale, wie zum Beispiel Alter, Geschlecht, Bildung, Größe des Wohnortes, eigene Kinder, alleine Leben und der Migrationshintergrund berücksichtigt. Zudem findet Eingang, inwieweit das Thema Innere Sicherheit bei der Wahlentscheidung der Befragten eine entscheidende Rolle spielt.

Im Modell 2 findet das Vertrauen in die eingebundenen Akteure als erklärende Variable Berücksichtigung. Dazu gehö-

ren neben dem Vertrauen in Landes-/Bundes- und EU-Politik das Vertrauen in die deutschen Gerichte und die Gerichte auf europäischer Ebene sowie das Vertrauen in die Landes-/Bundespolizei und den Verfassungsschutz. Darüber hinaus findet das Vertrauen in private Sicherheitsfirmen im Modell 2 als erklärende Variable Eingang.

Modell 3 koppelt schließlich die Bewertung der konkreten Einzelmaßnahmen Vorratsdatenspeicherung und Fluggastdatenspeicherung mit dem weniger konkreten sondern vielmehr (politisch gewollt) intransparenten und vielschichtigen Austausch personenbezogener Daten. Dadurch wird die Einschätzung von Sicherheitsmaßnahmen die eher punktuell stattfinden, also beispielsweise beim Fliegen, sowie die Bewertung von den Alltag gänzlich umfassenden Maßnahmen wie die Vorratsdatenspeicherung einbezogen.

Tabelle 1

Datenaustausch zwischen deutschen Sicherheitsbehörden

Parameter der Probit-Regressionen (0 = schlecht, 1 = gut)

	Modell		
	1: Sozdem	2: Akteure	3: Einzelmaßnahmen
Alter	0,002	-0,002	-0,001
Geschlecht männlich	0,2320*	0,166	0,2310*
Partner im Haushalt lebend	0,022	0,058	0,026
Eigene Kinder	0,038	0,078	0,054
Städtische Wohngegend	0,066	-0,177	-0,136
Akademischer Hintergrund	-0,036	-0,082	-0,031
Migrationshintergrund	-0,176	-0,113	-0,101
Wahlpräferenz Innere Sicherheit	0,2921*	0,209	0,092
Vertrauen in Landes-/Bundespolitik		0,164	0,112
Vertrauen in EU-Politik		0,045	0,011
Vertrauen in deutsche Gerichte		0,201	0,249
Vertrauen in EuGH		0,051	0,087
Vertrauen in Landes-/Bundespolizei		0,3554*	0,286
Vertrauen in Verfassungsschutz		0,5113***	0,4413***
Vertrauen in private Sicherheitsunternehmen		0,225	0,227
Positive Bewertung PNR in PNR ¹			0,6610***
Positive Bewertung VDS ²			0,158
Konstante	-44 477 812	35 204 791	-0,015

* $p < 0,05$; ** $p < 0,01$; *** $p < 0,001$; Zahl der Befragten: 622.

¹ PNR = Passenger Name Record.

² VDS = Vorratsdatenspeicherung.

Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

© DIW Berlin 2014

sogar sehr positiv gegenüber.¹⁸ Die Gruppe an Befragten mit ganz entschiedenem Misstrauen hingegen fällt mit knapp sieben Prozent sehr klein aus (Abbildung 5).

Männliche Befragte weisen eine höhere Akzeptanz für den Datenaustausch zwischen deutschen Sicherheitsbehörden auf. Gleiches gilt für Personen, die dem Thema Innere Sicherheit eine große Bedeutung beimessen (Tabelle 1).

Dieser Zusammenhang schwächt sich im zweiten Modell jedoch deutlich ab, wenn das Vertrauen in die am Datenaustausch beteiligten Akteure berücksichtigt wird. Dabei wird deutlich, dass großes Vertrauen in den Verfassungsschutz auch mit einer positiven Beurteilung des Datenaustausches zwischen deutschen Sicherheitsbehörden einhergeht. Auch das Vertrauen in die Landes- und Bundespolizeibehörden hängt positiv mit der Akzeptanz des Datenaustauschs zusammen.

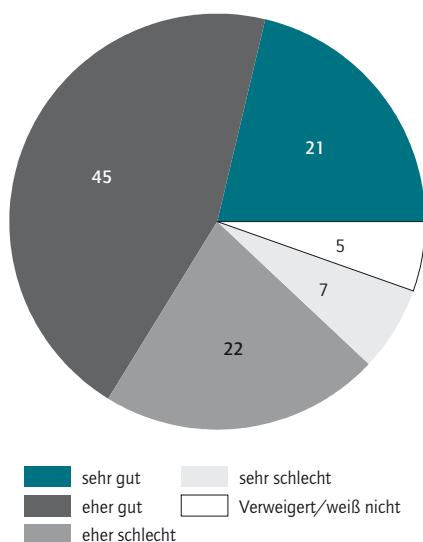
18 Der Befragungszeitpunkt November/Dezember 2011 war medial vom Aufkommen des NSU-Skandals geprägt. Im Mittelpunkt stand dabei die Kritik am mangelnden Informationsaustausch zwischen deutschen Sicherheitsbehörden. Eine Verzerrung hin zu einer positiveren Einschätzung dieser Zusammenarbeit kann daher nicht ganz ausgeschlossen werden – allerdings blieb die Kritik an der mangelnden Zusammenarbeit bis heute aktuell. Eine eingehendere Analyse zur medialen Berichterstattung über die ersten Wochen hinweg unter Bug, M., Röllgen, J., Münch, U. (2013): Föderalismus als Problem – Föderalismus als Lösungsansatz: Eine erste Aufarbeitung im Kontext des Skandals um die rechtsextremen Gewalttaten von Mitgliedern des Nationalsozialistischen Untergrunds (NSU). In: Europäisches Zentrum für Föderalismus-Forschung Tübingen (Hrsg.): Jahrbuch des Föderalismus 2012, Baden-Baden, 138–152.

Es besteht eine größere Akzeptanz für Datenaustausch zwischen deutschen Sicherheitsbehörden bei Männern.

Abbildung 5

Bewertung des Datenaustauschs zwischen deutschen Sicherheitsbehörden

In Prozent (N = 1 257)



Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

© DIW Berlin 2014

Der Austausch personenbezogener Daten zwischen deutschen Sicherheitsbehörden wird von einer deutlichen Mehrheit der Befragten positiv bewertet.

Dieser stark positive Zusammenhang von Vertrauen in den Verfassungsschutz und die Bewertung des Datenaustauschs zwischen den deutschen Sicherheitsbehörden bleibt bestehen, wenn die individuelle Bewertung der Speicherung von Vorrats- und Fluggastdaten im dritten Modell mit berücksichtigt wird. Männer weisen weiterhin eine höhere Akzeptanz für den Datenaustausch zwischen den Sicherheitsbehörden auf. Befragte, die die Speicherung von Fluggastdaten positiv bewerten, sind auch dem Datenaustausch zwischen deutschen Sicherheitsbehörden gegenüber aufgeschlossener,

Datenaustausch innerhalb der EU

Die Ergebnisse für die Bewertung des Datenaustauschs innerhalb der EU weisen in die gleiche Richtung. Allerdings ist der Anteil der Personen, die diese Form des Datenaustauschs positiv bewerten geringer. Gleichzeitig nimmt die Gruppe der Personen mit leichten Vorbehalten zu. Die Gruppe der entschieden misstrauischen Befragten gegenüber dem Datenaustausch auf EU-Ebene bleibt mit knapp sieben Prozent jedoch recht überschaubar.

Im ersten Modell zeigt sich, dass Befragte für die das Thema Innere Sicherheit wahlentscheidende Bedeutung hat, den EU-weiten Datenaustausch eher positiv bewerten. Personen mit Vertrauen in die Arbeit verschiede-

Tabelle 2

Datenaustausch zwischen EU-Staaten

Parameter der Probit-Regressionen (0 = schlecht, 1 = gut)

	Modell		
	1: Sozdem	2: Akteure	3: Einzelmaßnahmen
Alter	0,004	0,002	0,003
Geschlecht männlich	0,102	0,018	0,076
Partner im Haushalt lebend	-0,099	-0,070	-0,127
Eigene Kinder	0,087	0,123	0,105
Städtische Wohngegend	-0,007	-0,108	-0,067
Akademischer Hintergrund	-0,033	-0,099	-0,047
Migrationshintergrund	-0,187	-0,179	-0,151
Wahlpräferenz Innere Sicherheit	0,2433*	0,191	0,093
Vertrauen in Landes-/Bundespolitik		0,240	0,201
Vertrauen in EU-Politik		0,120	0,091
Vertrauen in deutsche Gerichte		0,211	0,249
Vertrauen in EuGH		0,2837*	0,3212*
Vertrauen in Landes-/Bundespolizei		0,2974*	0,246
Vertrauen in Verfassungsschutz		0,104	0,006
Vertrauen in private Sicherheitsunternehmen		0,2933**	0,2944*
Positive Bewertung PNR in PNR ¹			0,5922***
Positive Bewertung VDS ²			0,165
Konstante	-8 629 989	-41 328 319	-7 028 494

* $p < 0,05$; ** $p < 0,01$; *** $p < 0,001$; Zahl der Befragten: 614.

1 PNR = Passenger Name Record.

2 VDS = Vorratsdatenspeicherung.

Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

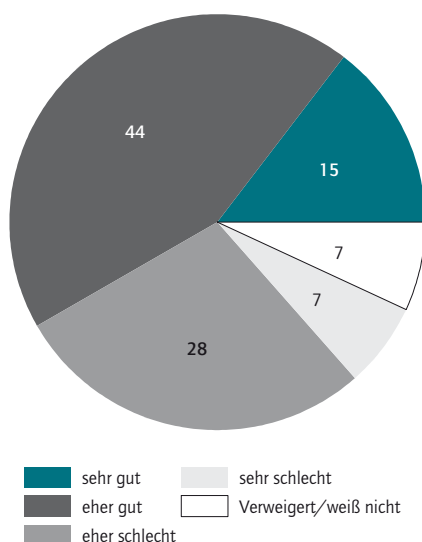
© DIW Berlin 2014

Befragte mit Vertrauen in die Arbeit des Europäischen Gerichtshofs bewerten den EU-weiten Datenaustausch positiver.

Abbildung 6

Bewertung des Datenaustauschs mit EU-Mitgliedstaaten

In Prozent (N = 1 257)



Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

© DIW Berlin 2014

Der EU-weite Datenaustausch wird von einer Mehrheit der Befragten positiv bewertet.

Tabelle 3

Datenaustausch mit Staaten außerhalb der EU

Parameter der Probit-Regressionen (0 = schlecht, 1 = gut)

	Modell		
	1: Sozdem	2: Akteure	3: Einzelmaßnahmen
Alter	0,004	0,002	0,004
Geschlecht männlich	0,174	0,118	0,169
Partner im Haushalt lebend	-0,091	-0,070	-0,118
Eigene Kinder	-0,010	0,036	0,005
Städtische Wohngegend	-0,022	-0,080	-0,036
Akademischer Hintergrund	-0,033	-0,040	-0,002
Migrationshintergrund	-0,2982*	-0,3265*	-0,3129*
Wahlpräferenz Innere Sicherheit	0,4288***	0,3786**	0,3010*
Vertrauen in Landes-/Bundespolitik		0,124	0,085
Vertrauen in EU-Politik		0,078	0,055
Vertrauen in deutsche Gerichte		0,199	0,239
Vertrauen in EuGH		0,003	0,012
Vertrauen in Landes-/Bundespolizei		-0,025	-0,083
Vertrauen in Verfassungsschutz		0,2999*	0,222
Vertrauen in private Sicherheitsunternehmen		0,2706*	0,2758*
Positive Bewertung PNR in PNR ¹			0,4721***
Positive Bewertung VDS ²			0,2696*
Konstante	-94 631 483	-42 143 838	-9453 817

* $p < 0,05$; ** $p < 0,01$; *** $p < 0,001$; Zahl der Befragten: 617.

1 PNR = Passenger Name Record.

2 VDS = Vorratsdatenspeicherung.

Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

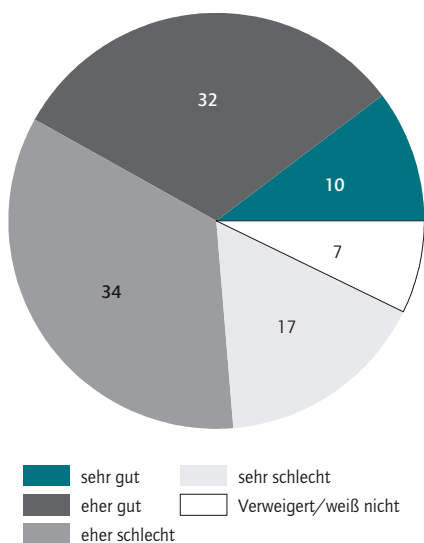
© DIW Berlin 2014

Befragte mit Migrationshintergrund bewerten den Datenaustausch mit Ländern außerhalb der EU eher kritisch.

Abbildung 7

Bewertung des Datenaustauschs mit außereuropäischen Staaten

In Prozent (N = 1 257)



Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

© DIW Berlin 2014

Der Datenaustausch mit Ländern außerhalb der EU-Grenzen wird eher kritisch bewertet.

ner Sicherheitsakteure wie Polizeibehörden auf Landes- und Bundesebene, Sicherheitsunternehmen und darüber hinaus den Europäischen Gerichtshof bewerten den EU-weiten Datenaustausch positiv (Modell 2) Der starke Einfluss des Vertrauens in private Sicherheitsunternehmen und das höchste EU-Gericht bleibt erhalten, wenn die Bewertung von Sicherheitsmaßnahmen wie die Speicherung von Vorrats- und Fluggastdaten mit einbezogen werden. Vor allem die positive Bewertung der Fluggastdatenspeicherung hängt stark positiv mit der Bewertung des Austausches von personenbezogener Daten innerhalb der EU zusammen (Tabelle 2).

Datenaustausch mit Drittländern wie den USA

Deutlich kritischer wird der Austausch personenbezogener Daten mit Staaten außerhalb der EU bewertet. Die explizite Nennung der USA als Beispielland führt dazu, dass die Interviewten gewissermaßen eine Übertragung auf die OECD-Welt vornehmen und damit an Drittstaaten mit grundsätzlich ähnlichem Rechtsverständnisdenken. Andererseits ist die USA das Land mit dem am medienwirksamsten Unstimmigkeiten bezüglich des Datenaustauschs mit der EU ausgetragen werden. Dadurch sollte den Befragten eine Bewertung des Datenaustausches mit den USA nicht völlig fremd sein.

Während der Anteil an entschiedenen Befürwortern des Datenaustausches hier auf gut zehn Prozent zurückgeht, verdoppelt sich der Anteil derer, die den Austausch *sehr kritisch* bewerten. Darüber hinaus kann auch eine Verdoppelung der Gruppe mit einer *eher kritischen* Einschätzung verzeichnet werden, so dass Vorbehalte gegenüber einem Datenaustausch außerhalb der EU als mehrheitsfähig erscheinen.

Interessanterweise spielt bei der Beurteilung des Datenaustausches mit Staaten außerhalb der Europäischen Union der Migrationshintergrund eine Rolle. Personen mit Migrationshintergrund bewerten den Datenaustausch eher negativ. Die Wahlpräferenz Innere Sicherheit spielt sogar eine noch etwas stärkere Rolle. Personen für die das Thema Innere Sicherheit eine wahlentscheidende Bedeutung hat, stimmen dem Datenaustausch eher zu (Tabelle 3). Diese Zusammenhänge sind im ersten und zweiten Modell zu beobachten¹⁹ und finden eine entsprechend Ergänzung durch den abermalig signifikanten Einfluss des Vertrauens in den Verfassungsschutz und in private Sicherheitsunternehmen. Werden die beiden Beispielmaßnahmen (Speicherung von Vorrats- und Fluggastdaten) im dritten Modell mit einbezogen, so gehen diese mit einer positiven Bewertung des Austausches personenbezogener Daten auch außerhalb der EU einher.

¹⁹ Die wichtigsten Herkunftstaaten in der Stichprobe sind Polen, Türkei und die ehemalige Sowjetunion.

Fazit

Das Vertrauen in staatliche Behörden und Kommunikationsunternehmen im Rahmen digitaler Sicherheitsmaßnahmen spielt in der Akzeptanz dieser Maßnahmen eine zentrale Rolle. Es zeigt sich allerdings eine gewisse Vertrauensdistanz, was den Datenumgang bei privaten Unternehmen (aber auch in abgeschwächter Form gegenüber staatlichen Behörden) anbetrifft. Dieser Befund gilt auch für die Bewertung des Austauschs verdachtsunabhängig gesamelter, personenbezogener Daten. Für das Vertrauen in den Datenaustausch sowohl zwischen deutschen Sicherheitsbehörden, auf EU-Ebene und mit weiteren Drittstaaten spielt das Vertrauen in diese Behörden selbst und das Vertrauen in private Sicherheitsunternehmen (die teilweise die operative Umsetzung des Datenaustausches und der Datenverknüpfung organisieren) eine zentrale Rolle. Die problematische Verquickung zwischen öffentlichen Sicherheitsbehörden und privaten Anbietern wie Sicherheits- und Kommunikationsdiensten und der erhöhte Regelungsbedarf werden insbesondere durch die sukzessive Veröffentlichung rund um Edward Snowden deutlich. Die Bedeutung des Vertrauens in private und staatliche Sicherheitsakteure überlagert meist den Einfluss einschlägiger soziodemographischer Faktoren und politischer Präferenzen wie etwa die subjektive Wichtigkeit Innerer Sicherheit für die Wahlentscheidung.

Grundsätzlich schwindet das Vertrauen in den Datenaustausch mit wachsendem Zugangskreis, wie die Bewertung des innerdeutschen und EU-weiten Datenaustauschs zeigt. Besonders augenfällig ist die deutlich kritische Einschätzung der Mehrheit der Befragten im Falle des Datenaustauschs mit Drittländern wie den USA.

Das Vertrauen in Sicherheitsbehörden und in private Dienstleister scheint demnach ein Garant für die Le-

gitimität digitaler und verdachtsunabhängiger Sicherheitsmaßnahmen zu sein. Diese Maßnahmen spielen eine immer gewichtigere Rolle im Alltagshandeln der Sicherheitsbehörden. Vergleichbaren Massendaten kommt auch eine bedeutende Funktion für die Wertschöpfung im gesamten Bereich der netzbasierten Wirtschaft zu. Sowohl der öffentliche Diskurs als auch die aktuelle Rechtsprechung legen Wert auf grundrechtschonende Umsetzungsmodalitäten und die Transparenz der einzelnen Maßnahmen.

Die von Seiten der Regierung eher zaghafte Aufarbeitung der NSA-Affäre oder das lang anhaltende Pochen auf eine Neuregelung der hoch umstrittenen Vorratsdatenspeicherung durch Vertreter deutscher Sicherheitsbehörden hat das Vertrauen in diese Behörden nicht gerade gestärkt. Hier ist ein offenerer, transparenter Umgang der Politik – und vor allem der Sicherheitsbehörden – notwendig. Für die Bevölkerung muss klar ersichtlich sein, welche Daten unbescholtener Bürger automatisiert ausgetauscht werden. Die Nutzungsvereinbarungen mit anderen Ländern sollten ebenfalls transparent gemacht werden.

Ebenso gefährden Datenskandale wie die millionenfache Entwendung von persönlichen Zugangsdaten in sozialen Netzwerken und Mailprogrammen das Vertrauen in die Sicherheit personenbezogener digitaler Daten im Netz. Damit wird auch das Vertrauen in private Anbieter von Kommunikationsdienstleistungen (genauso wie in Internetdienste wie Homebanking und Online-Shopping) gefährdet. Ein hoher Schutz der Kundendaten und Soft- und Hardwarelösungen die *privacy by design*, also den Schutz der Privatsphäre von Anfang als Geschäftsidee mitdenken, stellt daher einen Dreh- und Angelpunkt in der Weiterentwicklung und Weiterentwicklung des Internets dar.

Mathias Bug ist Wissenschaftlicher Mitarbeiter in der Abteilung Entwicklung und Sicherheit am DIW Berlin | mbug@diw.de

PUBLIC CONFIDENCE IN DIGITAL SECURITY POLICY

Abstract: Both economic and security policies increasingly rely on opportunities to use and analyze personal data. These opportunities are, however, not universally considered to be positive by the general public. This applies to digital surveillance in particular. DIW Berlin has analyzed how much trust the general public has in surveillance measures such as communications data retention or the storage of flight passenger data and to what extent this trust is affected by stakeholders involved in monitoring. DIW Berlin also studied how the public view the exchange of personal data between the German security authorities, between EU member states, and with third-party countries such as the US. To this end, it analyzed public trust based on representative data from the research

project entitled "Security in Public Space (SIRA)." The underlying survey was conducted in November and December 2011.

It revealed major differences in the acceptance of various surveillance measures. Dissemination of passenger data is seen more positively than data retention. In contrast, the general population has limited trust in companies involved in communications data retention and the storage of passenger data. In particular, their handling and protection of the data collected gets criticized. Furthermore, individuals who view the exchange of personal data positively have far more confidence in the work of the security authorities and private security companies.

JEL: H56, K14, Z18

Keywords: digitalisation, home affairs, inner security, attitudes, survey, security measures, trust, state authorities, information and communication companies



Mathias Bug ist Wissenschaftlicher Mitarbeiter in der Abteilung Entwicklung und Sicherheit am DIW Berlin

SIEBEN FRAGEN AN MATHIAS BUG

»Vorratsdatenspeicherung wird kritisch beurteilt«

1. Herr Bug, das DIW Berlin hat analysiert, welches Vertrauen digitale Überwachungsmaßnahmen in der Bevölkerung genießen. Wurden Ihre Befragungen vor oder nach den Enthüllungen von Edward Snowden durchgeführt? Die Befragung wurde Ende 2011 durchgeführt, als der Skandal rund um die NSU herauskam. Die Zusammenarbeit zwischen Polizei und Verfassungsschutzbehörden wurden zu dieser Zeit also durchaus diskutiert. Es gab aber zu dem Zeitpunkt noch nicht die ganz große Diskussion um digitale Daten, die durch die Enthüllungen von Edward Snowden ausgelöst wurde.
2. Seit langem wird über die Vorratsdatenspeicherung in Deutschland debattiert. Wie groß ist die Akzeptanz dieser Maßnahme in der deutschen Bevölkerung? Ein gutes Viertel der Befragten äußert starke Kritik an der Maßnahme und antwortet ganz entschieden mit „Das finde ich sehr schlecht.“ Ein weiteres Drittel sagt: „Das finde ich eher schlecht.“ Das ist bei einer Sicherheitsmaßnahme in Deutschland relativ überraschend. Es wurde noch die Akzeptanz von anderen Sicherheitsmaßnahmen abgefragt, und die Vorratsdatenspeicherung schnitt mit Abstand am schlechtesten ab.
3. Wo liegen die Gründe für das Misstrauen? Das mag einerseits daran liegen, dass die Vorratsdatenspeicherung so tief in die Privatsphäre eingreift und mit ihr Bewegungsmuster und soziale Netzwerke einer Person analysiert werden können. Wenn jedoch Datenspeicherung nur im Verdachtsfall mit einem richterlichen Beschluss gemacht würde, dann würde die Zustimmung sicher anders ausfallen. Dadurch, dass die Vorratsdatenspeicherung verdachtsunabhängig die gesamte Gesellschaft betrifft, findet sie in der Gesellschaft keine Unterstützung.
4. Fühlen sich die Bürger nicht sicherer durch die Vorratsdatenspeicherung? Auf unsere Frage dazu sagen lediglich sechs Prozent der Bevölkerung: „Ich fühle mich dadurch wirklich sicher.“ Weitere 27 Prozent sagen: „Ich fühle mich dadurch etwas sicherer.“ Aber immerhin zwei Drittel sagen: „Ich fühle mich eher unsicher“, oder,

„Ich fühle mich dadurch überhaupt nicht sicher.“ Wenn man diese Ergebnisse als Indikator nimmt, wirkt die Vorratsdatenspeicherung eher negativ auf das Sicherheitsgefühl der Bürger.

5. Die Vorratsdaten werden bei privaten Kommunikationsunternehmen gespeichert. Wird den privaten Unternehmen mehr oder weniger vertraut als den staatlichen Behörden? Das ist eine interessante Frage, denn Behörden und politische Vertreter haben für die Vorratsdatenspeicherung oft das Argument gebracht, dass die Speicherung ja nicht bei staatlichen Stellen, sondern bei den Kommunikationsanbietern stattfindet. Ich konnte aber feststellen, dass den Kommunikationsanbietern in Bezug auf den Umgang mit den auf Vorrat gespeicherten Daten deutlich weniger vertraut wird als den Behörden. Allerdings ist auch beim Vertrauen in die Behörden eine gewisse Distanz festzustellen.
6. Wie bewerten die Bürger die Übermittlung von Fluggastdaten? Die Fluggastdaten selbst werden von der deutschen Bevölkerung recht positiv bewertet. Eine ganz andere Frage ist, wie die Übermittlung in die USA oder andere außereuropäische Staaten bewertet wird. Die Befragten sehen es durchaus positiv, wenn die deutschen Sicherheitsbehörden Daten untereinander austauschen. Das gilt auch für den Austausch zwischen den Mitgliedsstaaten der EU. Dem Datenaustausch mit Staaten außerhalb der EU, wie zum Beispiel den USA, steht die Mehrheit der Bevölkerung distanziert gegenüber.
7. Wie könnte die Politik das Vertrauen der Bevölkerung wieder erhöhen? Es ist wichtig, mehr Transparenz an den Tag zu legen. Die Bundesregierung hat im Verlauf der Snowden-Affäre nur stückchenweise Informationen preisgegeben. Diese Salomitaktik ist auf lange Sicht keine gute Idee. Es wäre sinnvoll, transparent zu machen, welche Daten mit welchen Ländern ausgetauscht werden. Und wenn es Übereinkommen zur Datenübermittlung wie zum Beispiel mit den USA gibt, muss dann auch klar sein, wie die USA mit den Daten umgehen.

Das Gespräch führte Erich Wittenberg.



Das vollständige Interview zum Anhören finden Sie auf www.diw.de/interview

Monetarisierung der Privatsphäre: Welchen Preis haben persönliche Daten?

Von Nicola Jentzsch

Das digitale Wirtschaftsleben ist geprägt von der nahezu täglichen Angabe persönlicher Informationen zu verschiedenen Zwecken. Die Entlohnung dafür findet auf unterschiedliche Weisen statt: durch Preisreduktion, Produkt-Personalisierung oder scheinbar freie Nutzung von Dienstleistungen im Internet, beispielsweise Suchmaschinen. Das Weltwirtschaftsforum in Genf bezeichnet persönliche Informationen bereits als neue Ressource (*new asset class*). Und auf europäischer Ebene treibt man die Monetarisierung der Privatsphäre voran: So sollen Europäer künftig für ihren Verzicht auf Privatsphäre fairer entlohnt werden. Dabei wird offensichtlich jedoch ignoriert, dass es sich bei der Bewertung von persönlichen Daten durch Individuen um ein diffiziles Entscheidungsproblem handelt, bei dessen Untersuchung die ökonomische Forschung mehr oder weniger am Anfang steht. So besteht grundsätzlich die Frage, ob und inwiefern auf Geld basierende Allokationsmechanismen unverzerrte Preise für persönliche Daten erzeugen können.

Der Begriff der Monetarisierung der Privatsphäre beschreibt die Kompensation für den Verzicht auf Privatsphäre, also die Preisgabe von persönlichen Informationen gegen Bezahlung. Persönlich sind Informationen immer dann, wenn sie sich auf eine identifizierte oder identifizierbare Person beziehen.¹ Beispiele hierfür sind Kauf- und Zahlungsprofile im Online-Handel oder das Nutzungsverhalten in sozialen Netzen. Für den Tausch *Privatsphäre gegen Geld* finden sich im Wirtschaftsleben viele Beispiele, darunter Preisreduktionen durch den Einsatz von Kundenkarten, risikobasierte Bepreisung von Krediten oder Versicherungen oder die kostenlose Nutzung von Online-Angeboten.

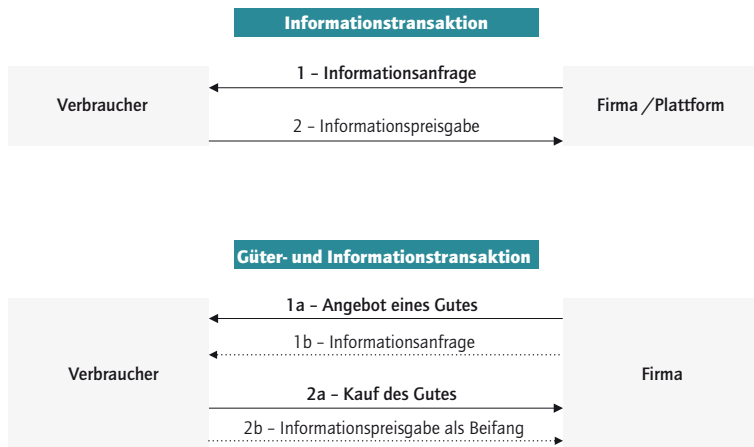
Hinter der Monetarisierung der Privatsphäre steht die Idee, dass Verbraucher gerechter für die Informationspreisgabe entlohnt werden sollen.² Nach Ansicht der Europäischen Kommission kann dies nur geschehen, wenn dem Verbraucher der ökonomische Wert seiner Daten klarer wird. Generell aber führt eine monetäre Anreizsetzung auch da einen Geldwert ein, wo vorher andere Anreize zur Informationspreisgabe bestanden, zum Beispiel Imagepflege auf Facebook, oder Zeitersparnis bei Einkaufsprogrammen.³ Die Europäische Kommission sammelt daher Vorschläge und Projekte, wie eine solche Entlohnung umgesetzt werden kann.

¹ Nach der Europäischen Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 bezeichnet der Ausdruck *personenbezogene Daten* „alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.“ Trotz dieser Definition ist der Begriff der persönlichen Information umstritten. Zum Beispiel ist unklar, ob IP-Adressen als persönliche Informationen zu werten sind.

² Dies ist das Ziel der neuen Horizon-2020-Ausschreibung der Europäischen Kommission (H2020-DS-2014-1). In ihr wird spezifiziert, dass sich persönliche Daten zu einem Wirtschaftsfaktor entwickelt haben, aber es nicht die Eigentümer der Daten sind, die damit Geld verdienen, sondern jene, die sie sammeln.

³ Gemeint sind Online-Angebote von Supermärkten und anderen Lieferanten, bei welchen der Nutzer Warenkörbe zur wiederholten Anlieferung konfigurieren kann.

Abbildung 1

Ökonomische Transaktionen mit persönlichen Daten

Quelle: Jentzsch et al. (2012).

© DIW Berlin 2014

Kombinierte Transaktionen sind komplexer als reine Informationstransaktionen.

te. Ein Vorschlag der IT-Industrie ist, dass Verbraucher ihre Daten online bei einer *Informationsbank* unterbringen oder in einem *Datentresor* einschließen können, um sie dann an Interessierte zu eigenen Bedingungen zu verkaufen. Hierzu müssen allerdings Methoden der Informationsbewertung entwickelt werden, die den Verbraucher bei genau diesen Transaktionen unterstützen.

Die Art der Entlohnung des Verbrauchers für seine Daten hängt von der Art der Transaktion ab. Im Folgenden soll daher zunächst erläutert werden, dass es sich bei Transaktionen mit persönlichen Informationen um unterschiedliche Arten des Tauschs handelt. Danach werden verschiedene Informationspreisgabe-Situationen betrachtet. Schließlich wird auf neuere experimentelle Erkenntnisse eingegangen, die zeigen, dass Menschen ihrer Privatsphäre einen positiven (ökonomischen) Wert beimessen. Zum jetzigen Zeitpunkt scheint es allerdings fraglich, ob es robuste Methoden gibt, mit denen der tatsächliche ökonomische Wert von persönlichen Daten erhoben werden kann.

Datenpreisgabe: Ein Spektrum vielfältiger Entscheidungen

Digitale Transaktionen, bei denen persönliche Daten angegeben werden, basieren auf unterschiedlichen Anreizen zur Informationsoffenlegung. So ist ein Beitrag in einem sozialen Netzwerk etwas völlig anderes als ein Einkauf bei einem Onlinehändler. Bei ersterem handelt es sich um eine reine Informationstransaktion, bei letz-

terem um eine kombinierte Transaktion aus Güter- und Informationstausch (Abbildung 1).

Bei einer reinen Informationstransaktion werden nur Informationen zwischen den Marktseiten ausgetauscht. So stellen Firmen wie Facebook und Google ihre Dienstleistungen scheinbar umsonst zur Verfügung und der Nutzer *bezahlt* mit seinem Nutzungsprofil. Dies ist ein sozialer Tausch, bei welchem zunächst kein Geld fließt. Monetäre Anreize entstehen erst auf der nachgelagerten Ebene, wenn die Informationen vom betreffenden Unternehmen beispielsweise zu Werbezwecken an Dritte verkauft werden. Für die meisten Facebook-Teilnehmer steht der Austausch untereinander im Vordergrund, also der Austausch mit sogenannten *Peers*. Für sie ist nicht entscheidend, dass sie ihren Freundeskreis einer Marketingfirma gegenüber offenbaren, die diese Informationen zu Geld macht. Der Verkauf der Daten geschieht ohne direkte Beteiligung des Nutzers, der die Daten abgegeben hat – er hat also auch kein Mitspracherecht bei der Preisbildung.

Bei Bestellungen im Internet kommt zur Informationstransaktion eine Gütertransaktion hinzu. Diese steht meist im Vordergrund und der Informationstausch wird zur Nebensache, dem sogenannten *Beifang*. Der Fokus des Verbrauchers liegt auf dem Erwerb des Gutes und die Datenpreisgabe ist nicht so offensichtlich wie bei der reinen Informationstransaktion.

Transaktionen mit persönlichen Daten unterscheiden sich auch durch den Akt der Identifikation des Handelnden. Während sich bei Facebook die Teilnehmer aktiv selbst identifizieren ist dies bei Google nicht der Fall, wo die Identifikation über die IP-Adresse des Computers stattfindet. Während eine aktive und selbst vorgenommene Identifikation in strategische Überlegungen des Entscheiders einfließen kann, ist dies bei einer verdeckten Identifizierung nicht möglich.⁴

Durch diese Anreizstrukturen ergeben sich unterschiedliche Motive und Strategien der Informationspreisgabe des Verbrauchers.

Ökonomische Incentivierung der persönlichen Informationspreisgabe

Für Verbraucher ist die ökonomische Bewertung der Offenlegung ihrer Daten oft kontextabhängig und stellt eher eine riskante Lotterie als eine nutzenmaximierende

⁴ Dies spiegelt sich auch in der Diskussion um das Identifikationspotential von Verkehrsdaten. Ein anderes Beispiel ist die biometrische Gesichtserkennung auf Facebook. Genaugenommen handelt es sich bei dieser um verdeckte Identifizierung.

Entscheidung unter vollständiger Information dar (Feri et al. 2013).⁵ Dies ist insbesondere der Fall, wenn Information als Beifang die Komplexität der Kauf- oder Nutzungsentscheidung erhöht. Dies führt oft zu einem Ignorieren der Nebentransaktion, um die Entscheidungskomplexität zu reduzieren.

Viele Entscheidungen über Informationspreisgabe sind binär: die Preisgabe kann nur akzeptiert oder abgelehnt werden. Eine binäre Entscheidung kann die Kosten der Ablehnung der Informationstransaktion erhöhen, da unter Umständen kein Vertrag ohne Akzeptanz der Nebentransaktion zu Stande kommt. Dies schränkt die Entscheidungsfreiheit ein. Ein Verbraucher hat derzeit wenig Mittel, die Konditionen des Informationsaustausches abzuändern, geschweige denn einen Preis für die Weiterverwendung der Daten zu verlangen.

Wie eingangs erwähnt, will die Europäische Kommission nun Vorschläge fördern, die es dem Verbraucher erleichtern, zu erkennen zu welchen Konditionen er seine Daten tauscht. Er soll künftig die Möglichkeit haben, bessere Konditionen in diesem Tausch zu erhalten.

Was ist der *richtige* Preis für persönliche Daten?

Eines der wichtigsten Ziele der Forschung zur Privatsphäre ist die Ermittlung eines möglichst unverfälschten Wertes persönlicher Informationen. Dieser würde theoretisch durch Angebot und Nachfrage am Markt entstehen, welcher die Wertschätzung von Individuen (als Anbieter) und die Wertschätzung der Unternehmen (als Nachfrager) der Informationen zum Ausgleich bringt. Ein solcher Marktpreis würde zu einer effizienten Preis- und Weitergabe von Informationen führen. In der Realität lassen sich aber Marktunvollkommenheiten wie Externalitäten beobachten. So muss man von vor- und nachgelagerten Märkten ausgehen. In dem vorgelagerten Markt treten Verbraucher als Informationsanbieter auf und Unternehmen als Nachfrager, die dann wiederum auf dem nachgelagerten Markt als Anbieter auftreten, um Daten an Dritte weiterzuverkaufen. Hierbei entstehen durch den Datenhandel auf dem nachgelagerten Markt Externalitäten für den Verbraucher, wenn er zum Beispiel Werbezuschriften erhält. Da der Verbraucher die Preisbildung auf diesem Markt nicht beeinflussen kann, kann er keinen hohen Preis für die Werbesprache setzen. Er wird hierfür also nicht kompensiert.

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) gibt einen Überblick über verschiedene Methoden, mit welchen der monetäre Wert von Informationen gemessen werden kann.⁶ Sie konzentriert sich hierbei größtenteils auf den nachgelagerten Markt. Eine Methode ist die Erhebung von Marktpreisen für Kredit- und Marketingprofile. Diese schwanken von wenigen US-Cents bis zu 20 bis 30 US-Dollar pro Profil. Eine zweite Methode ist die Schätzung der monetären Bewertung eines Datenprofils durch die Umrechnung der Unternehmenserträge je Datenprofil, wie beispielsweise bei Facebook-Profilen. Global würde das 4,34 US-Dollar pro Profil ergeben. Schließlich zieht die OECD auch die Schwarzmarktpreise heran, zu welchen gestohlene Datenprofile gehandelt werden; für Kreditkarteninformationen variieren die Preise von 0,85 bis 30 US-Dollar.

Diese Methoden haben zwei Schwächen: zum einen ist das Datensubjekt nicht direkt an der Preisbildung beteiligt und zum anderen erlaubt die Preisbildung auf nachgelagerten Märkten nicht unbedingt Rückschlüsse auf die Bewertung der Daten auf dem vorgelagerten Markt.

Eine Möglichkeit, den Wert von persönlichen Daten zu bestimmen, sind ökonomische Experimente. Diese konzentrieren sich auf die Angebotsseite des vorgelagerten Marktes. Wie verschiedene Experimente am DIW Berlin zeigen, liefern diese jedoch eher eine qualitative Indikation von Verbraucherverhalten bei Informationspreisgabe als reale Werte der Daten.⁷ Dies hat mehrere Gründe. Zum einen werden Experimente in Laboren durchgeführt, also in einer künstlichen Umgebung, in der Vertrauenseffekte eine Rolle spielen können. So kann es zum Beispiel sein, dass Experiment-Teilnehmer darauf vertrauen, dass ihre Daten sicher sind und sie daher freigiebiger mit ihnen umgehen als in der realen Welt.

Zum anderen ist es schwierig, einen anreizkompatiblen Mechanismus zu finden, über welchen Teilnehmer ihre Daten verkaufen können. Anreizkompatibel ist ein Mechanismus dann, wenn die Teilnehmer ihre wahre Wertschätzung offenbaren und zwar unabhängig von den Handlungen der anderen. Es zahlt sich für sie nicht aus, die Bewertung strategisch zu erhöhen oder zu reduzieren oder Fehlangaben zu machen. Mechanismen wie die Zweitpreisauktion gelten als anreizkompatibel,⁸

⁵ Feri, F., Giannetti, C., Jentzsch, N. (2013): Disclosure of Personal Information under Risk of Privacy Shocks. Working Papers WP875, Dipartimento Scienze Economiche, Università di Bologna.

⁶ OECD (2013): Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. OECD Digital Economy Papers, No. 220.

⁷ Eine Verhaltenskonstante ist, dass Personen, die in einem sozialen Vergleich schlechter abschneiden, einen höheren Preis für ihre Daten fordern als jene, die besser abschneiden.

⁸ Bei der absteigenden Zweitpreisauktion gewinnt das niedrigste Gebot, der Preis, der für das ersteigerte Gut bezahlt werden muss, entspricht dem zweitniedrigsten Gebot.

sie wurden aber für traditionelle Wirtschaftsgüter entwickelt. Bei immateriellen Gütern wie Informationen könnte die Anreizkompatibilität allerdings verschwinden, sobald Kosten der Privatsphäre existieren.

Kosten der Privatsphäre bezeichnen hierbei die Kosten der Preisgabe persönlicher Informationen. Diese können als vermehrte Anstrengung (beispielsweise Datenangabe in Formularen) auftreten, als monetäre Kosten (zum Beispiel Preisdiskriminierung), psychologische Kosten (wie Reputations- oder Imageschaden) oder als Kombination mehrerer dieser Faktoren.

Drittens besteht das Problem, dass Teilnehmer ihre persönliche und private Information allein durch ihre Teilnahme an einem Mechanismus offenbaren können. Dies bedeutet, dass die Teilnahme an einem Tausch bereits ein Signal ist, noch bevor die eigentliche Information preisgegeben wurde. Zum Beispiel könnten Teilnehmer nur dann einen Anreiz haben, ihre Daten zu verkaufen, wenn sie im sozialen Vergleich gut abschneiden. Wie Hermalin und Katz (2006) theoretisch zeigen, führt eine Preisgabe von Informationen durch alle „guten Typen“ automatisch zur Offenlegung der „schlechten Typen.“⁹ Dies ist insbesondere der Fall, wenn die Teilnehmer identifiziert sind.

Das Problem der Preisgabe durch Teilnahme ist auch Gegenstand der Forschung zu neueren Algorithmen, die mit dem Begriff der *differential privacy* bezeichnet werden.¹⁰ Hierbei geht es um die Entwicklung von Verfahren, welche keine Rückschlüsse auf Teilnahme oder Nicht-Teilnahme erlauben.

Privatsphären-Kosten sind also wichtig, weil sie zu Selbstselektionsdynamiken führen können. Personen, die ihre Privatsphäre nicht schätzen, sollten keine positiven Kosten aufweisen, wenn sie persönliche Daten offenlegen.

Einsichten aus der experimentellen Wirtschaftsforschung

In Zusammenarbeit mit akademischen Partnern (University of Cambridge, University of Bologna und Royal Holloway University of London) hat das DIW Berlin seit 2012 eine Reihe von ökonomischen Experimenten zur Privatsphäre in Labor und Feld durchgeführt, an

Tabelle 1

Überblick über die Experimente

	Implementierte Transaktion	Entscheidungsmodus
Feri et al. (2013)	Güter- und Informationstransaktion	Binär: 2 Euro
Jentzsch (2014)	Informationstransaktion	Individuelle Preissetzung

Quelle: Darstellung des DIW Berlin.

© DIW Berlin 2014

welchen mehr als 1 500 Personen teilnahmen.¹¹ Im Folgenden werden lediglich skizzenhaft die Kernresultate zweier Experimente berichtet, da sich diese noch in der Auswertung befinden. Es handelte sich bei den Experimenten um unterschiedliche Entscheidungssituationen und Transaktionen, was den Vergleich der Resultate zugegebenermaßen erschwert (Tabelle 1).

Im ersten Experiment (Feri et al. 2013) handelte es sich bei den persönlichen Daten um die Ergebnisse eines zuvor im Labor vollzogenen Tests, bestehend aus 22 Fragen eines Intelligenztests, die innerhalb von 17 Minuten zu beantworten waren. Das Testresultat wurde den einzelnen Teilnehmern vertraulich mitgeteilt. Die Daten implizierten einen sozialen Vergleich, bei dem manche schlechter abschnitten, da sie ein Ergebnis unter dem Median der Gruppe erzielt hatten. Das Testresultat konnten die Teilnehmer zusammen mit ihrem Vor- und Zunamen gegen eine Preisreduktion von zwei Euro für einen Einkaufsgutschein im Wert von fünf Euro preisgeben. Der Gutschein konnte für Güter wie Bücher oder DVDs, also physische Güter, eingelöst werden. Unter gewissen Umständen konnte es in diesem Experiment passieren, dass die Daten an alle im Labor weitergegeben wurden (für genauere Ausführungen zum Experimentablauf siehe Feri et al. 2013).

In einem zweiten Experiment (Jentzsch 2014) wurde anhand einer umgekehrten Zweitpreisauktion untersucht, ob Teilnehmern Kosten der Privatsphäre entstehen, und zwar in Form von Reputationskosten.¹² Hier konnten Teilnehmer ihre Testresultate auktionieren, wobei der Test derselbe war wie in Feri et al. (2013).

⁹ Hermalin, B., Katz, M. (2006): Privacy, property rights and efficiency: The economics of privacy as secrecy. *Quantitative Marketing and Economics*, 4(3), 209–239.

¹⁰ Kearns, M., Pai Malleh, M., Roth, A., Ullman, J. (2014): Mechanism Design in Large Games: Incentives and Privacy. *American Economic Review*, 104(5), 431–435; Xiao, D. (2013): Is privacy compatible with truthfulness? www.liafa.univ-paris-diderot.fr/~dxiao/docs/private.pdf.

¹¹ Finanziert wurden diese Experimente durch ein Projekt der Europäischen Agentur für Netz- und Informationssicherheit und einen Google Research Award, den die Autorin erhalten hat.

¹² Jentzsch, N. (2014): Auctioning Privacy-Sensitive Goods: A Note on Incentive-Compatibility. In: Preneel, B., Ikonomou, D. (Hrsg.): *Privacy Technologies and Policy 2014*, 133–142.

Tabelle 2

Zusammenhang von Testresultat und Verkauf

	Verkauf Testresultat		Insgesamt
	Nein	Ja	
Nicht unter Median	45	60	105
Unter Median	57	26	83
Summe	102	86	188

Pearson $\chi^2 = 12,4496$; $Pr = 0,000$.

Quellen: Feri et al. (2013); Berechnungen des DIW Berlin.

© DIW Berlin 2014

Teilnehmer, die nicht unter dem Median liegen, haben eine höhere Wahrscheinlichkeit ihr Testresultat zu verkaufen.

Festzuhalten ist, dass den Teilnehmer in keinem der Experimente die Gelegenheit geboten wurde, Fehlangaben zu machen, das heißt ihre Daten zu manipulieren, um so mögliche negative Konsequenzen der Informationspreisgabe abzuschwächen.

Das erste Experiment zeigte, dass Teilnehmer, die schlechter im Test abschnitten, also ein Testergebnis unter dem Median der Gruppe erzielt hatten, ihre Informationen signifikant weniger häufig preisgaben als jene, mit besseren Testergebnissen (Tabelle 2).¹³

Diese Sensibilität zeigte sich auch im Auktionsexperiment. Teilnehmer mit guten Testergebnissen verkauften ihre Daten eher und für einen geringeren Preis (durchschnittlich für 3,12 Euro) als Personen mit relativ schlechten Testresultaten, die entweder nicht verkaufen wollten oder nur für einen vergleichsweise hohen Preis (durchschnittlich für 5,97 Euro). So kann also auch der verlangte Preis einen Rückschluss auf das Testergebnis zulassen. Das Streudiagramm (Abbildung 2) zeigt die Verteilung der Gebote je Testresultat in dem Experiment.

In diesem Experiment war die absteigende Zweitpreisauktion¹⁴ – anders als für physische Güter – kein anreizkompatibler Mechanismus, da es Kosten der Privatsphäre für manche Teilnehmer gab. So ist die Wahrscheinlichkeit der Teilnahme an der Auktion geringer für Personen mit einem schlechteren Testergebnis. Würden diese Kosten durch Anonymisierung auf Null gesetzt, dann wäre diese Art der Auktion anreizkompatibel. Für manche Personen sind die Kosten aber so hoch, dass sie gar nicht an einem Tausch teilnehmen

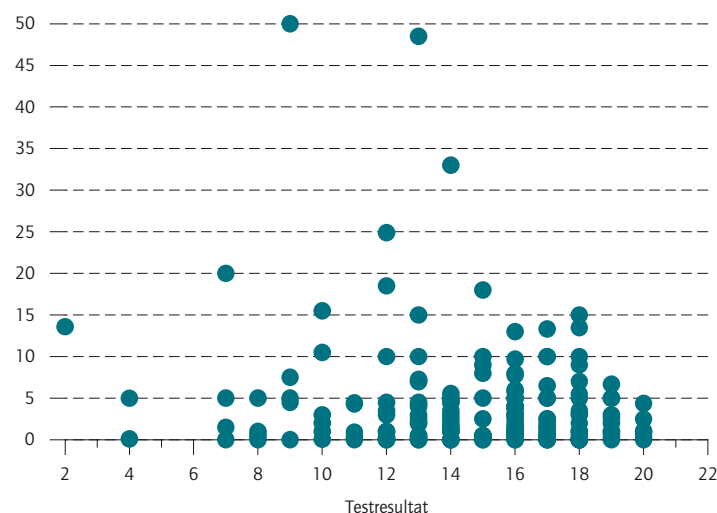
¹³ Ergebnisse der weiteren ökonomischen Analysen werden in Feri et al. (2013) diskutiert.

¹⁴ Diese wurde in dem Experiment als Beschaffungsauktion implementiert, bei der die Daten den Teilnehmern abgekauft wurden.

Abbildung 2

Gebot je Testresultat im Auktionsexperiment

In Euro



Quelle: Jentzsch (2014).

© DIW Berlin 2014

Gebote von Teilnehmern mit besseren Testergebnissen streuen weniger stark als Gebote von Teilnehmern mit schlechteren Ergebnissen.

wollen, auch wenn sie sich monetär gesehen besser stellen könnten. Dies wirkt sich wie ein Selbstselektionsmechanismus aus, da nur bestimmte Typen an dem Tausch teilnehmen.

Insgesamt kann also festgestellt werden, dass eine absteigende Zweitpreisauktion nicht notwendigerweise anreizkompatibel ist, wenn die Teilnehmer sicher identifiziert werden, nicht lügen können, über Informationen verfügen, die sensibel sind und ein Risiko der Transaktion besteht.

Schlussfolgerungen

Aus der intensiven Nutzung von Google und Facebook durch Millionen von Menschen wird oft geschlossen, dass diesen Nutzern ihre Privatsphäre nichts wert ist. Diese Verallgemeinerung ist nicht zulässig, da Transaktionen mit persönlicher Information auf sehr unterschiedlichen Anreizstrukturen basieren. So ist eine freiwillige Angabe selbstselektierter Information unter Freunden etwas völlig anderes als Einkäufe im Internet mit Kreditkarte. Im Augenblick befördert die Europäische Union Vorschläge zur Monetarisierung persönlicher Daten. Dahinter steht die Idee, dass Verbraucher, sobald ihnen der ökonomische Wert ihrer Daten bewusst wird, diese entweder

besser schützen oder nur gegen eine gerechtere Entlohnung preisgeben. Dies ist jedoch schwer umzusetzen, denn die Forschung zeigt, wie schwierig es ist, einen unverfälschten Wert persönlicher Informationen über einen anreizkompatiblen Mechanismus zu generieren. Während ökonomische Experimente zeigen, dass Personen ihren persönlichen Informationen einen Wert zumessen, wenn diese sensibel sind, gibt es im Moment jedoch keine robusten Methoden, um deren *wahren Wert* zu ermitteln. Vor diesem Hintergrund muss auch gefragt werden, was eine angemessene Entlohnung der Informationspreisgabe ist, wenn der Wert der Information unsicher ist, die Präferenzen kontextbezogen und sogar die

Definition des Begriffs „persönliche Information“ strittig ist. So gehen die Überlegungen der Europäischen Kommission zwar in die richtige Richtung, begründet durch die positive Wertschätzung mancher Personen an ihren Daten. Aber es gibt eine Reihe von wichtigen Fragen, die offen bleiben. So können über das Signal der Marktteilnahme Selektionsprozesse in Gang gesetzt werden, die besser untersucht werden müssen. Zweitens ist unklar, welche Informationen gehandelt werden, und schlussendlich bleibt offen, wie die Märkte – wenn sie etabliert würden – tatsächlich funktionieren werden. Schließlich sind persönliche Daten ein Wirtschaftsgut, das mit der zunehmenden Digitalisierung der Wirtschaft immer wichtiger wird.

Nicola Jentzsch ist Wissenschaftliche Mitarbeiterin in der Abteilung Wettbewerb und Verbraucher am DIW Berlin | njentzsch@diw.de

MONETIZING PRIVACY: THE VALUE OF PERSONAL DATA

Abstract: In today's digital economy individuals need to constantly provide personal information for different purposes. The compensation for information disclosure occurs through various ways such as price reductions, product personalization, or the apparently free use of Internet services such as search engines. The World Economic Forum in Geneva has already designated personal information as a new asset class. At the European level, too, the monetization of privacy is being promoted: The European Commis-

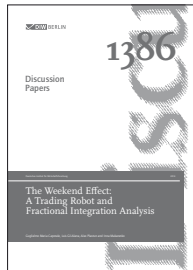
sion holds that Europeans should be more fairly remunerated for relinquishing their privacy. However, there seems to be some ignorance of the problem that the valuation of personal data by individuals is a complex decision and that economic research is more or less still in its infancy when it comes to analyzing this problem. The fundamental question here is whether and to what extent monetary allocation mechanisms can generate unbiased prices for personal data.

JEL: D43, L14, O30

Keywords: Privacy, data protection

Discussion Papers Nr. 1386

2013 | Guglielmo Maria Caporale, Luis Gil-Alana, Alex Plastun and Inna Makarenko



The Weekend Effect: A Trading Robot and Fractional Integration Analysis

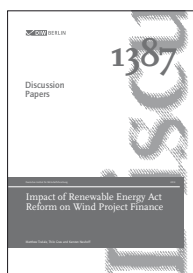
This paper provides some new empirical evidence on the weekend effect, one of the most recognized anomalies in financial markets. Two different methods are used: (i) a trading robot approach to examine whether or not there is such an anomaly giving rise to exploitable profit opportunities by replicating the actions of traders; (ii) a fractional integration technique for the estimation of the (fractional) integration parameter d . The results suggest that trading strategies aimed at exploiting the weekend effect can generate extra profits but only in a minority of cases in the gold and stock markets, whilst they appear to be profitable in most cases in the FOREX. Further, the lowest orders of integration are generally found on Mondays, which can be seen as additional evidence for a weekend effect.

www.diw.de/publikationen/diskussionspapiere



Discussion Papers Nr. 1387

2013 | Matthew Tisdale, Thilo Grau and Karsten Neuhoff



Impact of Renewable Energy Act Reform on Wind Project Finance

The 2014 reform of the German Renewable Energy Act introduces a mandatory shift from a fixed feed-in tariff to a floating premium system. This is envisaged to create additional incentives for project developers, but also impacts revenues and costs for new investments in wind generation. Thus uncertainties for example about balancing costs and the impact of the location specific generation profile on the average price received by a wind project are allocated to renewable projects. We first estimate the magnitude of the impacts on wind projects based on historic and cross-country comparison. We then apply a cash-flow model for project finance to illustrate to what extent the impact of the uncertainty for project investors reduces the scale of debt that can be accessed by projects and thus increases financing costs.

www.diw.de/publikationen/diskussionspapiere





Marcel Fratzscher ist Präsident im Vorstand am DIW Berlin
Der Beitrag gibt die Meinung des Autors wieder.

Deutschlands Schwäche ist selbst verschuldet

Die deutsche Wirtschaft ist im zweiten Quartal überraschend geschrumpft. Die Versuchung ist groß, den Russlandkonflikt dafür verantwortlich zu machen. Deutsche Exporte nach Russland und Osteuropa sind in den vergangenen Monaten gesunken. Der Umfang dieser Exporte ist jedoch, bezogen auf die gesamte Wirtschaft, vergleichsweise klein. Ihr Rückgang allein kann die wirtschaftliche Schwäche Deutschlands nicht erklären, zumal sich die Exporte in andere Regionen gut entwickelt haben. Es ist vielmehr eine starke Unsicherheit, die deutsche Unternehmen in ihren Investitionen hemmt. Die deutsche Investitionsquote gehört schon seit langem zu der niedrigsten aller Industrieländer. Die hohe Unsicherheit ist jedoch nicht durch den Russlandkonflikt verursacht worden. Hinter ihr steckt eine ganze Reihe weiterer Faktoren, die ihren Ursprung in Deutschland und der Euro-Zone haben.

So ist in den vergangenen Monaten klar geworden, dass die europäische Krise bei Weitem nicht bewältigt ist. Italiens Wirtschaft schrumpft bereits seit Anfang des Jahres, der Fortschritt bei wichtigen Reformen in Frankreich und anderen Ländern ist nach wie vor gering, und der Kollaps der portugiesischen Bank Espírito Santo verdeutlicht, dass einige Banken noch immer große Risiken für die Wirtschaft darstellen. Keine dieser Unsicherheiten wird sich schnell legen. Vor allem der Banken-Stresstest in der zweiten Jahreshälfte bedeutet weiterhin Unsicherheit.

Die Schwäche der deutschen Wirtschaft ist zu einem erheblichen Teil durch die enttäuschende Entwicklung der Euro-Zone zu erklären. Auch wenn die deutsche Perspektive gerne auf die globale Wirtschaft gerichtet ist, so sollte uns bewusst sein, wie stark die deutsche Wirtschaft von der der Euro-Zone abhängig ist. Deutschland wird nicht nachhaltig wachsen können ohne ein gesundes Wirtschaftswachstum in der gesamten Euro-Zone.

Auch die einheimischen Rahmenbedingungen für die deutsche Wirtschaft bergen nach wie vor viele Unsicher-

heiten – sei es bei den zukünftigen Energiekosten, den steuerlichen Belastungen, der Infrastruktur oder der Verfügbarkeit von Fachkräften. Die Inflation in Deutschland ist überraschend stark gefallen und bedeutet eine Planungsunsicherheit für zahlreiche, wenn auch nicht alle Branchen.

Wer eine schnelle Erholung der deutschen Wirtschaft im dritten Quartal erwartet, wird wohl enttäuscht werden. Die Mehrzahl der Indikatoren in den vergangenen drei Monaten – bei der Industrieproduktion, den Aufträgen für Unternehmen, als auch Erwartungsindikatoren – deuten darauf hin, dass die deutsche Wirtschaft wahrscheinlich auch im dritten Quartal schrumpfen wird. Technisch gesehen dürfte die deutsche Wirtschaft damit in eine Rezession abgleiten. Selbst wenn das vierte Quartal wieder stärkere Wachstumszahlen zeigen sollte, so wird die ursprüngliche Wachstumsprognose von 1,8 bis 2 Prozent für dieses Jahr unhaltbar sein. Die Wirtschaft wird wohl wenig mehr als ein Prozent zulegen können.

Eine so deutliche Revision erfordert auch eine Anpassung der Politik, da Steuereinnahmen und die Einzahlungen in die Sozialkassen geringer ausfallen werden. Damit könnte die fiskalische Konsolidierung gefährdet sein, und die Bundesregierung steht vor der Frage, wie sie diesen Ausfall kompensieren kann. Die schwachen Wachstumszahlen sollten ein Weckruf für die Wirtschaftspolitik in Deutschland und in Europa sein. Wir brauchen dringend einen Wachstumsimpuls, der die Binnennachfrage und vor allem die privaten Investitionen stärkt. Dazu müssen die Struktur-reformen auf der Angebotsseite entschieden umgesetzt werden, und die wirtschaftspolitische Unsicherheit – im Bereich der Banken, der Strukturreformen und anderer Standortfaktoren – muss gesenkt werden. Aber es ist auch eine aktive Investitionsagenda notwendig. Sie muss den Wettbewerb verbessern, den europäischen Binnenmarkt vollenden und die Finanzierungsbedingungen für Unternehmen in Europa erleichtern.