Bug, Mathias

Article

Bevölkerungsvertrauen in digitalisierte Sicherheitspolitik

DIW Wochenbericht

Provided in Cooperation with:
German Institute for Economic Research (DIW Berlin)

Suggested Citation: Bug, Mathias (2014) : Bevölkerungsvertrauen in digitalisierte Sicherheitspolitik, DIW Wochenbericht, ISSN 1860-8787, Deutsches Institut für Wirtschaftsforschung (DIW), Berlin, Vol. 81, Iss. 34, pp. 783-791

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 Infrastruktur[2] 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 2014[5] und schließlich aktuell durch vermeintlich russische Hacker[6] 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.digital-ist.de/index.php?id=201, abgerufen am 5. August 2014.

4 Institut für Demoskopie Allensbach (2013): Wirkungslose Aufregung. www.ifd-allensbach.de/uploads/tx_reportsndocs/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%C2%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.

Folgende Fragewortlaute sind für diesen Wochenbericht relevant:

Beurteilung Vorratsdatenspeicherung (C 5.1, C 5.2)

C 5.1: Wie gut oder wie schlecht finden Sie diese Maßnahme, sehr gut, eher gut, eher schlecht, sehr schlecht?

C 5.2: 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 (C 51 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?

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.

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 Bundesverfassungsgerichts[7] und des Europäischen Gerichtshofs[8] weisen in diese Richtung.[9]

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,

7 BVerfG, 1 BvR 256/08 vom 2. März 2010, Absatz-Nr. (1 – 345), www.bverfg.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.

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 Datenaustausch 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).

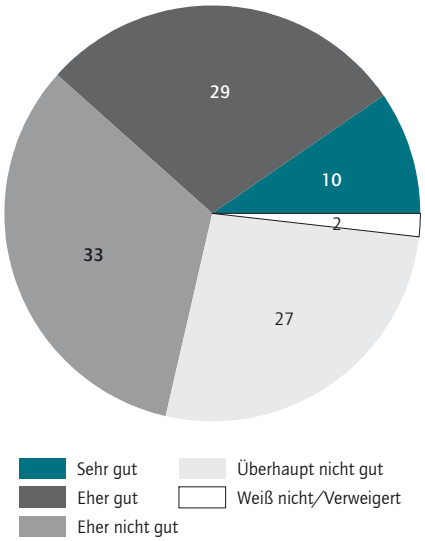
Neben der geringen Akzeptanz trägt die Vorratsdatenspeicherung zudem nur bei wenigen Befragten zu einem erhöhten Sicherheitsgefühl bei. Das Vertrauen in den Datenumgang fällt dabei ebenso kritisch aus, hängt aber stark von den beteiligten Akteuren ab. Behörden genießen gegenüber privaten Kommunikationsunternehmen 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 entschiede-

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., Pfaff-Rüdiger, 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)

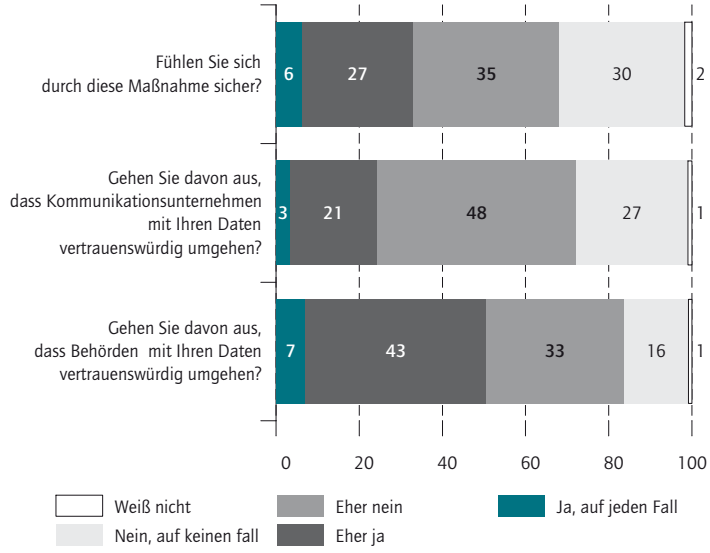


Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

Nur wenige Befragte befürworten die Vorratsdatenspeicherung uneingeschränkt.

Abbildung 2

Vorratsdatenspeicherung – Vertrauen in Akteure und Sicherheitsgefühl
In Prozent[1]



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

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

Vorratsdatenspeicherung steigert nur bei wenigen Befragten das Sicherheitsgefühl.

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 Schiffreise, 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

12 Weiter führende Analyse bei Bug, M., Wagner, K. (2014): Der digitalisierte Passagier. In: Humer, S. (Hrsg.): Digitale Wissenschaft. Im Erscheinen.

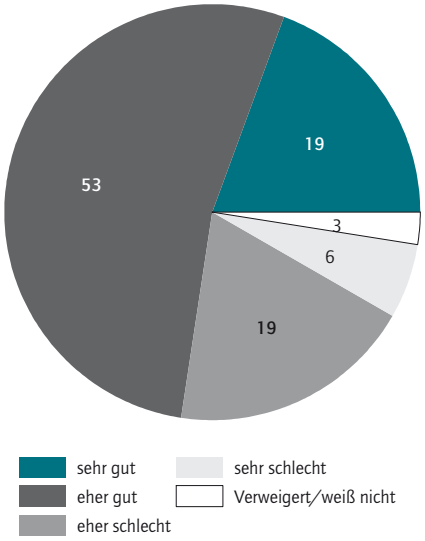
13 Busch, A. (2012): Die Regulierung transatlantischer Datenströme: zwischen Diktat und Blockade? In: Hofmann J, Busch A. (Hrsg.): Politik und die Regulierung von Information. PVS Sonderheft 46, Baden-Baden, 408–440.

14 Europäische Kommission (2013): TARGETED CALL FOR PROPOSALS. Law enforcement cooperation through measures to set up Passenger Information Units in Member States for the collection, processing, analysis and exchange of Passenger Name Record (PNR), data. ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/prevention-of-and-fight-against-crime/calls/call-2012/pnr-targeted-call/docs/pnr_call_for_proposals_2012_final_en.pdf, abgerufen am 5. August 2014.

15 Krempl, S., Kannenberg, A. (4. Juni 2014): Russland will europäische Flugpassagierdaten 3,5 Jahre lang speichern. www.heise.de/newsticker/meldung/Russland-will-europaeische-Flugpassagierdaten-3-5-Jahre-lang-speichern-2216276.html, abgerufen am 5. August 2014.

Abbildung 3

Beurteilung der Fluggastdatenspeicherung
In Prozent (N = 799)

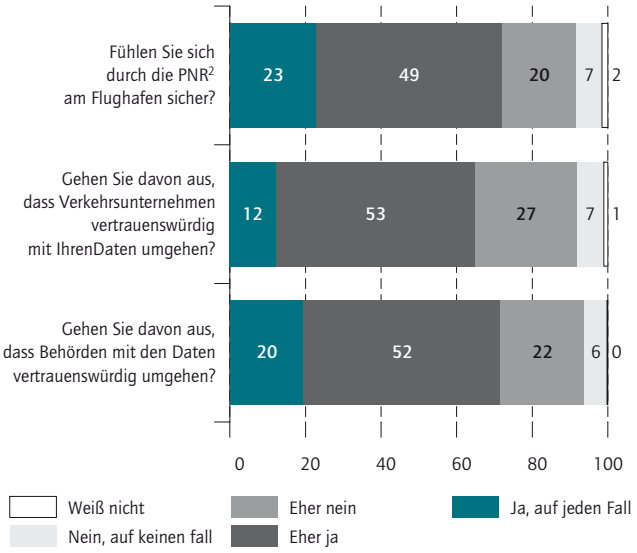


Quelle: Bug/Münch/Röllgen (2012): SIRA Koppeldatensatz, bisher unveröffentlicht.

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

Abbildung 4

Fluggastdaten – Vertrauen in Akteure und Sicherheitsgefühl
In Prozent[1]



1 Nur Flugpassagiere mit Vorwissen zur Maßnahme, N = 378.
2 Passenger Name Record.

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

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

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 Bereichen 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

16 Bug, M. (2014 b), a. a. O., 60.

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 gehören 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.

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

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

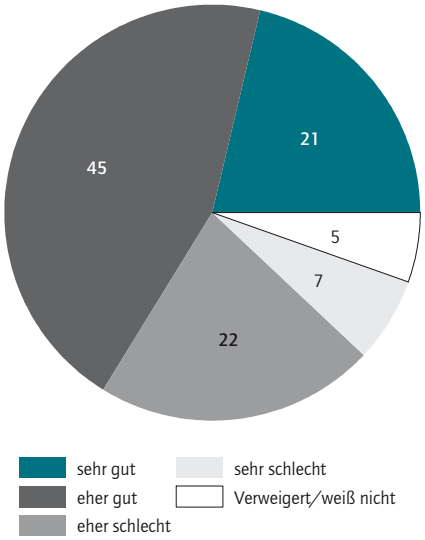
Männliche Befragte weisen eine höhere Akzeptanz für den Datenaustausch zwischen deutschen Sicherheitsbehörden auf. Gleiches gilt für Personen, die dem Thema Innere Sicherheit eine große Bedeutung beimessen (Tabelle 1).

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.

Abbildung 5

Bewertung des Datenaustauschs zwischen deutschen Sicherheitsbehörden
In Prozent (N = 1 257)



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

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

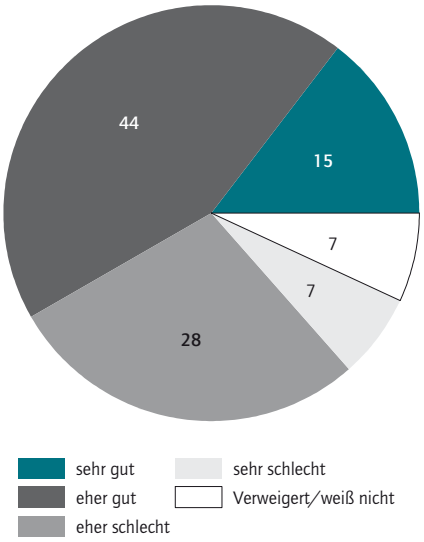
** p < 0,05; ** p < 0,01; *** p < 0,001; Zahl der Befragten: 614.*
1 PNR = Passenger Name Record.
2 VDS = Vorratsdatenspeicherung.

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

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.

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	−9 453 817

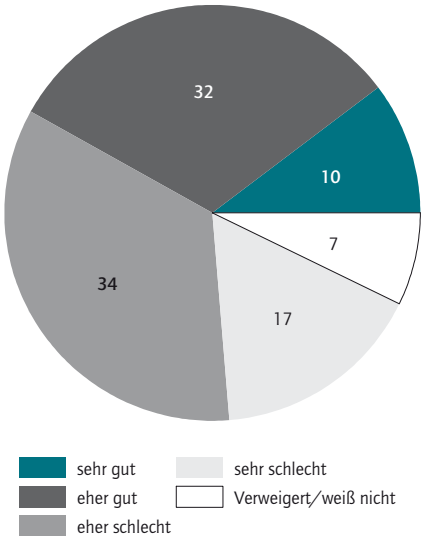
** p < 0,05; ** p < 0,01; *** p < 0,001; Zahl der Befragten: 617.*
1 PNR = Passenger Name Record.
2 VDS = Vorratsdatenspeicherung.

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

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.

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 beobachten[19] 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 Herkunftsstaaten 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 gesammelter, 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 Legitimität 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 Weiternutzung 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

DIW BERLIN

DIW Berlin — Deutsches Institut für Wirtschaftsforschung e. V.
Mohrenstraße 58, 10117 Berlin
T +49 30 897 89 -0
F +49 30 897 89 -200
www.diw.de
81. Jahrgang

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. 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