

LARS BRETTHAUER

WIDER DIE GENERALÜBERWACHUNG DER TELEKOMMUNIKATION

**DER KAMPF GEGEN DIE VORRATSDATENSPEICHERUNG
GEHT IN EINE WEITERE RUNDE**

Als politisches Thema hat die Vorratsdatenspeicherung in den letzten Jahren für viel öffentliches Aufsehen gesorgt. Wie zu erwarten war, hat die Große Koalition trotz zahlreicher Proteste das umstrittene «Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen» und damit auch die Wiedereinführung der Vorratsdatenspeicherung Ende vergangenen Jahres durchgesetzt. Aus konservativer Perspektive geht es bei dem Konflikt um die Frage, wie mit einer staatlichen Generalüberwachung der Bevölkerung die «kollektive Sicherheit» und vor allem der Schutz vor terroristischen Angriffen gestärkt werden kann. Dem steht aber eine Grundsatzdebatte über demokratische Kernprinzipien, Bürgerrechte und eine sich verändernde staatliche Überwachungs politik gegenüber, die von der Linken dringend weitergeführt werden sollte.

«Was bleibt, ist die Suche nach MissetreiterInnen, die der Auffassung sind, dass die zivile Gesellschaft nicht nur ein hochrangiges Gut darstellt, sondern auch in härteren Zeiten die weitere Demokratisierung der einzig vernünftige Weg ist.»¹

Bei der Vorratsdatenspeicherung handelt es sich um die Speicherung von Verkehrsdaten auf Vorrat durch die Telekommunikationsunternehmen, damit diese bei Bedarf von den Sicherheitsbehörden (Polizei, Verfassungsschutz und Nachrichtendiensten) abgerufen und genutzt werden können. Verkehrsdaten sind sogenannte Metadaten, die Auskunft über Kommunikationsvorgänge geben, das heißt darüber, wer, mit wem, wann, von wo und unter welchen Bedingungen kommuniziert hat. Mittels dieser Informationen können soziale Profile von Menschen erstellt werden, die tief greifende Einblicke erlauben in deren individuelle Kontakte, Netzwerke, Interessen, Aufenthaltsorte etc., was sie besonders interessant für jene macht, die ein sicherheitspolitisches, aber auch geschäftliches Interesse an Vorlieben, Gewohnheiten und Verbindungen bestimmter Individuen und Personenkreise haben. Zugleich stellt die Erfassung und Nutzung solcher Daten einen massiven Eingriff in die Persönlichkeitsrechte dar. Im Fall der Vorratsdatenspeicherung wird der damit verbundene Konflikt auf die Spitze getrieben: Beabsichtigt ist, den Zugriff der Sicherheitsbehörden auf die Verkehrsdaten der *gesamten Bevölkerung* auszuweiten, womit eine Generalüberwachung möglich würde. Dabei ist ge-

plant, den zeitlichen Rahmen, in dem dieser Zugriff möglich wäre, gesetzlich festzuschreiben.

DER KONFLIKT UM DIE (WIEDER-)EINFÜHRUNG DER VORRATSDATENSPEICHERUNG

Nachdem ein erster Vorstoß zur Einführung von Mindestfristen für die Speicherung von Telekommunikationsdaten 1996 im Bundestag gescheitert war, erhielt die Debatte nach den Terroranschlägen vom 11. September 2001 eine ganz neue Brisanz. Die damalige rot-grüne Bundesregierung erlaubte den Sicherheitsbehörden trotz massiver Proteste von Bürgerrechtsorganisationen den Zugriff auf jene Verkehrsdaten, die Telekommunikationsprovider für die Rechnungslegung speichern. Die Forderung, diese Unternehmen grundsätzlich zur Speicherung solcher Daten zu verpflichten, wurde wenige Jahre darauf virulent, als in Reaktion auf die Anschläge von Madrid (2004) und London (2005) die Forderung auftauchte, die Vorratsdatenspeicherung in ganz Europa verbindlich zu machen. Damals avancierte sie zu einer zentralen politischen Maßnahme im «Kampf gegen den internationalen Terrorismus». Im März 2006 verabschiedete das Europäische Parlament mit deutlicher Mehrheit schließlich eine Richtlinie zur Vorratsdatenspeicherung, die alle EU-Mitgliedstaaten dazu verpflichtete, bis 2007 die gesetzlichen Grundlagen zu schaffen, um eine solche einzuführen. Als Speicherfrist wurde eine Spanne von sechs bis 24 Monaten vorgegeben.

Die EU-Richtlinie von 2006 war von Anfang an umstritten. Ende 2007 verabschiedete der Bundestag jedoch das erste Vorratsdatenspeicherungsgesetz, das eine sechsmonatige Speicherung der Daten vorsah und bis 2010 Bestand hatte. In diesem Jahr erklärte das deutsche Bundesverfassungsgericht die deutschen Vorschriften zur Vorratsdatenspeicherung aus primär datenschutzrechtlichen Gründen für verfassungswidrig und daher ungültig. In den folgenden Jahren weigerte sich die damals amtierende Bundesjustizministerin Sabine Leutheusser-Schnarrenberger von der FDP wegen grundrechtlicher Bedenken, ein neues Gesetz zu verabschieden. Diese Vorbehalte wurden 2014 durch ein Urteil des Europäischen Gerichtshofs bestätigt, das auch die europäische Richtlinie zur Vorratsdatenspeicherung einkassierte. Begründet wurde dies mit der hohen Aussagekraft von Verkehrsdaten: «Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder einem anderen Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Person und das soziale Umfeld, in dem sie verkehren.»²

Trotz dieser scharfen Kritik des Europäischen Gerichtshofes begann in Deutschland unmittelbar nach den Terroranschlägen in Paris im Januar 2015 in der schwarz-roten Regierung erneut eine Debatte um die Wiedereinführung der Vorratsdatenspeicherung. Treibend war dabei zum einen die CDU/CSU-Fraktion mit Bundesinnenminister Thomas de Maizère, zum anderen SPD-Parteichef Sigmar Gabriel und – ihm folgend – Bundesjustizminister Heiko Maas. Maas legte im April 2015 Leitlinien für eine deutsche Regelung zur Vorratsdatenspeicherung vor, trotz scharfer Protesten beschloss dann die Große Koalition im Oktober 2015 eine zweite «Vorratsdatenspeicherung light», die eine Speicherung von Verbindungsdaten für zehn Wochen und von Standortdaten für Mobiltelefone (Telefonate, SMS, mobiles Internet) für vier Wochen vorsieht. Das entsprechende Gesetz trat im Dezember 2015 in Kraft, die darin enthaltenen Vorgaben mussten von den Telekommunikationsunternehmen jedoch nicht sofort umgesetzt werden. Sie haben 18 Monate Zeit dafür.³

Die Geschichte der Vorratsdatenspeicherung in Deutschland ist nicht ohne die Interventionen einer überaus aktiven Bürgerrechtsbewegung zu verstehen, die sich mit einer Vielzahl von politischen Aktionen und auch juristischen Klagen und Petitionen gegen die Vorratsdatenspeicherung gewehrt hat. Als prominentestes Beispiel ist hier der außerparlamentarische Arbeitskreis Vorratsdatenspeicherung zu nennen, ein Bündnis aus Aktiven der digitalen Bürgerrechtsbewegung, VertreterInnen von etablierteren Organisationen wie Berufsverbänden von JournalistInnen und ÄrztInnen, Beratungseinrichtungen und Hackerorganisationen wie dem Chaos Computer Club. Das Bündnis war bereits anlässlich der Verabschiedung der EU-Richtlinie aktiv und initiierte zusammen mit anderen Demonstrationen und Protestbriefe an die Mitglieder des Europäischen Parlaments. Es begleitete später die Gesetzgebungsverfahren in Deutschland mit ausführlichen juristischen und politischen Stellungnahmen und baute mit anderen eine breite kritische Gegenöffentlichkeit zum Thema auf. In Reaktion auf die Verabschiedung des ersten Gesetzes in Deutschland kam es 2007 zu einer der größten Verfassungsbeschwerden (im Namen von fast 35.000 BürgerInnen) in der bundesdeutschen Geschichte. Auf den

seit 2006 jährlich stattfindenden «Freiheit statt Angst»-Demonstration geht es längst nicht mehr nur um die Gefahren der Vorratsdatenspeicherung, vielmehr werden hier auch viele andere Themen, die mit der fortschreitenden Digitalisierung zusammenhängen, aufgegriffen, wie etwa die Einführung einer elektronischen Gesundheitskarte oder eines biometrischen Personalausweises.

Diese vielfältigen Proteste sind von keiner grundsätzlichen Ablehnung des digitalen Wandels geprägt, sondern vielmehr von einer eher deutlich technikaffinen Haltung. Das heißt, man bezieht sich positiv auf die Errungenschaften der neuen Informations- und Kommunikationstechnologien und begrüßt die Möglichkeiten, die mit dem Internet, sozialen Netzwerken, Chats, E-Mails, Mobilfunktelefonen und anderen neuen digitalen Kommunikationswegen im Alltag verbunden sind. Man nutzt diese zum Beispiel aktiv, um neue (Gegen-)Öffentlichkeiten etwa in Form von Blogs und neuen Websites entstehen zu lassen. Die Kritik richtet sich vor allem gegen die Kommerzialisierung des Internets und die kapitalistischen Verwertungsinteressen von transnationalen Konzernen, die inzwischen den Markt beherrschen und erhebliche Zugriffsmöglichkeiten auf persönliche Daten haben, die sie für ihre Geschäfte nutzen. Hierzu gehören Telekommunikationsanbieter wie die Telekom, O₂ und E-Plus ebenso wie das US-amerikanische Unternehmen Google mit seiner marktführenden Internet-Suchmaschine und Facebook, das weiterhin das weltweit wichtigste virtuelle soziale Netzwerk darstellt. Entsprechend wurde im Rahmen der Proteste gegen die Vorratsdatenspeicherung immer wieder dazu aufgefordert, quelloffene und nicht kommerzielle Anbieter von Verschlüsselungen, Suchmaschinen, Messenger-Diensten und Website-Hostern zu benutzen.

Ein zweiter wesentlicher Kritikpunkt dieser technikaffinen, aber herrschaftskritischen linken Bewegung ist die staatliche Überwachung digitaler Kommunikationsprozesse, die sich in Richtung einer staatlichen Generalkontrolle entwickle und ein für demokratische Gesellschaften inakzeptables Gefühl erzeuge, ständig unter Verdacht und im Visier von staatlichen Stellen zu stehen. Dies sei angsteinflößend und politisch schädlich, da damit individuelle und kollektive Prozesse der Selbstreflexion wie auch demokratische Prozesse der zivilgesellschaftlichen Organisation behindert würden. Dem Demonstrationsmotto «Freiheit statt Angst» entsprechend vertreten die bürgerrechtlichen Proteste gegen die Vorratsdatenspeicherung einen emphatischen Freiheitsbegriff: Man verwehrt sich nicht nur gegen eine staatliche Totalüberwachung und fordert das Recht ein, «in Ruhe gelassen zu werden», sondern betont die Notwendigkeit des ungestörten politischen Austausches und der öffentlichen Artikulation von gesellschaftlichem Dissens.

WIE SICH MIT DER VORRATSDATEN- SPEICHERUNG STAATLICHE ÜBERWACHUNG VERÄNDERT

Angesichts der derzeitigen politischen Lage und des Stands der technischen Möglichkeiten lassen sich mindestens vier grundlegende Bedenken gegen die Vorratsdatenspeicherung anführen. Erstens wird damit die legale staatliche Überwachung gesellschaftlicher Kommunikationsprozesse im Inland massiv ausgeweitet: Fand diese bisher vor allem punktuell und einzelfallbezogen statt, könnte diese demnächst flächendeckend und automatisiert erfolgen. Von besonderer Relevanz ist hierbei die zeitliche Speicherpflicht:

Können Sicherheitsbehörden bereits seit der Verabschiedung des Terrorismusbekämpfungsgesetzes im Jahr 2002 auf Daten zugreifen, die im Rahmen der Rechnungslegung von Unternehmen für jeden Kunden gespeichert werden, ist mit der Vorratsdatenspeicherung nun eine gesetzlich festgeschriebene Vorhaltefrist für diese Daten verbunden. Zweitens erhöht sich mit der Vorratsdatenspeicherung die Intransparenz staatlicher Überwachung und Herrschaftsausübung: Die Menschen wissen zwar von der flächendeckenden Speicherung ihrer Verkehrs- und Verbindungsdaten (was bereits eine einschüchternde Wirkung haben kann), sie werden jedoch darüber im Unklaren gelassen, zu welchen Anlässen und Zwecken diese von wem abgerufen werden. Mit der Vorratsdatenspeicherung wachsen die Macht- und Eingriffsbefugnisse der Sicherheitsbehörden gegenüber der Bevölkerung: Jede und jeder kann anlasslos zu einer/einem Verdächtigen werden.

Damit geht drittens ein verändertes Verständnis von Privatheit einher: Galt diese bisher durch das Fernmeldegeheimnis als eine gegenüber staatlicher Kontrolle schützenswerte Sphäre, in die nur gut begründet und nachträglich eingegriffen werden durfte, ermöglicht die Vorratsdatenspeicherung nun Einblicke in private Beziehungen aller Art in einer Tiefe und einem Umfang, die bis dato nicht denkbar waren. Zwar betonen diejenigen, die das Gesetzgebungsverfahren vorangetrieben haben, man beabsichtige mit der Vorratsdatenspeicherung keine Dauerüberwachung der Bevölkerung. Der überwiegende Teil der Daten bleibe lediglich für eine überschaubare Zeit bei den Telekommunikationsprovidern gespeichert und würde überhaupt nicht abgerufen. Das ändert jedoch nichts daran, dass hiermit das Recht auf Privatsphäre sowie Vertrauensverhältnisse erheblich eingeschränkt und Verschwiegenheitspflichten etwa von Anwältinnen oder Ärztinnen entwertet und infrage gestellt werden.

Diese präventive Vorverlagerung staatlicher Kontrolle durch die Vorratsdatenspeicherung ins «Private» steht viertens im engen Verhältnis zu anderen Formen staatlicher Überwachung. Mit den Enthüllungen von Edward Snowden sind vor allem die Überwachungstätigkeiten der US-amerikanischen Geheimdienste, insbesondere die der National Security Agency (NSA), in den öffentlichen Fokus gerückt und damit die internationale Dimension des Problems. Dabei ist zu beachten ist, dass es kaum rechtliche Regelungen für die Spionage im Ausland gibt. In den meisten Fällen sind hierbei die internen Einschätzungen der Geheimdienste maßgeblich. Die neuen Kenntnisse über die massive Reichweite weltweiter Spionagenetzwerke (angeführt von der NSA und ihrem britischen Partnerdienst Government Communications Headquarters), die aufgrund von bilateralen Abkommen zur Datenweitergabe auch die Arbeit hiesiger Sicherheitsbehörden beeinflussen, können zu der Einschätzung veranlassen, die nationale Vorratsdatenspeicherung sei demgegenüber vergleichsweise «bedeutungslos». Dem ist jedoch entgegenzuhalten, dass beide Kontroll- und Überwachungssysteme äußerst ernstgenommen werden müssen. Während die Überwachung durch die NSA in Deutschland eine rechtlich illegale Überwachung von ausländischen Diensten darstellt, bedeutet die Vorratsdatenspeicherung dagegen eine legale überwachungspolitische Ermächtigung der deutschen Sicherheitsbehörden. Man sollte beides als ergänzende überwachungspolitische Maßnahmen begreifen: So wird sich zum Beispiel mit der Vorratsdatenspeicherung in Deutschland der Datenpool bei den Telekommunikationsunterneh-

men, auf den potenziell auch die Geheimdienste zugreifen können, massiv vergrößern.

VORRATSDATENSPEICHERUNG IM PRÄVENTIV-AUTORITÄREN SICHERHEITSSTAAT

Dieses ist umso wichtiger, weil allein schon die Vorratsdatenspeicherung eine überwachungspolitische Maßnahme von erheblicher Tragweite bedeutet, die das politische System in Deutschland grundlegend transformiert. Sie stellt einen entscheidenden Schritt in Richtung eines «präventiv-autoritären Sicherheitsstaats» (Rolf Gössner)⁴ dar, in dem individuelle Freiheits- und Bürgerrechte entscheidend geschwächt und staatlichen Sicherheits- und Kontrollbedürfnissen unterworfen werden. Begründet wird dies mit einem stark erweiterten Sicherheitsbegriff, in dessen Zentrum die Gefahrenabwehr und Prävention steht. Hinzu kommt die gesellschaftliche Tendenz hin zu einem neuen Freund-Feind-Denken und das Propagieren eines «alltäglichen Ausnahmezustands», womit Ängste und Verunsicherungen in der Bevölkerung aufgegriffen und zum Teil gezielt instrumentalisiert werden. Die Vorratsdatenspeicherung wird in diesem Zusammenhang als ein besonders wirksames Mittel zur Bekämpfung von ganz unterschiedlichen Formen der Kriminalität verkauft, seien es politisch motivierte Sprengstoffanschläge, Kinderpornografie, systematischer Computerbetrug («Enkeltrick») oder Rechtsradikalismus. Auch wenn derzeit dem «Kampf gegen den islamischen Terrorismus» als Legitimationsgrundlage eine besondere Bedeutung zukommt, greifen BefürworterInnen der Vorratsdatenspeicherung auf ganz verschiedene Argumentationsmuster zurück. So ist zum einen immer wieder von der Notwendigkeit «staatlicher Sicherheit im digitalen Raum» die Rede, zum anderen wird davor gewarnt, der europäische Integrationsprozess werde scheitern, wenn man sich nicht auf eine neue Richtlinie zur Vorratsdatenspeicherung einigen könne.⁵

Dabei verläuft die Auseinandersetzung häufig recht einseitig. Es wird viel zu wenig darüber nachgedacht, wie ein staatlicher und gesellschaftlicher Umgang mit vorhandenen Risiken und Gefahren aussehen könnte, der nicht vor allem auf Kontrolle und Repression setzt. Gleichzeitig fehlt es an stichfesten Beweisen, dass Vorratsdatenspeicherung wirklich das leisten kann, was ihre BefürworterInnen versprechen: nämlich mehr «kollektive Sicherheit». Bislang gibt es aus keinem Land, in dem Vorratsdaten gespeichert werden, empirische Belege dafür, dass sie der Polizei oder Geheimdiensten bei der Vorbeugung und Verfolgung von Straftaten und Anschlägen tatsächlich geholfen haben. In einem «präventiv-autoritären Sicherheitsstaat» mit bis dato kaum vorstellbaren digitalen Möglichkeiten zur Überwachung der Gesellschaft kommt den Sicherheitsbehörden aber eine herausgehobene Stellung und auch Definitionsmacht zu. In Verbindung mit dem Sanktionspotenzial des staatlichen Gewaltmonopols entsteht hier eine neue Form staatlicher Herrschaft, die kaum mehr kontrolliert werden kann. Bestehende Schutzmechanismen, wie die, dass die Abfrage von Verkehrsdaten durch die Sicherheitsbehörden von richterlicher Seite bewilligt werden muss, können diesen Umstand nicht abschwächen.⁶ Ist die Vorratsdatenspeicherung und die damit verbundene Kontrollarchitektur erst einmal durchgesetzt und etabliert, wird diese zudem wahrscheinlich weitere Begehrlichkeiten wecken und verschiedene Seiten zum «Missbrauch» anregen.

Zusammenfassend kann festgehalten werden, dass die Vorratsdatenspeicherung eine Reihe von demokratischen

Kernprinzipien und Freiheitsrechten berührt: Hierzu zählen der Datenschutz, der Schutz der Privatsphäre, der Schutz von Berufs- und Betriebsgeheimnissen sowie die Meinungs-, Presse- und Organisationsfreiheit. Die gesellschaftlichen Kosten, die mit der Einführung der Vorratsdatenspeicherung einhergehen können, sind in ihrer langfristigen Bedeutung kaum abzuschätzen. Was durch die präventive staatliche Überwachung der Gesellschaft droht, sind verschiedene Formen der Selbstkontrolle und -zensur. Bereits das Wissen über die Existenz von so weitreichenden Überwachungsmöglichkeiten wird viele dazu bringen, ihr Kommunikations- und Organisationsverhalten zu verändern, das heißt, den Kontakt zu bestimmten Personen oder Kreisen im Zweifel abzubreaken, bestimmte Orte oder Versammlungen nicht mehr aufzusuchen und auf den Gebrauch von grundgesetzlich garantierten Freiheiten zu verzichten. Auch zentrale Träger einer kritischen Öffentlichkeit und starken Zivilgesellschaft wie etwa JournalistInnen oder JuristInnen gehören unmittelbar zu den potenziellen Opfern der Vorratsdatenspeicherung. Wenn etwa journalistischer Quellenschutz nicht länger garantiert ist, also die Gewissheit von InformantInnen und sogenannten Whistleblowern, nicht enttarnt zu werden, können die Medien ihrer Funktion als «vierte Gewalt» in einem demokratisch verfassten Rechtsstaat kaum mehr nachkommen. Was dies konkret bedeutet, kann derzeit in zahlreichen autoritären Staaten studiert werden.

AUSBLICK

Es wird nicht einfach werden, diesen Vorstoß in Richtung eines präventiv-autoritären Sicherheitsstaats auf nationaler und europäischer Ebene aufzuhalten. Dabei kommt es von linker Seite vor allem darauf an, verschiedene Strategien miteinander zu verknüpfen. Um die Vorratsdatenspeicherung in Deutschland doch noch zu kippen, bereiten unter anderem Bürgerrechtsorganisationen wie der Bielefelder Verein «Digital Courage» derzeit in Namen von Zigtausenden BürgerInnen erneut eine Beschwerde beim Bundesverfassungsgericht vor.⁷ Deren Erfolgsaussichten sind derzeit schwer einzuschätzen. So hat das Bundesverfassungsgericht im Januar einen ersten Eilantrag gegen das im Dezember in Kraft getretene Gesetz abgelehnt. Zudem ist zu beachten, dass sich die RichterInnen in ihrem Urteil von 2010 nicht grundsätzlich gegen eine Vorratsdatenspeicherung ausgesprochen, sondern lediglich den datenschutzrechtlichen Rahmen moniert hatten.⁸ Anders der Europäische Gerichtshof: Dieser hatte grundsätzliche Bedenken gegen die europäische Richtlinie zur Vorratsdatenspeicherung geäußert, da damit ein besonders schwerer Grundrechtseingriff verbunden sei.⁹

Während derzeit also unklar ist, was auf dem juristischen Wege erreicht werden kann und wie lange sich dieser hinziehen wird, könnte gleichzeitig die kritische Auseinandersetzung mit den Chancen und Risiken der neuen Kommunikationstechnologien in der Gesellschaft vorangetrieben werden. Hierzu gehört, das Wissen über Verschlüsselungsmethoden und Leistungen von Anonymisierungsdiensten zu verbreiten und damit möglichst vielen Menschen Instrumente an die Hand zu geben, wie sie sich gegen Maßnahmen wie die Vorratsdatenspeicherung und andere Überwachungsmaßnahmen zur Wehr setzen können. Perspektivisch müsste es aber darum gehen, nicht nur über technische Möglichkeiten und Entwicklungen aufzuklären, sondern sich noch stärker die

gesellschaftlichen Mitbestimmungs- und Selbstorganisierungspotenziale anzueignen, die etwa den sogenannten Digital Commons innewohnen.¹⁰ Das heißt als Aufgabe an die Linke: Angesichts der zunehmenden Digitalisierung in allen Lebensbereichen und den damit verbundenen staatlichen und Überwachungsbestrebungen gilt es weiterhin, in einem ersten Schritt bürgerrechtliche Errungenschaften wie Datenschutz, Schutz der Privatsphäre, Presse- und Meinungsfreiheit zu verteidigen und in einem zweiten Schritt verstärkt über Ansätze der digitalen Mitbestimmung und Selbstverwaltung nachzudenken. Zu einer solchen demokratischen «digitalen Perspektive von unten» gehört es auch, an einem solidarischen Gesellschaftsentwurf festzuhalten, der im Gegensatz zu den gegenwärtig, von verschiedensten Seiten forcierten, repressiven und präventiv-autoritären Maßnahmen auf solidarische Konfliktlösungsstrategien setzt.¹¹ Der Kampf um den Erhalt von Grundrechten wird so durch einen zusätzlichen wichtigen Aspekt erweitert.

Lars Bretthauer, ehemaliger Stipendiat der Rosa-Luxemburg-Stiftung, promoviert am Fachbereich Gesellschaftswissenschaften der Universität Kassel zum Thema Vorratsdatenspeicherung. Organisiert ist er bei reflect! – Assoziation für politische Bildung und der AkG – Assoziation für kritische Gesellschaftsforschung.

1 Farin, Klaus/Seidel-Pielen, Eberhard: Die Scharfmacher: Schauplatz Innere Sicherheit, Hamburg 1994. **2** Der Europäische Gerichtshof erklärte im Jahr 2014 die Richtlinie über die Vorratsdatenspeicherung von Daten für ungültig. Vgl. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf>. **3** Gierow, Hauke: Vorratsdatenspeicherung. Gesetz in Kraft – Speicherung noch nicht, 2015, unter: www.golem.de/news/ueberwachung-gesetz-zur-vorratsdatenspeicherung-tritt-in-kraft-1512-118101.html. **4** Gössner, Rolf: Menschenrechte in Zeiten des Terrors – Kollateralschäden an der «Heimatfront», Hamburg 2007. **5** Vgl. Deutscher Bundestag: Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Neuordnung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, Berlin 2007, S. 28 ff. **6** Vgl. hierzu Max-Planck-Institut für ausländisches und internationales Strafrecht: Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO, Freiburg 2008, S. 410. **7** Vgl. dazu <https://digitalcourage.de/blog/2016/aktuelles-zur-verfassungsbeschwerde-gegen-die-vorratsdatenspeicherung>. **8** Vgl. Bundesverfassungsgericht: Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß, unter: <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2010/bvg10-011.html>. **9** Der Gerichtshof erklärte die Richtlinie über die Vorratsdatenspeicherung von Daten für ungültig. Vgl. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf>, S. 2. **10** Vgl. hierzu z. B. Stadler, Felix: Digitale Solidarität, herausgegeben von der Rosa-Luxemburg-Stiftung, Reihe Analysen, Berlin 2014. **11** Ansätze für eine basisdemokratische Organisation des staatlichen Gewaltmonopols finden sich u. a. bei Narr, Wolf-Dieter/Roth, Roland: Transformationen von Menschenrechten und Demokratie, in: Komitee für Grundrechte und Demokratie (Hrsg.): Die globale Transformation menschenrechtlicher Demokratie, Münster 2008, S. 18–45.

IMPRESSUM

STANDPUNKTE wird herausgegeben von der Rosa-Luxemburg-Stiftung und erscheint unregelmäßig
V. i. S. d. P.: Stefan Thimmel
Franz-Mehring-Platz 1 · 10243 Berlin · www.rosalux.de
ISSN 1867-3163 (Print), ISSN 1867-3171 (Internet)
Redaktionsschluss: April 2016
Lektorat: TEXT-ARBEIT, Berlin
Satz/Herstellung: MediaService GmbH Druck und Kommunikation
Gedruckt auf Circleoffset Premium White, 100 % Recycling