Mathias Tusche, Stefan Hügel

Log 2/2016

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau der Bürgerrechte stehen. Wir dokumentieren hier einige davon. Die Aufzählung ist sicherlich nicht vollständig; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

Februar 2016

3. Februar 2016: Datenschützer kritisieren die Pläne der Bundesregierung, zur Verhinderung von „Geldwäsche" eine Obergrenze von 5.000 € für Barzahlung einzuführen. Klaus Müller, der Chef des Verbraucherzentrale-Bundesverbands, erklärt dazu: „Bargeld ist gelebter Datenschutz. Und der darf nicht aufs Spiel gesetzt werden." Bereits zuvor hatte die SPD den Vorschlag ins Spiel gebracht, aus den gleichen Gründen den 500-€-Schein abzuschaffen (Quelle: Frankfurter Allgemeine, Heise, vgl. auch den offenen Brief in der *FIfF-Kommunikation* 1/2016 auf Seite 36).

3. Februar 2016: Nach dem Jahresbericht des Parlamentarischen Kontrollgremiums des Deutschen Bundestages nahm die Überwachung von Internet und Telefonnetz 2014 deutlich zu. Im Rahmen der „strategischen Fernmeldeaufklärung" und der damit verbundenen Einschränkung des Schutzes des Fernmeldegeheimnisses aus Paragraph 10 des Grundgesetzes verfingen sich demnach im Untersuchungsraum insgesamt 25.209 Telekommunikationsverkehre im Überwachungsnetz. 2013 waren es 15.401. Dies zeigt, dass trotz der Empörung über die weltweite Ausspähung der Telekommunikationsdaten, die 2013 offenbar wurde, die Bespitzelung der Bevölkerung weiter ausgebaut wird (Quelle: Heise).

3. Februar 2016: Die Tragfähigkeit des als Nachfolger von *Safe Harbor* ausgehandelten Datenschutzabkommens *Privacy Shield* wird von Bürgerrechtlern bezweifelt. Laut der Initiative *European Digital Rights* (EDRi) hat die Kommission dem Kaiser nur neue Kleider übergestreift. Nicht nur in dem skizzierten, noch völlig unreifen und löchrigen Schutzschild seien schwere Fehler vorhanden, sondern auch in damit zusammenhängenden zusätzlichen Rechtsinstrumenten. Dies betreffe insbesondere den Entwurf für einen *Judicial Redress Act*, der EU-Bürgern eigentlich ein Klagerecht in den USA in Datenschutzfragen eröffnen soll. Ferner habe der US-Gesetzgeber mit dem *Cybersecurity Act* Fakten geschaffen, der Unternehmen einen Freibrief zum Datentransfer an nationale Geheimdienste ausstelle (Quelle: EDRi, Heise).

5. Februar 2016: Aus dem Jahresbericht des schweizerischen Aufsichtsgremiums der parlamentarischen Geschäftsprüfungsdelegation geht hervor, dass der Schweizerische Geheimdienst Daten aller Reisenden bestimmter Flüge sammelt. Bekannt war, dass die Daten von Passagieren gesammelt würden, die aus sogenannten Risikoländern in die Schweiz einfliegen. Das diene der Terrorismusabwehr, wurde seinerzeit vom zuständigen Ministerium bestätigt. Nicht bekannt wurde bisher allerdings, dass dies sämtliche Flugpassagiere betreffe. Fluggesellschaften müssen auf Verlangen dem Staatssekretariat für Migration (SEM) die Passagierdaten für Flüge aus bestimmten Destinationen zur Verfügung stellen. Eigentlich hätte der Nachrichtendienst nur Informationen über ausländische Staatsangehörige aus „Risikoländern" erhalten dürfen (Quelle: Neue Zürcher Zeitung, Heise).

5. Februar 2016: Nach dem offiziellen Bericht der UN-Arbeitsgruppe für willkürliche Inhaftierungen wurden die Freiheitsrechte von Julian Assange mit der Inhaftierung von 2010 und dem anschließenden Hausarrest verletzt (Quelle: Heise).

5. Februar 2016: Der Verfassungsschutzchef in Thüringen, Stephan Kramer, fordert den Einbau von Hintertüren in Krypto-Messengern. Sicherheitsbehörden könnten Chats auf Diensten wie Threema nicht umfassend überwachen, klagt er. Die Forderung stößt in den folgenden Tagen auf scharfe Kritik. Landesdatenschützer Lutz Hasse erklärt, dass das in Folge von NSU- und NSA-Skandal verloren gegangene Vertrauen der Menschen in die Nachrichtendienste noch längst nicht wiederhergestellt sei. Weil der Staat nichts tue, um die digitale Sicherheit seiner Bürger zu gewährleisten, seien die Menschen auf Verschlüsselungstechnologien aller Art geradezu angewiesen (Quelle: Heise).

12. Februar 2016: Ein Ransomware-Virus legt das Lukas-Krankenhaus in Neuss lahm. Der Virus wurde als Anhang einer E-Mail verschickt. Das Krankenhaus ist zeitweise nur eingeschränkt funktionsfähig, weil viele Systeme heruntergefahren wurden. Aufgrund der Virusinfektion mussten offenbar mehrere Operationen verschoben werden. Nach Angaben der *Westdeutschen Allgemeinen Zeitung* sind britische Antivirus-Spezialisten dabei, den Virus zu bekämpfen und die IT-Systeme des Krankenhauses nach und nach wieder hochzufahren. Auch zwei andere Krankenhäuser in Nordrhein-Westfalen sollen sich den Virus eingefangen, den Vorfall aber nicht öffentlich gemacht haben (Quelle: WDR, Westdeutsche Allgemeine Zeitung, Heise).

22. Februar 2016: Ein neuer Bundestrojaner für die Quellen-Telekommunikationsüberwachung steht offenbar kurz vor der Einsatzgenehmigung. Für eine Neuentwicklung setzte das Bundesverfassungsgericht in seinem Urteil im Februar 2008 enge Grenzen. So soll der heimliche Fernzugriff auf Computer nur noch bei überragend wichtigen Rechtsgütern möglich sein. Es müssen etwa die Gefahr für Leib und Leben oder Straftaten gegen den Bestand des Staates bestehen (Quelle: Deutschlandfunk, Heise).

22. Februar 2016: Die SPD erwägt nach dem jüngsten Brandanschlag auf ein Asylbewerberheim im sächsischen Bautzen eine Videoüberwachung für Flüchtlingsheime. Es sei nicht hinnehmbar, dass nur rund ein Viertel der Anschläge auf Asylunterkünfte von der Polizei aufgeklärt werde, sagte SPD-Generalsekretärin

Katarina Barley nach der Sitzung des Parteivorstands (Quelle: Vorwärts, Heise).

23. Februar 2016: Bei einer Anhörung im Deutschen Bundestag haben Experten vor einer Rüstungsspirale im Cyberspace gewarnt. Das „Wettrüsten im Cyberspace" dürfe nicht weiter verstärkt werden; die Bundeswehr solle „generell keine offensiven Fähigkeiten" im Internet entwickeln. Die Bundeswehr sei verfassungsrechtlich verpflichtet, auf Cyberangriffe zu verzichten. Sie bergen immer Eskalationsrisiken, angesichts rechtlicher und technischer Unsicherheiten. Wichtiger sei es, Schutzmechanismen für eine „passive" Cyberabwehr zu entwickeln (Quelle: Heise).

23. Februar 2016: Aus Veröffentlichungen von Wikileaks geht hervor, dass Bundeskanzlerin Angela Merkel weitaus mehr überwacht wurde als bisher bekannt. Unter anderem seien Gespräche zwischen ihr und dem UN-Generalsekretär Ban Ki-moon aus dem Jahr 2008 ausgewertet worden. Auch weitere Gespräche zwischen Regierungschefs und Diplomaten sind offenbar abgehört worden (Quelle: Wikileaks, Heise).

23. Februar 2016: Peter Altmaier, Chef des Bundeskanzleramts, hat auf dem europäischen Polizeikongress in Berlin ein „neues Datenbewusstsein" gefordert. Die Idee der Datensparsamkeit, so findet er, stoße an ihre Grenzen. Er fordert auch, Mautdaten für die Aufklärung von Straftaten zu nutzen und lobt die internationale Zusammenarbeit der Geheimdienste im „Kampf gegen den Terrorismus". Diesen müssten alle Daten zur Verfügung gestellt werden, um frühzeitig terroristische Netzwerke zu erkennen (Quelle: Heise).

März 2016

1. März 2016: Großbritanniens Innenministerin Theresa May hat trotz heftiger parlamentarischer Kritik an ihrem ersten Entwurf für ein neues Überwachungsgesetz eine nur geringfügig überarbeitete Neuauflage der *Investigatory Powers Bill* vorgelegt. Laut *Guardian* wurden unter den wesentlichen Punkten lediglich die geplanten Maßnahmen zur Umgehung von Verschlüsselung abgeschwächt. Internetanbieter müssen für jeden Kunden die besuchten Webseiten für 12 Monate speichern. Einzelne Kompetenzen der Sicherheitsbehörden seien gegenüber der ersten Fassung sogar noch ausgeweitet worden (Quelle: Guardian, Telegraph, Heise).

3. März 2016: Aus Sicht der Bundesregierung gibt es zahlreiche Einsatzmöglichkeiten des Europäischen Datenrelaissystems (EDRS) bei Sicherheitsbehörden und Militärs. Aufgaben von Notfallorganisationen, Militär- und Grenzbehörden, zur Unterstützung von Außeneinsätzen der EU und zur Überwachung der Meere könnten durch die Satellitenaufklärung fast in Echtzeit mit Hilfe von EDRS erfüllt werden. Durch technische Schnittstellen und Strukturen können Daten schnell an die jeweiligen Anwender übermittelt werden. Die „Weltraum-Datenautobahn" dürfe „nicht zu einer weiteren Militarisierung und damit schließlich in eine Sackgasse" führen, erklärte dazu der linke Bundestagsabgeordnete Andrej Hunko. Die derzeitige Strategie ist seiner Ansicht nach eine „massive Subvention für die Rüstungsindustrie" (Quelle: Heise).

4. März 2016: Der Schweizer Nationalrat spricht sich für eine Beibehaltung der sechsmonatigen Aufbewahrungsdauer von Verbindungsdaten – sogenannten Randdaten – aus dem Fernmeldeverkehr aus. Zuvor war eine Ausweitung der Speicherungsdauer auf 12 Monate gefordert worden. Mit den Verbindungsdaten kann man feststellen, wer wann mit wem wie lange telefoniert hat und wer an wen beispielsweise E-Mails versendet. In der Schweiz werden die elektronischen Kommunikationsdaten bereits seit über 10 Jahren gespeichert. Aktuell soll das *Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs* (BÜPF) revidiert werden, dessen Grundzüge bereits seit vergangenem Jahr von den beiden Häusern des Parlaments festgelegt wurden (Quelle: Heise).

4. März 2016: Anfang Februar wurde das Verwaltungssystem der bayerischen Kleinstadt Dettelbach nahe Würzburg durch eine Infektion mit einer Version des Trojaners *Teslacrypt* komplett lahmgelegt. Die Stadt zahlte daraufhin das geforderte Lösegelt von 1,3 Bitcoin (aktuell rund 500 Euro), wie das Polizeipräsidium Unterfranken mitteilte. Offenbar konnten die Daten aber nur zum Teil wiederhergestellt werden (Quelle: Heise).

11. März 2016: Der Europäische Rat fordert die Mitgliedsländer auf, Webseiten zu entfernen oder blockieren zu lassen, die zu terroristischen Straftaten aufrufen. Wird illegal in IT-Systeme oder Datenflüsse eingegriffen, so soll dies nach Auffassung des Rates als Terrorakt gewertet werden (Quelle: Heise).

12. März 2016: Nach Ansicht des französischen Innenministers Bernard Cazeneuve behindern Technologieunternehmen die Aufklärung der jihadistischen Terroranschläge von Paris vom November 2015, bei denen 130 Todesopfer zu beklagen waren. Den Ermittlern sei es bisher nicht gelungen, die Daten zu entschlüsseln, die auf den Mobiltelefonen der mutmaßlichen Attentäter gespeichert sind. „Weil sie sich Zeit nehmen, machen es die Technologieunternehmen schwerer für Frankreich, weitere Terrorangriffe zu verhindern", erklärte der Innenminister gegenüber dem US-Sender CNN in Washington (Quelle: CNN, Heise).

14. März 2016: Die Bundespolizei soll nach Plänen der Bundesregierung zukünftig mit sogenannten Bodycams ausgestattet werden. Die Kameras hätten sich im Einsatz in verschiedenen Bundesländern bewährt. Auf Länderebene, in Hessen und Rheinland-Pfalz, habe die Zahl der Übergriffe auf Polizisten abgenommen, so der innenpolitische Sprecher der SPD-Bundestagsfraktion, Burkhard Lischka (Quelle: Rheinische Post, Heise).

16. März 2016: Nach Ansicht von 27 Bürgerrechtsgruppen, darunter die *American Civil Liberties Union* (ACLU), *Amnesty International*, der Verein *Digitale Gesellschaft*, die *Electronic Frontier Foundation* (EFF), die Initiative *European Digital Rights* (EDRi) und *La Quadrature du Net* ist der *Privacy Shield* (*Datenschutzschild*), der zwischen den USA und der EU ausgehandelt wurde, für die betroffenen Bürger nicht sicher genug. In einem offenen Brief wenden sie sich mit der Forderung an die europäische Artikel-29-Datenschutzgruppe, das Europäische Parlament und den Ministerrat, das Abkommen abzulehnen. Das Vertrauen in die digitale Wirtschaft werde untergraben und die Gefahr von Menschenrechtsverletzungen erhöht, beispielsweise durch geheimdienstliche Überwachungsprogramme. Das US-Recht erfülle nicht die europäischen Vorgaben, so die Bürgerrechtler. Die

Probleme, die den Europäischen Gerichtshof (EuGH) veranlasst hätten, das Vorgängerabkommen *Safe Harbor* zum Datentransfer in die USA abzulehnen, seien nicht behoben (Quelle: Heise).

16. März 2016: Aus Sicht des US-Unternehmens *Apple* geht das FBI mit seiner Auslegung des aus dem Jahr 1789 stammenden *All Writs Act* zu weit. Die Forderungen seien vom Parlament bisher explizit abgelehnt worden, erklärt Apple in seiner Antwort auf scharfe Vorwürfe des FBI. Die Geschichte könne nicht einfach umgeschrieben werden, indem der über 200 Jahre alte *All Writs Act* als „allmächtiger Zauberstab" charakterisiert werde. Es sei lediglich ein begrenztes verfahrenstechnisches Werkzeug (Quelle: Heise).

17. März 2016: Auf rund 8.000 Webseiten hat die Generalstaatsanwaltschaft Russlands die Löschung missliebiger Inhalte durchgesetzt. Der Behörde hatte dazu aufgefordert, „extremistisches Material" zu entfernen, unter anderem Videos, Artikel und Kommentare. Dazu gehörten russischsprachige Seiten, die Bürger für die Terrorgruppe *Islamischer Staat* (IS) anwerben wollten, so der Leiter der Abteilung *Terrorismus und Extremismus*, Timur Abregow. Um sich dem IS anzuschließen, sind nach Angaben des Innenministeriums bislang mehr als 3.400 russische Staatsbürger nach Syrien gereist. In der Gesetzgebung Russlands können allerdings auch Informationen über Drogen, Suizide und sexuelle Minderheiten oder politische Kritik an Russlands Außenpolitik in der Ukraine und in Syrien unter den Begriff Extremismus fallen. Wegen angeblich extremistischer Inhalte seien schon dutzende Nutzer sozialer Netzwerke zu teilweise langen Haftstrafen verurteilt worden (Quelle: Interfax, Heise).

17. März 2016: Dem Ex-Kanzleramtschef und Außenminister Frank-Walter Steinmeier war nach eigenen Angaben nicht bekannt, dass der BND befreundete Regierungen und Organisationen ausgespäht habe. Nach Ansicht des Bundesaußenministers ist die Ausspähung schädlich (Quelle: Heise).

18. März 2016: Die Bundesregierung sieht sich nicht in der Lage, weitere Informationen zum Ausmaß der NSA-Überwachung und die Rolle hiesiger Einrichtungen im US-Drohnenkrieg zu ermitteln, so Bundesaußenminister Frank-Walter Steinmeier im NSA-Untersuchungsausschuss des Bundestags. Mehr als die Versicherung von US-Präsident Barack Obama, dass vom US-Stützpunkt Ramstein in Rheinland-Pfalz keine Drohnenangriffe „gesteuert" würden, sei beispielsweise nicht zu erwarten, so der Minister. Es gebe keine tragfähigen Anhaltspunkte, diese Zusage des US-Präsidenten anzuzweifeln (Quelle: Heise).

23. März 2016: Nach den Anschlägen in Brüssel spricht sich der EU-Abgeordnete Jan Philipp Albrecht für die Zusammenarbeit der EU-Geheimdienste aus. Wie der CDU-Politiker Elmar Brok ist er aber auch der Ansicht, dass die Verschärfung von Gesetzen dafür nicht erforderlich sei (Quelle: Heise).

24. März 2016: Gemeinsam mit anderen Innenpolitikern und Polizeigewerkschaftlern spricht sich Bundesinnenminister Thomas de Maizière nach den Brüsseler Bombenexplosionen für einen besseren Austausch sicherheitsrelevanter Daten in Europa aus. „Datenschutz ist schön, aber in Krisenzeiten wie diesen hat Sicherheit Vorrang", erklärte er in den Tagesthemen der ARD. Der Chef des Axel-Springer-Konzerns, Mathias Döpfner, bislang ebenfalls kein ausdrücklicher Datenschutzverfechter, antwortete umgehend. „Skandal" und „Offenbarungseid des Rechtsstaates" nannte der Verleger den Satz des Bundesinnenministers. Wenn man es nach solchen Anschlägen mit dem Rechtsrahmen nicht mehr genau nehme, hätten die Terroristen gewonnen (Quelle: ARD, Die Welt, Heise).

April 2016

7. April 2016: Nach zahlreichen Bürgerrechtsorganisationen hat sich auch der *Bundesverband der Verbraucherzentralen* (vzbv) gegen den zwischen den USA und der EU vereinbarten *Datenschutzschild* ausgesprochen. Europäisches Datenschutzrecht werde durch das Abkommen unterlaufen; es dürfe so nicht verabschiedet werden, meint der Bundesverband (Quelle: Heise).

7. April 2016: Die Konferenz der Datenschutzbehörden von Bund und Ländern rufen die Hersteller von Fitnessarmbändern, Smart Watches und Mobilanwendungen zur Achtung der Persönlichkeitsrechte der Nutzer auf. Genannt wird dabei auch speziell die Privatsphäre von Arbeitnehmern und Versicherten. „Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen", warnen die Datenschutzbeauftragten in einer Entschließung. Bedienfehler oder unzureichende Technik könnten dazu führen, dass Gesundheitsinformationen unabsichtlich preisgegeben werden. Einige Dienste wiesen zudem „erhebliche Sicherheitsdefizite" auf, so dass Unbefugte auf die sensiblen Daten zugreifen könnten. Unter bestimmten Umständen bestehe überdies das Risiko, dass Einzelne sich aufgrund „massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge" genötigt fühlten, derartige Technik einzusetzen (Quelle: Datenschutzbeauftagte des Bundes und der Länder, Heise).

9. April 2016: Das EU-US-*Privacy-Shield,* das das vom EuGH abgelehnte *Safe-Harbor*-Abkommen ersetzen soll, das bisher den Datentransfer zwischen den USA und der EU geregelt hat, stößt weiterhin auf heftigen Widerstand. Die US-Administration hat der EU-Kommission schriftlich einen besseren Schutz für Daten, die aus der EU in die USA übertragen werden, zugesichert. Überwachungsmaßnahmen sollen demnach auf das „Notwendige und Verhältnismäßige" begrenzt werden, und die US-Seite will der Kommission jährlich Bericht erstatten (Quelle: Heise).

9. April 2016: Nach einem im Internet aufgetauchten Entwurf, der in den Vereinigten Staaten den Einsatz von Verschlüsselung regeln soll, wären zukünftig nur solche Systeme legal, die sich umgehen oder leicht entschlüsseln ließen (Quelle: Heise).

10. April 2016: Die Einsatzfähigkeit der heftig umstrittenen neuen Software zur Quellen-Telekommunikationüberwachung („Bundestrojaner"), den IT-Experten des Bundeskriminalamts (BKA) im Lauf von drei Jahren entwickelt haben, hat sich aus Sicht der Behörden als deutlich eingeschränkt erwiesen. Jihadisten, Rechtsextremisten oder andere Gefährder nutzten vor allem WhatsApp oder andere Instant-Messenger zur Kommunikation, so ein Beamter eines Landeskriminalamts (LKA) gegenüber der Zeitung *Die Welt*. Es sei nicht möglich, solche Chat-Programme mit der speziell angefertigten Software abzuhören (Quelle: Die Welt, Heise).

11. April 2016: Die US-Regierung setzt das IT-Unternehmen *Apple* im Streit um Verschlüsselung noch stärker unter Druck, als es bisher bekannt war. In einem weiteren Gerichtsverfahren, das Bürgerrechtler nun öffentlich machten, fordert die US-Regierung ebenfalls von Apple Hilfe beim Entsperren eines iPhones (Quelle: Heise).

12. April 2016: WhatsApp wird in die Krypto-Messenger-Topliste der *Electronic Frontier Foundation* (EFF) aufgenommen; die Organisation lobt die Verschlüsselung. Neben der starken Verschlüsselung von WhatsApp stellt die Electronic Frontier Foundation dabei auch die einfache Handhabung heraus: Die EFF hebt besonders hervor, dass bei der Kompromittierung eines Schüssels Chats aus der Vergangenheit dank *Forward Secrecy* (durch *Axolotl Ratcheting*) weiterhin verschlüsselt bleiben. Nutzer können bei WhatsApp außerdem die Identität von Kontakten überprüfen. Lediglich ein QR-Code muss vom Smartphone-Bildschirm eines Chat-Partners gescannt oder die Sicherheitsnummer verglichen werden (Quelle: Heise).

12. April 2016: Als zuverlässige Basis für *Trusted Computing*, also für vertrauenswürdige Datenverarbeitung, gelten digitale Zertifikate. Bisher liegen die praktisch und gewerblich nutzbaren Infrastrukturen dafür jedoch in der Hand weniger großer Anbieter. In einem Forschungsvorhaben der Bundesregierung zu alternativen Zertifizierungsinfrastrukturen soll nun der „Konflikt zwischen ‚Marktzugang' und ‚Sicherheit' beim Trusted-Computing-Konzept" untersucht werden (Quelle: Heise).

12. April 2016: Nach vierjährigen Beratungen stimmt der Ausschuss für bürgerliche Freiheiten in Straßburg einer EU-Grundverordnung zum Datenschutz und einer Richtlinie für die Datenverarbeitung zu polizeilichen Zwecken zu. Der Berichterstatter des europäischen Parlaments für die Datenschutzverordnung, der Grüne Jan Philipp Albrecht, spricht von „einem riesigen Erfolg". EU-Justizkommissarin Vera Jourova erklärte, künftig gelte für alle Unternehmen, die in der EU Geschäfte machen wollten, gleiches Recht. Nutzer können nun unter anderem Informationen leichter aus dem Internet löschen lassen (*Recht auf Vergessenwerden*). Zudem sollen sie ihre Daten bei einem Anbieterwechsel leichter von einem Anbieter zum nächsten mitnehmen können (*Portabilität*). Internetkonzerne sind verpflichtet, eine ausdrückliche Zustimmung zur Datennutzung einzuholen und ihre Produkte datenschutzfreundlich voreinzustellen (Quelle: dpa, Heise).

12. April 2016: Neben der EU-Datenschutzgrundverordnung lässt das europäische Parlament auch die PNR- (Passenger Name Records) Richtlinie passieren. Die Richtlinie verpflichtet Fluggesellschaften, den Staaten der EU ihre Datensätze mit den Daten der Fluggäste zu überlassen. Persönliche Daten von Fluggästen wie Name, Kreditkartennummer und Essenswünsche werden dabei künftig auf Vorrat gespeichert. Es soll aber keinen automatischen Austausch aller Daten zwischen den EU-Staaten geben (Quelle: dpa, Heise).

13. April 2016: Die Bundesdatenschutzbeauftragte Andrea Voßhoff stimmt den Kritiker.innen der neuen Rahmenvereinbarung zwischen EU und USA zum Datentransfer von Unternehmen zu. Die Datenschützer der EU-Staaten fordern damit Nachbesserungen beim EU-US-Datenschutzschild *Privacy Shield* zum Informationstransfer in die USA. Unter anderem sind die Datenschützer besorgt, dass immer noch massenhaft Informationen im Dienst der öffentlichen Sicherheit gesammelt würden. Diese Möglichkeit werde derzeit durch den Datenschutzschild nicht verhindert. Den Änderungswillen der EU-Kommission zweifelt auch der österreichische Datenschutzaktivist Max Schrems an, der das EuGH-Urteil gegen *Safe Harbor* erreicht hatte. Die Vereinbarung sei ein „kompletter Misserfolg", sie werde nur durch den Druck der US-Regierung und einiger Branchen am Leben erhalten (Quelle: dpa, Heise).

15. April 2016: Das Bundesamt für Verfassungsschutz (BfV) führe nach Aussagen von Mitarbeiter.innen generell „keine anlasslose verdachtsunabhängige Massenüberwachung" durch, auch die Spähsoftware *XKeyscore* werde nicht zu diesem Zweck eingesetzt. Lediglich Individualkommunikation auf der Grundlage von G10-Anordnungen, mit denen das Fernmeldegeheimnis eingeschränkt werden kann, werde überwacht (Quelle: Heise).

16. April 2016: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Andrea Voßhoff, wirft dem Bundesnachrichtendienst (BND) Missachtung ihrer Behörde vor. Dies berichtet das Nachrichtenmagazin *Der Spiegel*. Er beruft sich dabei auf einen 60-seitigen Bericht zur Zusammenarbeit Deutschlands und der USA in der Überwachungsstation in Bad Aibling. Der BND habe sich demnach geweigert, der Bundesdatenschutzbeauftragten die Selektoren-Listen zu überlassen, die die NSA dem BND zum Ausfiltern und Weiterleiten von Telekommunikationsdaten zugeleitet hatte. Alle Selektoren, die in deutschen Systemen verarbeitet werden, unterlägen deutschem Recht und damit der Kontrolle durch die Bundesdatenschutzbeauftragte, heißt es in Voßhoffs Bericht weiter. Die NSA-Selektoren hätten nach Voßhoffs Einschätzung niemals für die Kommunikationsüberwachung des BND verwendet werden dürfen (Quelle: Der Spiegel, Heise).

16. April 2016: Für die Nutzung und Weitergabe von Informationen per Internet sind Kurz-URLs nützlich, wie sie von Diensten wie *bit.ly* angeboten werden. Nutzer geben damit aber unbeabsichtigt wesentlich mehr private Informationen preis, als sie beabsichtigen und ihnen bewusst sein dürfte. Zu diesem Ergebnis kommt eine Studie des *Jacobs Technion-Instituts* der *Cornell-Universität* im US-Bundestaat New York. Wie die Autoren Martin Georgiev und Vitaly Shmatikov zeigen, lassen sich Short-Links besonders gut scannen, gerade weil sie nur aus wenigen Zeichen bestehen (Quelle: Cornell-Universität, Heise).

18. April 2016: Auf ihrer Frühjahrskonferenz in Heringsdorf auf Usedom haben sich die Verkehrsminister der deutschen Bundesländer für eine deutlich ausgeweitete Videoüberwachung in Bussen und Bahnen ausgesprochen. Sie fordern in einem Beschluss die „flächendeckende, tageszeitunabhängige Videoaufzeichnung in öffentlichen Verkehrsmitteln" im Sinne einer „einheitlichen Sicherheitsphilosophie im öffentlichen Personennahverkehr". Die „Vorgaben des Datenschutzes" sollen aber bei der Videoüberwachung beachtet werden. Die Opposition im Bundestag kritisiert den Vorstoß der Verkehrsminister. Der verkehrspolitische Sprecher der Linksfraktion, Herbert Behrens, warnt vor einem „Einstieg in die Totalüberwachung des öffentlichen Raumes" (Quelle: Heise).

18. April 2016: Die Klage einer Frau aus Lüdenscheid gegen das Freihandelsabkommen CETA zwischen der EU und Kanada wird mittlerweile von 51.736 Mitkläger.innen unterstützt. Durch die Klage soll das Freihandelsabkommen CETA zwischen der EU und Kanada vor dem Bundesverfassungsgericht gestoppt werden. Die Klägerin, Marianne Grimmenstein, sieht durch das Abkommen ihre Bürger- und Verbraucherrechte bedroht; gemeinsam mit dem Bielefelder Rechtsprofessor Andreas Fisahn hat sie eine Verfassungsbeschwerde vorbereitet. In einem Interview mit der *Neuen Westfälischen Zeitung* erläutert Fisahn, dass Investoren klagen könnten, wenn nach ihrer Ansicht in ihr Eigentum eingegriffen wird. „Das liegt laut CETA-Vertrag vor, wenn die vernünftigen Gewinnerwartungen geschmälert werden." Das Spektrum der möglichen Klagen sei sehr breit. Es könnte nach Aussage von Fisahn auch gegen Umwelt- oder Arbeitsschutzregeln oder die Mitbestimmung von Betriebsräten geklagt werden; eben alles, was die Gewinnerwartung schmälert (Quelle: dpa, Neue Westfälische Zeitung, Heise).

19. April 2016: Die fünf nördlichsten deutschen Bundesländer planen, bis 2020 die Telekommunikationsüberwachung ihrer Polizeien zu zentralisieren. Der zugehörige Staatsvertrag liegt nun nach langer Vorbereitung vor. Know-how würde durch die länderübergreifende Kooperation gebündelt und es würden Kosten gespart, erläutert die niedersächsische Staatskanzlei in einer Mitteilung (Quelle: Heise).

20. April 2016: Das BKA-Gesetz wird durch das Bundesverfassungsgericht teilweise für verfassungswidrig erklärt. Seit 2009 durften Ermittler Wohnungen akustisch und durch Kameras visuell überwachen und Telefonate abhören. Das Gesetz war auch Grundlage für den „Bundestrojaner" zur Quellen-Telekommunikationsüberwachung, mit dem sich Kommunikationsdaten, beispielsweise aus Chats, bei Terrorverdächtigen ausspähen lassen. Kritiker sehen durch diese weitreichenden Befugnisse Bürgerrechte verletzt und forderten Nachbesserungen. Aus ihrer Sicht ist nicht ausreichend sichergestellt, dass der intime Bereich unangetastet bleibt. Das BKA darf auch Daten an die Geheimdienste und an ausländische Stellen weitergeben. Den Kritikern des Gesetzes hat das Bundesverfassungsgericht nun teilweise Recht gegeben; das Gesetz muss umfassend nachgebessert werden (Quelle: Heise, dazu auch unsere Stellungnahme auf Seite 14).

28. April 2016: Das Start-Up-Unternehmen *ZeroZero* aus China hat eine etwa taschenbuchgroße und 240 Gramm leichte sogenannte *Hover Camera* vorgestellt. Die fliegende Kamera, die eine Auflösung von 13 Megapixel liefert und sich an den gewonnenen Bilddaten anstatt an GPS orientiert, soll Personen erkennen und diesen dann folgen können. Nutzer.innen können von der Kamera aufgenommene Personen markieren; die Fotodrohne folgt dieser Person dann und kann sie beispielsweise umkreisen (Quelle: Heise).

Mai 2016

2. Mai 2016: Das kostenlose Internetangebot *Free Basics* von *Facebook* hat Eben Moglen, Gründer des *Software Freedom Law Center,* kritisiert. Er nannte es ein Sinnbild für das Grundübel der digitalen Wirtschaft. Der Konzern übernehme zwar die Zugangsgebühren zu einem eingeschränkten Netz, dies aber im Gegenzug zu einer Komplettüberwachung der Nutzer, so der US-Amerikaner auf der re:publica in Berlin. Das Bekanntwerden der Überwachungstechniken habe bei den staatlichen Agenten nur dazu geführt, die Spirale weiter nach oben zu drehen und mehr oder weniger unverhüllt die Echtzeitüberwachung und Abbildung der gesamten Bevölkerung in Form *sozialer Graphen* zu fordern (Quelle: Heise).

2. Mai 2016: Die Hintergründe der Aktion, mit der TTIP-Dokumente befreit wurden, hat Greenpeace auf der re:publica vorgestellt. Die Umweltaktivisten richteten vor dem Brandenburger Tor einen transparenten Leseraum ein, der auch von Politikern besucht werden konnte. Bei der Aktion wurden rund 75 Prozent der TTIP-Papiere zu den unterschiedlichen Verhandlungspositionen der USA und Europa veröffentlicht; Greenpeace Niederlande hat sie zusätzlich ins Netz gestellt (Quelle: Greenpeace, Heise).

4. Mai 2016: *Prozesse algorithmischer Entscheidungsfindung* will die Beobachtungsplattform *Algorithm Watch* unter die Lupe nehmen. Auf der Berliner Tagung re:publica wurde die Plattform von Informatikern, Journalisten und Philosophen vorgestellt. Algorithmen sollen untersucht werden, die beim *Algorithmic Decision Making* (ADM) zum Einsatz kommen. Algorithm Watch will, ähnlich Foodwatch, „Regulierungsstrategien" entwickeln und dafür sorgen, dass technische Prozesse nicht für den Verstoß gegen Bürgerrechte genutzt werden. Gesellschaftlich relevante Technik soll untersucht werden, so beispielsweise *Predictive Analytics* bei der Polizei oder die automatisierte Vorprüfung von Visumanträgen (Quelle: Heise).

9. Mai 2016: Die neuen Vorschriften zur Vorratsdatenspeicherung will der Münchener Zugangsanbieter *Spacenet* verwaltungsgerichtlich gemeinsam mit dem Providerverband *eco* zu Fall bringen. Sebastian von Bomhard, Vorstand der *Spacenet AG*, stellte die Klage des von ihm geführten Internetproviders gegen das jüngste Gesetz zur Vorratsdatenspeicherung vor. Angeblich gehe es um den Kampf gegen den Terror, doch im Netz der Fahnder blieben dann höchstens „die kleinen Cybercrime-Dinge" hängen, sagte er. Auch mit dem neuen Vorhaben sei es nicht möglich, organisierte Kriminalität wirksam zu verfolgen. Die wenigen Daten seien von Strafverfolgern bisher „durchschnittlich anderthalb Jahre nach dem Vorfall" angefragt worden; dies liegt weit jenseits der gesetzlichen Speicherpflicht (Quelle: Heise).

9. Mai 2016: Twitter hat jetzt die Kooperation des Dienstleisters *Dataminr*, an dem das Unternehmen 5% Anteile besitzt, mit US-Geheimdiensten beendet. Interne Analysen von Twitter-Nachrichten sollen nicht zur Überwachung genutzt werden. Die Geheimdienste sollen sich wie „jeder andere auch" mit den öffentlichen Daten begnügen. Damit haben die US-Geheimdienste den Zugang zu einem Dienst verloren, durch den die Twitter-Nachrichten in Echtzeit analysiert werden können. Unter Berufung auf informierte Kreise berichtet das *Wall Street Journal*, dass *Dataminr* die Verträge mit Geheimdiensten auf Drängen von Twitter beendet habe. Das Unternehmen sei inzwischen das einzige, das direkten Zugriff auf den gesamten Strom an Tweets bekomme und an Kunden weiterverkaufen dürfe. Durch das Ende der Kooperation wird die zunehmende Entfremdung zwischen US-Technikunternehmen und US-Geheimdiensten deutlich (Quelle: Wall Street Journal, Heise).

10. Mai 2016: Der britische Aktivist Lauri Love muss die Passwörter zu seinen verschlüsselten Festplatten nicht an die Ermittlungsbehörden übergeben. Die Klage der *National Crime Agency* wurde von einem Gericht in London zurückgewiesen, die den Aktivisten zur Übergabe seiner Passwörter zwingen lassen wollte. In dem Zivilverfahren geht es um die Rückgabe einiger beschlagnahmter Computer und Datenträger des Hackers. Behörden können Verdächtige nach dem britischen Anti-Terror-Gesetz (*Regulation of Investigatory Powers Act*, RIPA) nur dann zur Herausgabe von Passwörtern zwingen, wenn konkrete Hinweise auf einen terroristischen Hintergrund vorliegen. „Mit der Ablehnung des NCA-Antrags hat das Gericht klargestellt, dass Behörden nicht versuchen dürfen, die vom Parlament eingesetzten Schutzvorkehrungen zu umgehen" (Quelle: Heise).

Wissenschaft & Frieden 2/2016 „Stadt im Konflikt – Urbane Gewalträume"

mit Dossier „Gescheiterter Friedensprozess und Bürgerkrieg in der Türkei"

Artikel zu den verschiedenen Aspekten von Krieg, Konflikt und Gewalt im städtischen Umfeld stehen im Mittelpunkt der Mai-Ausgabe von Wissenschaft & Frieden. Es geht um den Zusammenhang von Stadt, Land und Krieg, um künstliche Städte als Übungsräume für aktuelle und künftige Kriege, architektonisch-psychologische Überlegungen zu Stadt und Gewalt, um städtische Widerstandsformen sowie Flucht und Rassismus im Kontext der Stadt.

Es schreiben:

- Jürgen Scheffran: Stadt – Land – Krieg / Unsicherheit in urbanen Gewalträumen
- Andrea Kretschmann: Krieg und artifizieller Städtebau
- Jürgen Oßenbrügge: Formen urbaner Gewalt
- Nicole Conrad und Klaus Harnack: Stadt und Frieden – Eine architektonisch-umweltpsychologische Betrachtung
- Bettina Engels: Spontan und gewaltsam? – Riots als städtische Protestform
- Sascha Radl: Soziale Konflikte in Ägypten – Schnittstellen zwischen Land und Stadt
- Markus Bayer und Janet Kursawe: Gewaltfreier Widerstand und urbaner Raum
- Alfred Marder: Städte als Friedensbotschafter
- René Kreichauf: Flucht, Stadt und Rassismus – Geflüchtete in europäischen Städten

Weitere Artikel befassen sich mit dem Bundeswehreinsatz gegen den „Islamischen Staat", dem Verhältnis NATO-Russland, den Drohneneinsätzen, der Idee eines „Mächtekonzerts" für das 21. Jahrhundert sowie einem Projekt der Bürgerwissenschaften. Die kommentierte Presseschau behandelt das Thema „Bundeswehreinsatz im Innnern".

Dossier „Gescheiterter Friedensprozess und Bürgerkrieg in der Türkei"

Anfang 2013 rief der inhaftierte PKK-Vorsitzende Abdullah Öcalan nach Gesprächen mit der türkischen Regierung den Beginn einer demokratischen Ära aus. Die Waffen sollten einem Wettbewerb der Ideen weichen, die Guerilla sich aus der Türkei zurückziehen. Drei Jahre später muss nicht nur das Scheitern der Verhandlungen, sondern auch eine militärische Eskalation des Konflikts festgestellt werden. Seit Monaten werden urbane Zentren der überwiegend kurdisch besiedelten Region in der Türkei bombardiert und in zahlreichen Städten findet ein Häuserkampf statt. Im Dossier werden die Ursachen der aktuellen Eskalation diskutiert und Einsichten in den Charakter des Konflikts vermittelt.

Wissenschaft & Frieden 2/2016 **„Stadt im Konflikt – Urbane Gewalträume"**, € 7,50 plus Porto.

Wissenschaft & Frieden 1/2016 **„Forschen für den Frieden"**, 7,50 € plus Porto.

W&F erscheint vierteljährlich. Jahresabo 30 €, ermäßigt 20 €, Ausland 35 €, ermäßigt 25 €, Förderabo 60 €. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.

Bezug: W&F, Beringstr. 14, 53115 Bonn,
E-Mail: *buero-bonn@wissenschaft-und-frieden.de,*
www.wissenschaft-und-frieden.de