

Datenschutz zwischen regulatorischer Reform und soziotechnischer Revolution: "Die Fortentwicklung des Datenschutzes", Berlin, 2.-3. November 2017

Martin, Nicholas; Karaboga, Murat

Veröffentlichungsversion / Published Version

Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:

Martin, N., & Karaboga, M. (2018). Datenschutz zwischen regulatorischer Reform und soziotechnischer Revolution: "Die Fortentwicklung des Datenschutzes", Berlin, 2.-3. November 2017. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis / Journal for Technology Assessment in Theory and Practice*, 27(1), 70-73. <https://doi.org/10.14512/tatup.27.1.70>

Nutzungsbedingungen:

Dieser Text wird unter einer CC BY Lizenz (Namensnennung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:

<https://creativecommons.org/licenses/by/4.0/deed.de>

Terms of use:

This document is made available under a CC BY Licence (Attribution). For more information see:

<https://creativecommons.org/licenses/by/4.0>

den, der einen theoretischen Rahmen zur Analyse digitaler Infrastrukturen in der Wissenschaft anbot. Diese Zugänge sind vielleicht nicht völlig neu, bislang aber weniger etabliert.

Koexistenz als Haltung

Insgesamt zeigten die Diskussionen auf der Tagung eine gewisse Reife des Feldes auf. Die Zeiten der großen Fragen um die soziale Konstruktion von Wissenschaft und Technik, den epistemischen (Sonder-)Status von wissenschaftlichem Wissen und den Stellenwert von (Sach-)Technik innerhalb der Sozialtheorie scheinen erst einmal vorbei zu sein. Die verschiedenen Zugänge werden kaum noch im Grundsatz in Frage gestellt; stattdessen wird – in weiten Teilen – die Pluralität anerkannt. Auch diese Haltung mag ein Resultat eines mehr 30 Jahre langen Diskussionsprozesses über die gesellschaftliche Rolle von Wissenschaft und Technik sein.

70

BERICHT

Datenschutz zwischen regulato- rischer Reform und soziotechni- scher Revolution

„Die Fortentwicklung des Datenschutzes“,
Berlin, 2.–3. November 2017

Nicholas Martin, *Fraunhofer-Institut für System- und Innovationsforschung,
Breslauer Straße 48, 76139 Karlsruhe (nicholas.martin@isi.fraunhofer.de)*

Murat Karaboga, *Fraunhofer-Institut für System- und Innovationsforschung
(murat.karaboga@isi.fraunhofer.de)*

Im Nachgang der Snowden-Enthüllungen traf die Idee, Datenschutz und Privatheit auf breiter wissenschaftlicher Basis zu untersuchen, im Bundesministerium für Bildung und Forschung auf fruchtbaren Boden. Das hieraus entstandene interdisziplinäre Forschungsprojekt „Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt“ veranstaltete im November 2017 in Berlin seine zweite Jahrestagung. Vor dem Hintergrund der Herausforderungen für den Datenschutz, die sich aus der extremen Geschwindigkeit der technisch-wirtschaftlichen Entwicklung ergeben, sollten die Möglichkeiten einer Fortentwicklung des Datenschutzes diskutiert werden, unter Einbezug rechtlicher, technischer und sozialwissenschaftlicher Ansätze. Aufmerksamkeit richtete sich insbesondere auf die Wirkungen, Potentiale und möglichen Unzulänglichkeiten der ab dem 25. Mai 2018 EU-weit anzuwendenden EU-Datenschutzgrundverordnung (DSGVO). Die DSGVO ersetzt die 1995 erlassene EU Datenschutz-Richtlinie. Sie beansprucht für sich, den Datenschutz in der EU grundlegend zu modernisieren und zukunftsfest zu machen.¹ Zentrale Frage der von über 150 WissenschaftlerInnen, zivilgesellschaftlichen AkteurInnen und VertreterInnen aus Politik, Wirtschaft und Behörden besuchten Veranstaltung war, ob die DSGVO diesen Anspruch einlösen kann.

Weitere Informationen

Tagungsprogramm:
<http://www.gwtf.de/2017-programm-GWTF.pdf>

¹ Siehe auch Friedewald, Michael: Datenschutz-Folgenabschätzung in dieser Zeitschrift Jg. 26, Nr. 1–2, S. 66–71, Aug. 2017.

Hintergrund und Herausforderungen

Die sich für den Datenschutz ergebenden Herausforderungen wurden in Vorträgen von Prof. Alexander Roßnagel und Prof. Gerrit Hornung (beide Universität Kassel, Recht), Dr. Frank Pallas (TU Berlin, Wirtschaftsinformatik) sowie Martin Rost (Landeszentrum für Datenschutz Schleswig-Holstein) skizziert.

Wie Frank Pallas in seinem Vortrag beschrieb, führt die rasche Fortentwicklung der Informationstechnik und der auf ihr fußenden Geschäftsmodelle zu einer allumfassenden Vernetzung der Gesellschaft und immer präziseren Erfassung des täglichen Lebens. Dies betrifft längst nicht mehr nur die Erstellung detaillierter Nutzerprofile durch Suchmaschinen und Soziale Netzwerke, die unsere Interessen, Einkäufe, Kommunikationsverhalten und sonstigen Vorlieben aufzeichnen. Zu diesen mittlerweile fast „herkömmlichen“ Datenverarbeitungen treten nun ausgefeilte Systeme zur Bild-, Biometrie- und Emotionserkennung, die Aufzeichnung von Gesundheits- und sonstigen Daten durch Wearables wie Fitness Tracker, der Aufbau weitreichender, durchwegs vernetzter Sensorsysteme im Rahmen von Industrie 4.0/Internet der Dinge und *Ubiquitous Computing* (Smart Car/Home/Health, Assistenzsysteme, etc.) und zunehmend selbstlernende und automatisierte Analyseverfahren, die sehr große Datenmengen aus unterschiedlichsten Quellen verarbeiten können (Big Data, Künstliche Intelligenz). Dies führt zu einer explosionsartigen Zunahme der verfügbaren personenbezogenen Daten, und immer komplexeren, selbst für Fachleute nur schwer durchschaubaren Datenflüssen und -verwertungsketten. Gerrit Hornung unterstrich in seinem Vortrag daher, dass Datenschutzregulierung unter erschwerten Bedingungen ist: Aufgrund der Geschwindigkeit des Fortschritts klaffen Innovations- und Regulationszyklen regelmäßig auseinander, die Gesetzgebung droht regelmäßig von der technischen Entwicklung überholt zu werden. Was hier stattfindet, so Pallas, ist nicht mehr der „übliche Fortschritt“, sondern ein Paradigmen-

führt den Datenschutz-Grundsatz der Transparenz an subjektive Grenzen (Überforderung) und objektive Grenzen der Informationsvermittlung. Ebenso geraten in einer Welt, in der Daten für vielfältige, im Vorhinein *unbekannte und unvorhersehbare* Zwecke verarbeitet werden sollen (Big Data) die Grundsätze der Zweckbindung massiv unter Druck.

Menschen sind daher permanent mit der Notwendigkeit konfrontiert, abzuwägen, ob und wie die Nutzung digital-vernetzter Dienste den Raum für selbstbestimmtes Handeln vergrößert – oder nicht. Einerseits versprechen die fraglichen Dienste den Nutzern, ihr Leben zu erleichtern, zu bereichern und ihnen zusätzliche Steuerungsmöglichkeiten zu bieten. Andererseits ist die Nutzung oftmals mit zeitlich fernliegenden, abstrakten oder sich gar nicht individuell, sondern gesellschaftlich niederschlagenden Risiken und Problemen verbunden, welche in der individuellen Abwägung auch praktisch kaum abzuschätzen sind. In der Folge ergibt sich oftmals eine Höherbewertung unmittelbarer Vorteile. Gegenwärtige, auf (informationeller) Selbstbestimmung fußende Datenschutzkonzeptionen geraten angesichts dieser Schwierigkeiten zunehmend an ihre Grenzen.

Streitpunkt DSGVO: Zukunftsfähigkeit, Rechts(un)sicherheit und Sanktionspotentiale

Inwiefern bietet die DSGVO eine adäquate Antwort auf diese Herausforderungen? Alexander Roßnagel sprach zwei Kritikpunkte aus: Erstens, mangelnde Zukunftsfähigkeit angesichts neuer Technologien. Die Verordnung enthalte keine einzige Regelung, um die spezifischen Grundrechtsrisiken zu adressieren, die aus Technologien wie Big Data oder Ubiquitous Computing hervorgingen. Stattdessen führe ein missverstandenes Prinzip der Technikneutralität in der DSGVO zu Risikoneutralität, und damit tendenziell zu einer Absenkung des bestehenden Datenschutzniveaus. Wie etwa die eCall-Verordnung zeige, sei risikoadäquate Regulierung jedoch sehr wohl möglich. Zweitens

Gegenwärtige, auf (informationeller) Selbstbestimmung fußende Datenschutzkonzeptionen geraten zunehmend an ihre Grenzen.

wechsel hin zu „vollkommen neuen sozio-technischen Arrangements“. Diese Entwicklungen, betonten sowohl Pallas wie Alexander Roßnagel, hebeln oft traditionelle Grundsätze und Modi operandi des Datenschutzes aus.

Insofern Systeme und Dienstleistungen grundlegende Infrastrukturen der digitalen Gesellschaft bereitstellen, ist deren *Nicht-Nutzung* bei voller Teilhabe an der Informationsgesellschaft häufig nur begrenzt möglich. Nutzer stehen insofern vor einem faktischen Zwang, ihre „Einwilligung“ zur Nutzung ihrer Daten zu geben. Die vorgebliche Kostenlosigkeit der Angebote (in Wahrheit, ihre entgeltfreie Nutzung im Gegenzug für Datenabgabe) verführt zusätzlich zur Nutzung. Die Vielzahl der Datenverarbeitungsvorgänge und Komplexität der Verarbeitungsketten

werde, wie auch Gerrit Hornung ausführte, die DSGVO nicht wie beabsichtigt zu einer Harmonisierung des Datenschutzrechts in der EU führen. Was die nationalen Gesetzgebungen bisher in tausenden von Einzelschriften regulieren, versuche die Verordnung in 51 abstrakten Artikeln zu adressieren. Gepaart mit der Vielzahl von Öffnungsklauseln werde Interpretationsbefugnis somit wieder an Mitgliedsstaaten, Aufsichtsbehörden und Gerichte (letztlich: den EuGH) verlagert. Auch wegen der Langsamkeit gerichtlicher Prozesse seien daher Rechtsunsicherheit und fehlende Harmonisierung zu erwarten.

Diese Kritik an der DSGVO wurde nicht von allen geteilt. Vertreter des Bundesjustizministeriums (Carsten Hayungs), der EU Kommission (Paul Nemitz) und des Europäischen Daten-



Abb. 1: Frank Pallas beschreibt die vernetzte Datenerfassung des alltäglichen Lebens.

Quelle: Forum Privatheit

schutzbeauftragten (Achim Klubunde) verwiesen auf politische Realitäten: Die DSGVO sei *die* DSGVO, die in Europa politisch möglich war; ferner werde das in der DSGVO vorgesehene Kohärenzverfahren relativ schnell ein *case law* und damit Harmonisierung schaffen (Hayungs). In einer Demokratie entstehe Recht immer aus Kompromissen (Nemitz). Angesichts des massiven Lobby-Aufwandes sei das Ergebnis durchaus zufriedenstellend (Klubunde). Etwas unterthematziert in dieser Debatte blieb die grundsätzlichere Frage, ob in einer von US-Konzernen dominierten Welt globaler Datenströme nationale Alleingänge im Datenschutz noch möglich sind, bzw. ob die Anhebung des gesamteuropäischen Schutzniveaus eine mögliche Senkung deutscher Standards nicht kompensiere – auch weil erst die EU-weite Regulierung das Ausspielen von Marktmacht in globalen regulatorischen Debatten ermöglicht.

Ob eine Absenkung deutscher Standards *in der Praxis* wirklich zu befürchten ist, blieb ungewiss. Gerade im Beschäftigten-Datenschutz sah Nadine Absenger (DGB) durchaus Tendenzen zur Aufweichung, die aber auf das neue Bundesdatenschutzgesetz, nicht die DSGVO, zurückgingen. Sowohl Paul Nemitz wie auch Moritz Karg (Hamburgischer Datenschutzbeauftragter) glaubten, dass Wettbewerb unter den europäischen Gerichten und Datenschutzbehörden um den besseren Grundrechtsschutz

sowie *peer pressure* tendenziell zu Race-to-the-Top-Dynamiken und somit – trotz oder gerade wegen der Auslegungsbedürftigkeit wichtiger Teile der DSGVO – zu einer Anhebung des Gesamtschutzniveaus führen würden. Nemitz und Karg wie auch Philip Schütz (Universität Göttingen) sahen die durch die DSGVO geschaffene Möglichkeit, empfindliche Geldbußen (bis zu vier Prozent des weltweiten Jahresumsatzes) zu verhängen, als potentiell sehr wirksames Druckmittel um „Disziplin in den Markt“ (Nemitz) zu tragen. Wo früher Unternehmen eher herablassend mit Datenschutzbehörden umgesprungen seien, gingen sie jetzt gleich in „Habachtstellung“, berichtete Karg. Nemitz rief die Aufsichtsbehörden daher auf, von ihren neuen Gewalten offensiv Gebrauch zu machen und den Gang vor die Gerichte nicht zu scheuen. Auch Thilo Weichert (Netzwerk Datenschutzexpertise) warnte, dass, sollten sich die Sanktionen als „Papier-tiger“ erweisen, Firmenverhalten sich schnell wieder ändern könnte.

Wieviel häufiger die Aufsichtsbehörden nun allerdings die gerichtliche Konfrontation mit großen, finanziell potenten Unternehmen suchen werden, bleibt abzuwarten. Die Mittel- und Personalausstattung der Aufsichtsbehörden ist, wie Schütz und Weichert bemerkten, meist sehr knapp. Marit Hansen (Datenschutzbeauftragte, Schleswig-Holstein) verwehrt sich daher

PLÄDOYER

Filme in Foresight- und TA-Analysen

Regula Valérie Burri, *HafenCity Universität Hamburg (HCU)*
 Überseeallee 16, 20457 Hamburg (regula.burri@hcu-hamburg.de)

auch gegen den Tenor, dass die Aufsichtsbehörden „jetzt alles richten müssten“. Dies sei schlicht unrealistisch; Datenschutz bleibe auch die Verantwortung der Gesellschaft als Ganzes.

Die praktischen Grenzen rechtlichen und behördlichen Vorgehens werfen die Frage nach technischen Lösungen (*Privacy by Design and Default*; PbDD) auf. Deren Einsatz ist in der DSGVO verpflichtend vorgesehen (Art. 25). Rege, zunehmend interdisziplinäre Forschungstätigkeit findet in diesem Bereich statt. So hörten die TagungsteilnehmerInnen u. a. von Projekten zu automatisierter und dynamischer Zertifizierung (NGCert), datenschutzgerechten Entwurfsmustern für Systementwickler (AnEkA), und Tracking Basisschutz für Nutzer (An.On). Wie

Datenschutz bleibt die Verantwortung der Gesellschaft als Ganzes.

Frank Pallas jedoch ausführte, ist technischer Schutz nicht umsonst zu haben. Bestimmte Verschlüsselungen können Kosten um 90 % steigern. Umsetzung von PbDD erfordere daher auch genaue Kenntnis der Kosten und explizite Nutzen-Kosten Abwägungen.

Fazit

Datenschutz als Querschnittsthema der Informationsgesellschaft, rapider soziotechnischer Wandel und verstärkte regulatorische Aktivität haben Dynamik in die Forschung getragen. Wie die regen, manchmal hitzigen Diskussionen während der Konferenz verdeutlichten, wird diese auch vorerst nicht abflauen.

Die nächste Jahrestagung des Forums Privatheit findet am 11. und 12. Oktober 2018 in München statt, zum Thema „Datenökonomie: Verbraucherverhältnisse und Geschäftsmodelle“.

Weitere Informationen

www.forum-privatheit.de

Proceedings der Jahrestagungen des Forums Privatheit:

Roßnagel, A.; Friedewald, M.; Hansen, M. (Hg.)

(in Vorbereitung): Die Fortentwicklung des Datenschutzes:
 Springer Vieweg (DuD-Fachbeiträge)

Friedewald, M.; Lamla, J.; Roßnagel, A. (Hg.) (2017):

Informationelle Selbstbestimmung im digitalen Wandel
 Wiesbaden: Springer Vieweg (DuD-Fachbeiträge)

Zukunftsvisionen wird seit einiger Zeit eine bedeutende Rolle für die Erkennung und Bewertung von Technologieentwicklungen und deren Folgen zugeschrieben. In diesem Beitrag plädiere ich speziell für eine größere Aufmerksamkeit der Technikfolgenabschätzung (TA) auf Filme als interessante und aufschlussreiche zusätzliche Quelle für die Untersuchung von soziotechnischen Zukunftsvisionen. Gerade in Filmen drücken sich gesellschaftliche Imaginationen über mögliche zukünftige Technikentwicklungen und deren Implikationen für die soziale Ordnung besonders deutlich aus. Filme sind deshalb, so der hier vertretene Ansatz, in Foresightstudien und TA-Analysen zu berücksichtigen.¹

Schon zu einem frühen Zeitpunkt wurde eine Diskussion um Leitbilder in der Technikentwicklung geführt (Dierkes et al. 1996). Grunwald (2012) forderte die Analyse von „Technikzukünften“, die er als „Vorstellungen über zukünftige Entwicklungen, in denen Technik eine erkennbare Rolle spielt“ (ebd., S. 23), definiert sowie eine daraus folgende „hermeneutische Erweiterung der Technikfolgenabschätzung“ (Grunwald 2015). Grin und Grunwald (2000) wiesen auf die Bedeutung eines entsprechenden „Vision Assessment“ hin. Lösch et al. (2016) schlagen ebenfalls die Analyse technologiebezogener Zukunftsvorstellungen wie beispielsweise Zukunftsbilder, Technikvisionen, Szenarien und Leitbilder vor, die sie unter dem Begriff „soziotechnische Zukünfte“ zusammenfassen. Dabei erkennen Lösch et al. (2016) an, dass soziotechnische Zukünfte in höchst unterschiedlichen Formen wie beispielsweise in Technikleitbildern, Simulationen, Szenarien, Roadmaps oder allgemeiner in Utopien und Dystopien auftreten und nicht nur durch Texte, sondern auch in Geräten, Bildern oder Organisationen materiell artikuliert werden (ebd., S. 8). Filme werden nicht explizit erwähnt.

Solche „Projektionen und Vorstellungen, die implizit oder explizit Zusammenhänge zukünftiger gesellschaftlicher Verhältnisse imaginieren“ (ebd., S. 7), gelte es in der TA zu analysieren. Für die TA seien diese Vorstellungen dabei nicht als Prognosen,

¹ Wie in Lösch et al. (2016, S. 6) wird hier diesbezüglich kein kategorialer Unterschied zwischen TA und Foresight gemacht, auch wenn diese beiden Felder in Bezug auf verschiedene Aspekte differenziert werden könnten (Zweck 2000).